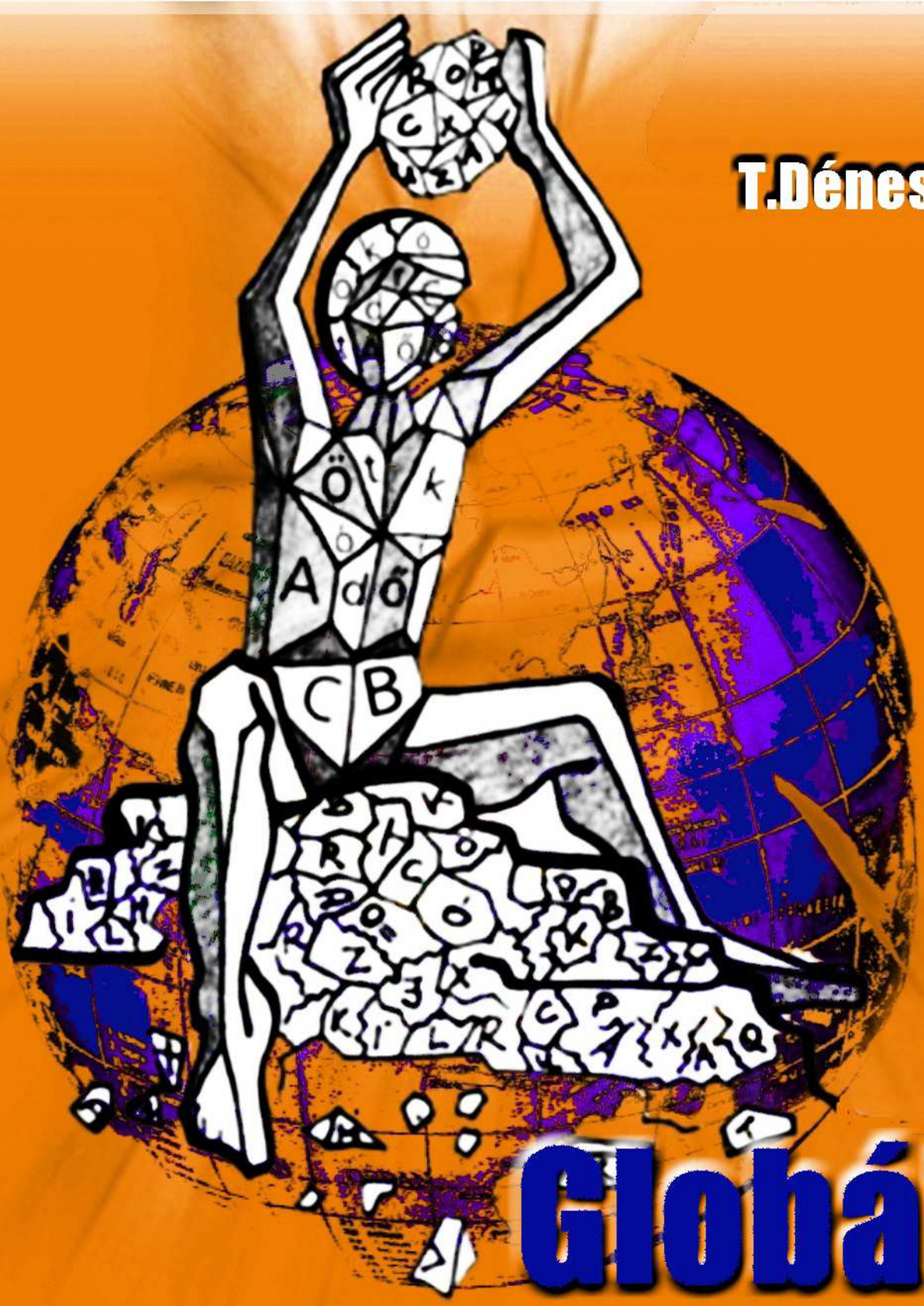
T.Dénes Tamás



a Globális TITOK

A 21. század kulcsa:

Biztonság az
Információalapú
Társadalomban

A Globális Titok

*A 21. század kulcsa: **B**iztonság az **I**nformációalapú **T**ársadalomban*

Szerző: *T.Dénes Tamás*

Nemzeti Kulturális Alap
Alkotói ösztöndíj támogatásával készült.

Készítette: *T.Dénes Tamás, Budapest, 2012.*
www.titoktan.hu

Sorszámozott példány

Sorszám: **0000**

ISBN 978-963-08-4453-6

Tartalomjegyzék

	E l ő s z ó, amelyben fény derül arra, hogy az *e-mber* az *e-társadalom* epszilonja	5
1.	**A titok relativitása, avagy mi a *mély titok* ?**	11
2.	**Két gondolkodási modell: *„Találd meg!” – „Találd ki!” (rejtés és rejtjelzés)***	18
3.	**Az *információbiztonság titka* a *redundancia***	25
3.1.	C.E. Shannon a modern információelmélet atyja	25
3.2.	Redundancia az információelméletben	26
3.3.	Redundancia a kommunikációban	30
4.	**A rejtjelzés és rejtjelfejtés forradalma: gépesítés a 20. században**	34
4.1.	Rejtjelző kerék	34
4.2.	Rejtjelző henger	36
4.3.	Rejtjelző gép	38
5.	**A számítástechnika gyökerei a rejtjelfejtésben fogantak**	49
5.1.	Összekapcsolt korongokból számológép	49
5.2.	A gépi rejtjelfejtés kezdete	53
5.3.	Az Enigma megfejtése, avagy a modern számítástechnika születésének titka	54
5.4.	Vissza Leibnizhez, akit megbabonázott a 2-es számrendszer	62
5.5.	Mégis Neumann-elvű napjaink számítógépe?	64
6.	**Tömeges információ + globális kommunikációs hálózat = globális e-társadalom**	67
6.1.	Valóban információt termel az információipar?	68
6.2.	Információrobbanás az információs társadalom kezdete?	70
6.3.	Globális társadalom paradoxon	71
6.4.	Biztonságos információs társadalom paradoxon	72
6.5.	A klasszikus és a globális kommunikáció modellje	75
7.	**Turing-teszt az e-társadalom napi gyakorlata** ***(Valódi vagy virtuális információ?)***	77
7.1.	A Turing-teszt	78
7.2.	A Turing-teszt és az e-kommunikáció	80
7.3.	A zero-knowledge proof („előismeretek nélküli bizonyítás”)	81
7.4.	A sakknagymester probléma	83
7.5.	Az átlagéletkor probléma	83
7.6.	A 21. század új kérdése: *Valódi vagy virtuális információ?*	85
7.7.	Turing szemléltető példája	86
7.8.	A Turing-teszt e-gyakorlata	88
7.9.	PÉLDÁK a már alakuló virtuális „valóságra”	90

8. Tömeges titkosítás és egyéni biztonság 92
(A dokumentumvédelem problémái és új módszerei)
8.1. Személyhez kötött és tömeges dokumentumok 92
8.2. Biometrikus azonosítás, avagy a szemény egyedisége és a dokumentum személyessége 96
8.2.1. Néhány szó a biometriáról 97
8.2.2. A legelterjedtebb biometrikus technológiák 97
8.2.3. Adatvédelmi aggályok 98
8.2.4. A biometrikus azonosító mint adat 99
8.3. Digitális aláírás, avagy a dokumentum tartalmának és tulajdonosának hitelessége 100
8.3.1. Elektronikus aláírás 101
8.3.2. Digitális aláírás 103
8.4. Digitális ujjlenyomat, avagy a dokumentumvédelem periódusos rendszere 106
8.4.1. A hiányzó láncszem a digitális ujjlenyomat 106
8.4.2. Dokumentumok azonosítása kriptológiai úton 107

9. Az Internet, avagy a globális hálózatok biztonságáról 111
9.1. Az Internet kialakulásából fakadó gyengeségek 113
9.2. A tűzfalak biztonsága 114
9.3. Az elektronikus kereskedelem biztonsága 116
9.4. Banki alkalmazások biztonsága 117
9.5. Adatbankok hitelessége és biztonsága 119
9.6. A mágnes-, illetve memóriakártyák biztonsága 121
9.7. A memóriakártya a biztonságos hozzáférés-védelem eszköze 123
9.8. A digitális pénz 124
9.9. A hozzáférés-védelem új módszerei 126

10. A NAGY TESTVÉR valósággá válik, avagy *nyílt globalizáció* ellen *rejtett háború* 128
10.1. George Orwell irodalmi utópiája: 1984 128
10.2. Newspeak azaz Újbeszél nyelv 130
10.3. *Újbeszél* az e-kommunikációban 131
10.4. NAGY TESTVÉR az e-társadalomban ECHELON-ná vált 133
10.5. Valóban mindent „lát” és „hall” a NAGY TESTVÉR? 134
10.6. NAGY TESTVÉR a tengerek mélyén 136
10.7. NAGY TESTVÉR az interneten 137
10.8. A STOA jelentések leleplezték az 50 éves NAGY TESTVÉR-t 138
10.9. A „húsevő” NAGY TESTVÉR 143
10.10. Polgári szabadságjogok, vagy „terrorizmus elleni küzdelem”? 147
10.11. NAGY TESTVÉR a 21. században, avagy a biztonság „visszalő” 151
10.12. A GLOBÁLIS NAGY TESTVÉR „beporozza a világot” 152
10.13. Leon Theremin alias Lev Szergejevics Tyermen (1896-1993) 154
10.14. Sir Robert Alexander Watson-Watt (1892-1973) 155
10.15. RFID az 1960-as évektől napjainkig 156
10.16. Néhány lehetséges RFID alkalmazás 157
10.17. Porszem nagyságú RFID chipek 157
10.18. RFID a NAGY TESTVÉR szolgálatában 158
10.19. ZÁRSZÓ, ami nem mondható el *újbeszélül* 160
11. ZÁRSZÓ UTÁN (*Meg kéne állni egy percre és elgondolkodni!)* 164
***„Lilatehén effektus”* vagy INFOSANCE a 21. század jövője?**
IRODALOMJEGYZÉK 167

E l ő s z ó

amelyben fény derül arra, hogy az *e-mber* az *e-társadalom* epszilonja

„Civilizációnk újkeletű és még nem nyomta rá bélyegét a testünkre.
Ha egészségesek akarunk lenni, testünket vissza kell helyeznünk
abba a környezetbe, amely számára kialakult."
(Szent-Györgyi Albert: Az élő állapot,
Kriterion Könyvkiadó, 1973.)

Ritka pillanatok részesei vagyunk, a Föld lakosságának kevesebb mint 20%-át kitevő, úgynevezett modern társadalmak egyedei, akiknek ajtaján kopogtat a 21. század információalapú e-társadalmának virtuális, vagy éppen túlságosan valóságos „szelleme". Ritka pillanat ez, hiszen az evolúció tíz … százezer … millió éves folyamában egy új emberfajta (tán csak mutáció?), az *e-mber* kialakulásának lehetünk tanúi, esetleg részesei.

Az elektronizáció cérnaszálán függő homo-sapiens az *e-mber* (ejtsd: *ímber*), aki az élővilág legkiszolgáltatottabb, legsebezhetőbb fajává küzdi le magát a táplálkozási lánc csúcsáról, miközben folyamatosan fejlődésről beszél.
Az *e-mber*, mint új fogalom, természetesen simul az *e*-mail (*ímél*), *e*-business (*íbiznisz*), *e*-banking (*íbanking*), *e*-society (*íszoszájeti*) stb. sorba, így talán fölösleges is a kiejtés zárójeles közlése, bár számomra az *„e" i*-ként való kiejtése modellértékű, mint a kritikátlan amerikanizálódás egyik jellegzetessége. Való igaz, hogy az angolban az *„e"* hangot szó elején, általában *„í"*-nek ejtik, az pedig mindenki számára világos, hogy esetünkben az *„e"* az *electronic* szó rövidítéseként használatos. Minden ilyen rövidítésnek (és szóösszetételnek) tehát van valódi magyar megfelelője, az *elektronikus* szó, amely szintén *„e"* betűvel kezdődik, ám magyar kiejtése egyszerűen *„e"* és semmiképpen sem *„í"*.
Mindazok, akik tehát szeretnék megőrizni magyar anyanyelvüket, nyugodtan mondják, hogy *e-levelezés* (az e-mail helyett), *e-kereskedelem* (az e-business helyett), vagy *e-társadalom* (az e-society helyett), ahol az *e*-t egyszerűen, magyar módra *e*-nek kell kiejteni.

Hogy *e* kérdés jóval mélyebb gondolatokat hordoz annál, hogy puszta nyelvészkedésnek tekintsük, érthetővé válik, ha teszünk egy kis gondolati kitérőt.

Erdős Pál (1913-1996)

Erdős Pál (1913-1996) a 20. század magyar matematikus óriása, az egész világon a matematika nagykövetének tekintették. Matematikai eredményein kívül különleges volt saját emberi világa is, amelynek részét képezte a speciális Erdős-nyelv (Erdős szótár). A család szereplőit sajátosan nevezte el: a férjet „rabszolgá"-nak, a feleséget „úr"-nak, míg a gyermeket *„epszilon"*-nak mondta[1]. Ez utóbbi onnan ered, hogy a matematikában a kicsiny mennyiségeket a görög epszilonnal szokás jelölni (a görög *epszilon* betű: ε). Erdős Pál egész életét a matematikával kötött „házasságban" élte le, így saját gyermeke nem volt. Mégis különösen szerette a gyermekeket, tehát nem a lekicsinylés, a jelentéktelenség vezette őt a „névadáskor". Rendkívüli memóriája arra is kiterjedt, hogy

[1] Az Erdős-nyelv egyedi, mélyen humánus világszemléletéről és magáról Erdős Pálról különleges megközelítésben olvashat az érdeklődő olvasó Czeizel Endre legújabb könyvében, amelyet a magyar matematikus géniuszokról, azok géniuszságának genetikai és társadalmi okairól írt [CZEIZEL E. 2011].

bármerre ment a világban, tudta minden kollégájáról, hogy van-e gyermeke és a személyes találkozásokkor első kérdései között szerepelt a *„Hogy van az epszilon?”*.

Napjaink globalizálódó társadalmi gyakorlatában mégis az *„e-mber”*-ről, az e-társadalom jelentéktelen, globálisan szorongó, felnőttként is *kicsiny gyermek-embere* és gyerekként *jelentéktelen kicsiny felnőttnek kezelt embere* jut eszembe. Be kell látnunk, hogy a mélyen emberi Erdős-nyelvnek ehhez mindössze annyi köze van, hogy a görög ABC-ben az *epszilon (ε)* megfelel a magyar *e*-nek. Vagy mégsem?

Erdős Pál 1990. nyarán
a szerző feleségével és a három epszilonnal
Eszter (13), Andrea (9), Ádám (3)

Hiszen az *epszilon* matematikai jelentése szerint, az emberiségnek is csak kicsiny része, kb. 15-20%-a van abban a helyzetben, hogy a közeli jövőben az e-társadalom kézzelfogható közelségébe kerülhet.

Ha a 20. század végén elkezdődött mesterséges rohanás[2] ilyen ütemben folytatódik, akkor az emberiség 80-85%-ának elszakadása a 15-20%-ától ugyanilyen rohamos mértékben (exponenciálisan) növekszik, míg véglegesen behozhatatlanná válik. Azaz a Földön élő emberiség két „kasztra” szakad szét. Márpedig, mint tudjuk, a kasztrendszer nem engedi meg a kasztok közötti mobilitást!
Mivel az e-társadalom az információ birtoklásán alapuló, azaz információalapú globális társadalmi rendszer, így a két kaszt közötti határt már nem az országhatárok fogják kijelölni, hanem egy globális gazdasági és kulturális koncentráció, amely valósággá teszi a globálisan centralizált társadalom orwelli rémét. Ez a globális társadalom tehát az *e-lit* (azaz információ-birtokos) és a *marionett bábuként kiszolgáltatott e-mberek tömegének* kasztjára bomlik, amely tulajdonképpen megfelel a 2000 évvel ezelőtti rabszolgatartó társadalom modern formájának.

Az *e-lit* kaszt teljes gazdasági és információs kiszolgáltatottságban tarthatja a *tömeg*et, azaz az ókorinál ördögibb rabszolgaság valósulhat meg: az *információs gyarmatosítás*. A *tömeg* teljes, észrevehetetlen manipulálhatósága, a virtuális és valós világ teljes összekeveredése, az *információs rabszolgaság*. Most kéne kicsit megállni!
Higgadtan végiggondolni a hosszú távra kiható súlyos döntéseket. Most még (talán) lehet nem benevezni a *„virtuális agárversenyre”*!

[2] Melyet ***„virtuális agárverseny”*** effektusnak neveztem el, aminek zászlajára eme feliratot írhatnánk: ***„Érjük utol a nemlétező nyulat egy virtuális agárversenyen!”***

Elismerem, a fenti gondolatok szárazak és mellbevágók. Manapság még az informatikával, információbiztonsággal és az ezekkel kapcsolatos döntésekkel foglalkozók körében is átláthatatlanok. Erre utal az az eufórikus hangulat, amely a globális e-kommunikációs rendszereket körülveszi, olyannyira, hogy a jövendő kor, az információsnak nevezett (információalapú) társadalom eddig ismeretlen és korszakos problémáiról teljességgel elvonja a figyelmet. A hivatalos felfogás hajlamos az információalapú társadalmat valamiféle technikai bravúrnak (pl. internet, e-kommunikáció, digitális technika, stb.), semmint emberi életek, emberi viszonyok bonyolult rendszerének tekinteni, amelyben a legfontosabb kérdés: *„Hogy van az epszilon?”*. Mindezek alapján, egyáltalán nem egyszerű nyelvészeti probléma, hogy …

Vajon új emberi minőség az *e-mber*,
avagy a 21. század e-társadalma lesz az *új e-mber kovácsa*[3]?

Az információipar, mint a 20. század második felének új és egyre hatalmasabb ágazata, megkezdte és a 21. század első évtizedeiben egyre rohamosabb ütemben folytatja az információ tömegtermelését. Ezen új ágazat alapanyaga, félkész és végterméke is az *információ*. Az emberiség kisebb része(!) elérkezett egy olyan társadalmi modell beteljesedéséhez, amelynek középpontjában az információ áll, és legnagyobb hatású ágazata az információipar, ez az ***információalapú társadalom***, amelyre ma még jobban illik az *adat-hír dömping társadalom* elnevezés.
Ahogy a fejlett országokban az elektromosság nélkülözhetetlenné vált az élet minden területén és kialakult a teljes elektronikus függőség a társadalomban, úgy vagyunk szemtanúi annak, ahogy kialakulóban van az információfüggőség (*adat-hír függőség).*

Az információtechnológia alkalmassá vált az idő és a tér távolságainak szinte nullára zsugorítására. *Ez a jelenség teszi az információrobbanást korszakhatárrá és az információalapú társadalmat új társadalmi formává.*

A klasszikus kommunikáció magában rejtette a személyesség, az azonosíthatóság jegyeit. Az így kialakított kétoldalú, szimmetrikus függőség *(Te tudod, hogy én ki vagyok, én tudom, hogy Te ki vagy),* kölcsönös ellenőrizhetőséget és ezáltal *kölcsönös biztonságérzetet* teremtett.
Az információalapú társadalom azonban a tömegesen és gyorsan elérhető információdömping oltárán feláldozza a személyességet és egy *fekete doboz* modellt valósít meg. Ebben a modellben egy óriási információtárolóval kommunikál minden felhasználó. A modell úgy működik, hogy mindenki egy közös dobozba („fekete doboz”) helyezi be az információit és ebből annyit vehet ki, amennyire a „fekete doboz” engedélyt ad. A függőség tehát egyoldalúvá vált, ami a tömeges felhasználók *kiszolgáltatottságát* és így *biztonságának hiányát* eredményezi.

A probléma az információalapú társadalom kulcskérdéséhez vezet. A 20. század 30-as éveiben A.M.Turing a mesterséges intelligencia kutatásának atyja fogalmazta meg az alábbi gondolatmenetet: *"Azt állíthatjuk, hogy egy gép gondolkodik, ha kérdéseket tehetünk fel neki,*

[3] *Az új ember kovácsa (Pedagógiai hősköltemény)* Anton Szemjonovics Makarenko (1888-1939) fő műve, amelynek címe már-már szállóigévé vált. Irodalmi formában fogalmazza meg pedagógiai hitvallását: *„Az emberi élet igazi ösztönzője a holnap öröme … Először az örömöt magát is meg kell szervezni, életrehozni és lehetőséggé változtatni. … Az ember nevelése azt jelenti, hogy megadjuk azt az ösztönzést neki, amely a holnap öröméhez vezet.”* Az eredeti orosz kiadást (Педагогической поэме) Makarenko így datálta: Harkov, 1925-1935. Első magyar kiadása 1947-ben jelent meg az Új Magyar Könyvkiadónál (1957. óta Európa Könyvkiadó) *Pedagógiai hősköltemény* címmel.

éspedig tetszőleges kérdéseket és az úgy válaszol, hogy ha nem 'nézünk oda', nem tudjuk, hogy a felelet géptől, vagy embertől származik-e."

Turing gondolatmenete látnoki volt, ugyanis tökéletesen illeszkedik az információalapú társadalom globális kommunikációs hálózataira. Hiszen a kommunikációs hálózat minden felhasználója valóban egy monitor előtt ül és kérdéseket tesz fel. A monitoron megjelenő válaszok tartalmából azonban, ha odanézünk sem dönthető el biztonságosan a válaszoló személye, így annak valódi, vagy virtuális volta sem!
A válaszoló *személyének, azaz az információ forrásának bizonytalansága* felveti az általa képviselt információk valódiságának, a ***virtuális információknak*** a problematikáját. Ez az információalapú társadalom kulcskérdése: a GLOBÁLIS TITOK.

Ugyanakkor a 21. század globális társadalmi fejlődésének deklarált célja, a *tudásalapú társadalom*, amely csak biztonságos ismeretekre, azaz a tudás biztonságára épülhet!
Különösen éles a probléma, ha figyelembe vesszük, hogy ma már a világháló, az elektronikus és digitális információtárolás és továbbítás különböző eszközei egy *"mindentudó elektronikus kommunikátorrá" olvadnak össze*, amely szinte láthatatlanul vezérli, irányítja életünket. A társadalom alapvető működési formájává válik a ***tömeges titkosítás és egyéni biztonság paradoxon.***

Eddigi TitokTan köteteimben igyekeztem felhívni az Olvasó figyelmét arra, hogy a titkokról, a titkok elrejthetőségéről és megőrizhetőségéről minden korban jelentősen megoszlottak a vélemények. Az *információbiztonság*, mint bármely biztonsági terület tehát nagymértékben függ a társadalmi közfelfogástól, az úgynevezett *veszélyérzet*től. Példaképpen idézzünk fel két különböző korból származó szélsőséges felfogást:
Benjamin Franklin (18. század vége): *„Hárman akkor tudnak titkot tartani, ha közülük kettő halott."*
Henry L. Stimson (1920-as évek): *„Úriember nem olvassa mások levelét."*

Míg az utóbbi vélemény a titkok megőrzésébe vetett maximális bizalmat, addig a másik a szélsőséges bizalmatlanságot fejezi ki. Vajon a ma már köztudomásúvá vált, egész Földünket behálózó és a teljes e-kommunikációs forgalmat „figyelő" ECHELON (műholdas lehallgató, vagy Carnivore rendszer) ismeretében a mai valóság melyik véleményhez áll közelebb?

Az *információalapú* társadalom, de különösen a célul kitűzött *tudástársadalom* alapkérdése tehát, e kötet alcímébe rejtett *BIT*[4], röviden a VALÓSÁGOS vagy VIRTUÁLIS JÖVŐ?
A probléma lényege az, hogy egy részben (vagy egészében!) virtuális információkkal feltöltött fekete doboz rendszer, a gyanútlan felhasználó számára eldönthetetlen módon *virtuális valóságot* állít elő.
Érthető tehát, hogy ha a globális modellben ismereteink megszerzése egyetlen kommunikációs köldökzsinóron kötődik az átláthatatlan kezekben tartott "fekete dobozhoz", úgy az abban tárolt GLOBÁLIS TITOK virtuális ismereteket és így virtuális valóságot generál. Ez a ma még csupán elméleti lehetőség az emberiség számára beláthatatlan veszélyeket rejt:

Az információk tömegét és az ezeket tároló és működtető rendszereket birtokló hatalom manipulációs lehetőségét az egyes e-mberek, csoportok, sőt az egész társadalom felett!

[4] ***B***iztonság az ***I***nformációalapú ***T***ársadalomban

Ördögi eszköz tehát az "információs fegyver", amellyel észrevétlenül lehet láthatatlan információs rabszolgaságba sodorni emberek millióit.

A 21. század szinte első napjaiban (2001. szeptember 11-én) a Földünket körülvevő és „védő" információpajzs, akárcsak a természetes védelmet nyújtó ózonpajzs, kilyukadt!
Az ECHELON szimbolikus jelentései (harcvonal, harcrend) valóságossá váltak, a fenti kérdések megelevenedtek és a sok ezermilliárd dolláros titkos befektetés, amely a *„terrorizmus elleni védekezés zászlaja alatt"* az elmúlt három évtizedben történt, nyilvánvaló kudarcot szenvedett. A dollár milliárdokkal a titkosítás több száz éves módszerei, a sztegonográfiai módszerek, a rejtjelzés nélküli rejtés, a szöveg a szövegben, kép a képben módszerei állnak szemben. A sztegonográfia elektronikus renaisance-át éli. A szomorú az, hogy mint a történelem során már annyiszor, elsőként a rossz oldalon. Sajnos ismét beigazolódott A.Einstein igen bölcs gondolata: *„A történelem mindössze arra tanít meg bennünket, hogy az emberiség semmit sem tanul a történelemből."*
2001. szeptember 11-e óta a GLOBÁLIS TITOK-ról, az e-világ biztonságáról alkotott *egyértelmű képet* kényszerül az emberiség *átfesteni*. A történelem dupla felkiáltójellel hívta fel az emberiség figyelmét arra, hogy a jövendő társadalom kulcsa a *BIT*, azaz a biztonság legyen!

Szeretném a titkosítás-szakértő szemüvegén át a kód és kódolás társadalmi beágyazódását bemutatni, amely elvezet a 21. századi társadalmak kulcsához. Az utóbbi 20 évben folytatott kutatásaim meggyőztek arról, hogy a 20. századi titkosítás fejlődésének szemüvegén át lehet csak igazán megérteni korunk információalapú társadalmának biztonsági problémáit (a terrorizmus és maffia, valamint a legmodernebb elektronikus bűnözést is beleértve).
Meg kell érteni mindenkinek, döntéshozóknak és a társadalom testét alkotó tömegeknek egyaránt, hogy az információalapú társadalom mélyén jelen könyv címe szerinti *BIT* munkál. A rohamos sebességgel növekvő technikai fejlődés, a totális elektronizációhoz és a digitális technika hétköznapi elterjedéséhez, vagyis a soha nem látott bonyolultságú globális társadalomhoz vezet. Márpedig egy tömeges információt kibocsátó, továbbító és tároló társadalomban csak a tömegesen alkalmazható, ám mégis egyedi biztonságot nyújtó rendszerek jelentenek társadalmi méretű biztonságot. Ez Jókai utópisztikus regényére asszociálva a *„jelen század reménye"*.

A 21. században tehát már nem csak az atom, a kémiai, vagy biológiai fegyverek társulnak a *„csodafegyver"* fogalmához, hanem a láthatatlan és ezért talán legördögibb *„információs fegyver"*, amely képes valódi emberekből virtuális társadalmat létrehozni. Így a hatalom manipulációs lehetőségei elképzelhetetlen mértékben megnőhetnek és az információalapú társadalom *„a hatalom üzleti vállalkozásává válhat"*.

A kriptológia (a titkosítás és titokfejtés tudománya) szemüvegén át mutatom meg, hogy az információs gyarmatosítás nyomasztó víziója helyett bölcsebb, ha a valódi és virtuális titkok megkülönböztetésére idejében felkészülünk.
Mindeközben igyekszem az Olvasót közérthető formában bevezetni a kriptológia legújabb elméleti eredményeibe és ezek alkalmazási lehetőségeibe.

Jelen kötettel legfőbb célom, hogy az információs (csoda)fegyver csak rémes utópia maradjon. Hogy ez nem csupán óhaj, vagy figyelmeztető kiáltás, azt a kötet második részében tárgyalt megoldási utak bizonyítják!
E fejezetek rávilágítanak arra, hogy az információalapú társadalom ma még elérhető nagy lehetősége, egy neorenaissance, azaz modern információs renaissance kor, *a 21.század*

INFOSANCE[5] *korának megteremtése, amely tulajdonképpen egyesíti a klasszikus és modern értékeket, vagyis az emberi értékek, az alapvető természeti és társadalmi törvények sokoldalú megközelítése, a modern technika, a digitalizáció, az infokommunikáció eszközeinek segítségével. Tehát az információalapú, majd tudástársadalom igen mély biztonsági problémái felett kiviláglik az „információs fegyver helyett INFOSANCE" pozitív jövőképe.*
A szerző által az ezredfordulón bevezetett fogalom, az INFOSANCE a gondolkodó ember klasszikus képességeinek optimális egyesítése a mindent átszövő, globalizálódó e-technikával és az egyre teljesebb, biztonságosabb információ szimmetrikus, egyenrangú birtoklásával. Az INFOSANCE olyan e-társadalom képét rajzolja fel, amelynek középpontjában új, modern renaissance *e-mber* áll, akinek történelmi lehetősége egy "új ablak nyitás", amely a felhalmozott óriási technikát, a globális kommunikációs és informatikai rendszereket egyesíti a renaissance mintájú szabad, szárnyaló, kreatív, emberi gondolkodással. Ebben a társadalomban természetessé válik Erdős Pál humanista kérdése: *„Hogy van az epszilon?"*, azaz *„Hogy van az e-mber?"*
Az INFOSANCE társadalma tehát kreatív társadalom, amely akárcsak az emberi kreativitás, a társadalmi túlélés alapfeltétele.

Ajánlom e kötet gondolatait minden fiatal figyelmébe,
akik már olyan e-világba születnek, amely az e-társadalmat
hajlamos technikai bravúrnak tekinteni.
Legalább ennyire ajánlom e gondolatokat mindazoknak a döntéshozóknak
(nevezzük nevén: az e-hatalomnak), akik egyszerre a 21. század
információs „csodafegyverének" birtokosai és kiszolgáltatottjai.

Budapest, 2012. a Szerző

[5] A szerző által definiált mozaikszó: INFOrmációs renaisSANCE

1. A titok relativitása avagy mi a *mély titok* ?

„A rejtjelfejtés az agy gyarló feltörése,
mivel a világ minden dolga,
az egész természet,
merő rejtjel és titkosírás.”
(Blaise de Vigenére 1523-1596)[6]

Egy könyv megírásának talán legnehezebb intellektuális pillanata a címadás. Néhány szóba kell tömöríteni több száz oldalnyi, jelen esetben több évtizednyi gondolatot. Vagyis az Olvasó pontosan fordítva találkozik a szerző gondolataival, mint ahogy azok megszülettek. Először olvassa a könyv címét, amely annyira felkeltette az érdeklődését, hogy a kötetet kézbe vegye, és csak ezután találkozik a részletesen kifejtett gondolatokkal, amelyekért a mű valójában megszületett. Minél rövidebb a cím, annál személyesebb asszociációk tapadnak hozzá és annál jobban hasonlít a szerző egyfajta Erdős-szótárához. Különösen igaz ez akkor, ha a címben a TITOK szó szerepel, amelynek jelentése az emberiség talán legmélyebb titka, amint az Blaise de Vigenére fenti mottóban idézett gondolatából kitűnik.

Gyerekkorom óta különös vonzalom köt a TITOK fogalmának megértéséhez. E vonzalom hajszálgyökerei talán kisgyerekkoromból erednek, amikor Erdős Pál ellátogatott hozzánk és értetlenül hallottam, amint két matematikai probléma megbeszélése között apámtól megkérdezte: *„Mit csinál az epszilon?”* Azt valahogy megéreztem, hogy az *epszilon* valami nagyon tudományos dolog lehet, de el sem tudtam képzelni, hogy mit csinálhat az *epszilon*?
Jóval később megértettem, hogy ez csak az Erdős-nyelv birtokában értelmezhető, sőt *A kis herceg* bevezetőjét olvasva, arra is rádöbbentem, hogy pontosan azt éltem át, amit Antoine de Saint-Exupéry (1900-1944) a kisgyerekkori rajzával, amely egy *óriáskígyót ábrázol amint éppen egy elefántot nyel el*, de a fölnőttek egyszerűen csak *kalapnak* nézték.
Azonban az én esetemben minden pontosan fordítva történt. Nem fölnőttként, hanem kicsiny gyermekként álltam értetlenül Erdős Pál gyermekien szabad nyelvi asszociációja előtt, miközben egyáltalán nem azt a fölnőtt következtetést vontam le az esetből, amit a Saint-Exupéry rajzát szemlélő fölnőttek[7], sőt kíváncsiságomat egy életre felkeltette, hogy *„mit csinálhat az epszilon?”*.[8]

---

[6] Blaise de Vigenére a 16. század, de mondhatjuk, hogy a titkosítás történetének egyik legjelentősebb alakja. Munkásságát részletesen tárgyalja a TitokTan Trilógia 2. kötet 13. fejezete [TDT 2004-k].

[7] *„Most aztán a fölnőttek azt ajánlották, ne rajzoljak többé óriáskígyót se nyitva, se csukva, …”* (Antoine de Saint-Exupéry: A kis herceg)

[8] Abban mégis hasonlít a történetünk, hogy Saint-Exupéry gondolkodását is egész életében végigkísérte *„a kalap”* esete. Olyannyira, hogy sajnálatosan rövid életének utolsó évében megírta egyetlen „mesekönyvét”, *A kis herceget*, amely nagyon is a fölnőtteknek szólt és amelynek gondolatcsírája éppen *„a kalap”* kisgyerekkori esete volt. Több mint érdekesség, inkább az alkotó emberi elme figyelemreméltó tanulsága, hogy Saint-Exupéry vadászpilótaként sok könyvet írt repülős történetekről (1926. A pilóta, 1929. A déli futárgép, 1931. Éjszakai repülés, 1939. Az ember földje, 1942. A hadirepülő, 1943. Levél egy tűszhoz), amelyek szinte a feledés homályába merültek. Egyetlen „mesekönyvét”, az 1943-ban megjelent *A kis herceg*-et azonban azóta a világ minden jelentősebb nyelvére lefordították és számtalan kiadást ért meg. Talán nem véletlen, hogy *A kis herceg* történetének középpontjában éppen az emberi TITOK áll, amelyet Saint-Exupéry igyekszik röviden definiálni, *„Tessék, itt a titkom. … Ami igazán lényeges, az a szemnek láthatatlan.”*, de mégis egy egész könyv kellett hozzá, hogy leírja.

Talán éppen ez vetette el bennem a titkos gondolatmagot, amelyből hosszú évek alatt fejlődött gondolatvirággá a *mecsoti* mozaikszó, azaz a *mese-csoda-titok* fogalma[9], ami megdöbbentően rímel Lukács György (1885-1971) filozófus irodalomelméleti tételére [LUKÁCS GY. 1918]:
„A mese úgy viszonylik az összes többi irodalmi műfajhoz, mint a nem-euklidészi geometriák az euklidészihez”.
Azaz minden más irodalmi műfaj a tökéletes szellemi szabadságot megtestesítő mese valamely speciális esete. Hol a helyszínek, hol a szereplők, hol a cselekmény közelít a megélhető valósághoz. Így foghatjuk fel a fenti kötőjeles szóhármast (*mese-csoda-titok*), akár egyetlen fogalom három alakjának, amelyből megalkothatjuk egy szóba tömörített titkos fogalmunkat, a *mecsoti*-t.
Eme gyermekien játékos hangzású mozaikszó, ugyanúgy működik, mint számtalan társa a mesékben, mint valamely varázsige, melynek kimondása nem csupán egyetlen csodálatos ajtót nyit ki, hanem egész gondolkodásunkat helyezi a gyermeki szabadság ezer-meg ezerajtós palotájába. A mesékben a természeti törvények, de még a társadalmi érdekek vaskeze sem szorítja határok közé az emberi vágyat, inkább az állandó csodatörténés a korlátlan vágyteljesülés víziójának nyit utat. Miközben a fantázia-gondolatok mélyén a titok elrejtésének és megfejtésének ősi ösztöne dolgozik.

Jogos tehát a kérdés és igen meglepő a válasz, melyet Hermann Imre (1889-1984) S. Freud egyik legjelentősebb követője így fogalmazott meg: *„Mi van már most a titokban, ami a közlési vágyat állandóan ébren tartja? Egy szóval megnevezhetjük: a titok elszigetelő ereje. Amíg titkomat magamban őrzöm, magányos ember vagyok. Nem a titok tartalma izolál, de a titokőrzés ténye önmagában … A nyelv nemcsak a közlés, hanem az eltitkolás eszközéül is szolgálhat.”*

Bizony, a *mecsoti* és így az egész irodalom, maga a titkosítás, amely a nyelv segítségével rejti el legnagyobb közös titkunkat, a valóságot, csupán azért, hogy aztán a közlési vágy emberi ösztönét kiélve el tudják mesélni azt. A gyermeki őszinte nyitottság a világ minden titkának befogadására, és egyben az elfojthatatlan közlési vágy a *mecsoti* lényege, az emberi lét értelme és talán igazi célja is. Nem véletlen, hogy Karinthy Frigyes *Előszó*-ként, azaz mindenek előtt, éppen a titokról és éppen így ír:

„Nem mondhatom el senkinek,
Elmondom hát mindenkinek.
Próbáltam súgni, szájon és fülön,
Mindnyájatoknak, egyenként, külön.
A titkot, ami úgyis egyre megy
S amit nem tudhat más, csak egy meg egy.”
(Karinthy Frigyes: Előszó részlet)

A „Mit csinálhat az epszilon?” *gyermeki kíváncsisága által elvetett gondolatmag negyven éven át érlelődött, míg a matematika, a titkosítás és titokfejtés (kriptográfia, kriptológia), az információalapú társadalom kutatásának táptalaján, megérett bennem a TitokTan gondolata. A TitokTan műfaját tekintve, egyfajta kultúrtörténet, amely a kultúrát a titkosításszakértő különös szemüvegén át mutatja be.*

[9] A *mecsoti* fogalmát a *Titkosítás és … szépirodalom* című kötetemben [TDT 2010] indítottam útjára. A *mecsoti* a ***me***se, ***cso***da, ***ti***tok szavak első szótagjaiból képezett mozaikszó.

Az ezredfordulón határoztam el, hogy több évtizede felgyűlt és rendszerezett ezirányú gondolataimat három kötetben foglalom össze, amely TitokTan Trilóga *címmel került az Olvasók kezébe ([TDT 2002-k], [TDT 2004-k], [TDT 2005-k]).*

T*emérdek*
I*nformáció,*
T*alány, ami*
O*lykor*
K*iderül*

Matematikusként nyilvánvaló volt, hogy vállalkozásomat az alapvető fogalom, vagyis a titok *definíciójával kell kezdenem. Ez annál is természetesebb volt, mivel a sok ezer oldalnyi forráskutatásból világossá vált, hogy a köznyelv vagy alapfogalomként kezeli a* titok *fogalmát, vagy egyszerűen szinonímákat, körülírásokat használ annak meghatározására (ismeretlen, rejtély, kevesek által ismert, stb.). Illusztrációként íme néhány szélsőséges, ám szerzőik okán mindenképpen figyelemreméltó példa:*

„Mert nincs oly rejtett dolog, ami napfényre ne jőne: és oly titok, ami ki ne tudódnék." Újtestamentum (Máté 10:26)

„Titokban bizony már csak oly szó marad, mi kettőé. Három közt meg nem marad, s bizony, hogyha négy tudja, széjjelszalad." Firdauszi perzsa költö (934-1020)

„Hárman akkor tudnak titkot tartani, ha közülük kettő halott." Benjamin Franklin (1706-1790) Az Amerikai Függetlenségi Nyilatkozat kezdeményezője

„A titok ajtaját nem olyan nehéz kinyitni, mint ahogy azt a tudatlan emberek gondolják. Ellenkezőleg, az a szörnyű, milyen nehéz bezárni." Akutagava Rjunoszuke (1892-1927) japán író

„Úriember nem olvassa el mások levelét."[10] Henry L.Stimson (1867-1950) az USA külügyminisztere 1929-30 között

„*Akik azt lódítják, hogy egy rejtjelzett levelet minden előzetes segítség nélkül el tudnak olvasni úgy, hogy annak tárgyát sem ismerik, azok nagyobb sarlatánok, mint azok, akik azt lódítják, hogy megértenek egy nyelvet, amelyet korábban nem tanultak."*
Arouet Francois Marie Voltaire (1694-1778) a francia felvilágosodás kiemelkedő gondolkodója

E néhány példa jól illusztrálja, hogy a titok definíciók többnyire a titok legfontosabb jellemzőjeként az azt birtoklók számát jelölik meg, de néha a titok tartalmát, vagy ami ezzel rokon, a megfejthetőségét emelik ki. Tehát a jelen fejezet mottójában idézett Vigenére gondolat alapján sem meglepő, hogy a „mi a titok?" kérdés egyszerű definícióval történő megválaszolása helyett az eredmény, a titok „relativitáselmélete" lett, amelynek részletes kifejtéséhez a TitokTan Trilógia teljes első kötetére volt szükség.

Akutagava Rjunoszuke szavaival mondhatjuk, hogy a titok egy-egy „ajtó" mögött rejtőzködik. Az ember a kezdetektől fogva mindig arra kíváncsi, hogy mi van az ajtók mögött? Ezért megpróbál minden ajtót kinyitni. Sokszor könnyű a dolga, mivel az ajtó félig, vagy csak résnyire, de nyitva van, így a kíváncsiskodó bekukkanthat rajta. Talán éppen a mindig kíváncsi gyermeknek találták ki a kulcslyukat, amin keresztül lélegzetvisszafojtva megpróbál megtudni mindent, ami az ajtó mögött rejtezik. Aztán fölnőtt korában már csak diszkréten megáll az ajtó előtt és mutatóujját pisszegő szája elé emelve, mindenkit izgatottan csendre int, mert odabenn … valami titok tartózkodik.
Mi? vagy Ki? van az ajtó mögött, többnyire már csak erre szeretne választ kapni a sok Saint-Exupéry-féle „kalap-fölnőtt", akit a tisztán kíváncsi „epszilon-gyermek"-től eltérően sokszor

[10] Eredeti szöveg: *„Gentlemen do not read each other's mail."*

a válasz nem is érdekel, mert már előre „tudja”, hogy az néha kiábrándító. Pedig nem tudhatjuk soha, hogy melyik ajtó mögött van igazi *titok*. Ezért aztán évezredek óta megpróbálunk továbbra is minden ajtót kinyitni, belesni, befülelni, minden érzékszervünkkel átjutni a túloldalra, ahol a *titok rejtezik*.
Minél fölnőttebbek leszünk, annál inkább az ajtókból már csak a zárakat látjuk. Valami belső hang suttogja, hogy *„Nyisd ki és menj be!”*. Valami titkos erő vonz (vagy taszít?) a túloldali *titok* felé, és mint a túltermelt gyomorsav a gyomorból, törnek fel és marnak a kérdések: *„Ki zárta be az ajtót és miért?”*, *„Milyen kulcs nyitja a zárat és hol lehet az a kulcs?”*, *„Ki lehet-e nyitni kulcs nélkül a zárat?”*, vagy agresszív változatban: *„Ki lehet-e feszíteni, vagy be lehet-e törni az ajtót?”*. A sikertelen kísérletek idővel a legtöbb fölnőttben megfogalmazzák a gondolatot: *„Nem is olyan érdekes, hogy mi van az ajtók mögött.”* … majd megfáradtan letesz a kérdezésről is.

Pedig mi, akik felnőve is képesek vagyunk nem „kalap-fölnőttek”-ké válni, hanem epszilon nyitottsággal nézzük a világot, tudjuk, hogy mindig a zár, az ajtó kinyitása az igazi titok, függetlenül attól, hogy mi, vagy ki van az ajtó mögött. Mert a kulcs megtalálása, vagy kitalálása, az ajtón a zár kinyitása, maga az emberi megismerés, a gondolkodás, ahogy azt Blaise de Vigenére bölcs tömörséggel megfogalmazta: *„… a világ minden dolga, az egész természet merő rejtjel és titkosírás.”*

A végtelen számú ajtó tehát maga a természet, a társadalom, az élő és élettelen világ, de legfőképpen maga az ember. A megismerés, a kíváncsiság pedig az örök fogócska, a „rabló-pandúr”, a „macska-egér”, az az ördögi játék, amelyben kiderül, hogy minden kinyitott ajtó mögött ezer meg ezer még bezárt ajtót találunk, melyeket eddig még ismeretlen zárakkal zárt be az ismert, vagy titkos másik fél, a „rabló”, a „pandúr”, vagy éppen maga a természet.

A TitokTan Trilógia első kötetének alcíme a Kódtörő ABC jelzi, hogy igyekszik a *titok természetét* és hol rejtett, hol nyilvánvaló törvényeit körüljárni, azaz feltörni a definíció lényegét. Ehhez kísérőt, segédet, titkos útitársat is adtam az Olvasó mellé, aki végigkísérte a *titok* körüli szellemi kalandtúrán.
Kódtörő nem egy klasszikus detektív ... nem egy hétköznapi lény ... Ő *Kódtörő* a *rendszer(elme)*, akiben ott lappang az ősi kíváncsiság, a megismerés, a kutatás, a rendszerezés vágya, ... Ő maga a *rend(szerelme)*.
Kódtörő nem angol, nem belga, nem francia, nem amerikai és persze nem magyar, ... Őt nem lehet egyetlen nemzetnek sem kisajátítani, mert Ő minden emberből egy kicsi ...
Kódtörő nem kövérkés és nem is sovány, nem alacsony, de nem is magas, nem tudni a korát (öreg-e vagy fiatal?), no meg azt sem, hogy mennyi pénze van, mert Ő minden emberből egy kicsi ...
Kódtörő nem jó és nem rossz, nem szép, de nem is rút, nem hiú és nem szerény, nem gonosz és rosszindulatú, nem szomorú, nem is vidám, nem gép, nem elektronikus robot, mégsem fárad el soha, mert Ő minden emberből egy kicsi ...

Akkor hát milyen tulajdonságai vannak *Kódtörő*nek? - kérdezi Ön. És én erre azt válaszolom, hogy egyetlen tulajdonsága van: *a kíváncsiság*, a titkok elrejtésének és megfejtésének ősi ösztöne, mert Ő minden emberből egy kicsi ... mert *Ő a rend(szer)elme*.
*Kódtörő*nek ezer és millió arca van, mindannyiunkhoz közel áll, mert mindenki azt láthatja belőle, amit látni akar. *Kódtörő* nyomozó? Mi után nyomoz Ő? Lehet, hogy Ő maga a *titok*?!

Íme a névjegye:

K*ét énem*
Ó*koroktól*
D*iszkréten*
T*itokfejtő, ám*
Ö*rök*
R*ejtélyeket*
Ő*rző*

Kódtörő ebben a kötetben is végigkíséri Önt gondolati kalandtúránkon és minden fejezet végén megjelenik, mert hiszen Ö a *rend(szer)elme*.

Kódtörő segít megérteni, hogy a *titok nyitja* és egyben az emberré válás kulcsa, pontosan a homo sapiens megkülönböztető jegye: *a gondolkodás, a fogalomalkotás megjelenése*. *A gondolkodás tehát ősidőktől az emberiség közös titka.*

Kezdetben a gondolkodás a *titok* mennyiségi definícióinak megfelelően magányos „műfaj" volt, mivel a szó mai értelmében vett kommunikáció híján, minden egyed csupán a saját „érvényesülésére" használhatta fel.
Az utókor számára az emberiség e közös titkának eredete is igen érdekes *titok*, mivel olyan ősi korokról kell képet alkotnunk, amelyekből alig-alig maradtak tárgyi emlékek (írásosak pedig egyáltalán nem, hiszen ekkor még az írásbeliség csírái sem alakultak ki).
A magányos gondolkodás, az egyedi *titok* egyre bonyolultabb és hatékonyabb eszközök és cél elérési stratégiák formájában nyilvánult meg, azaz az emberi társadalom a magányos titkokat (gondolatokat) igyekezett a közös célok érdekében egyesíteni. Így alakult ki a Hermann Imre által jelzett „közlési vágy" kényszere, azaz maga a kommunikáció, ennek kihívására a beszédnyelv, majd a gondolatok rögzítésére az írás.
Ezzel párhuzamosan az emberiség közös titka -a gondolkodás- egyre inkább a gondolatok eltitkolásának eszközévé is vált (különböző nyelvek, jelrendszerek, titkosírások kialakulása). A titkolódzás gyermeki játékból a fölnőttek komoly tevékenysége lett, míg a 20. század elektronizációs technikai robbanása lehetőséget teremtett az információ tömeges áramlására, a legősibb jelrendszer –a számok- újra felfedezése pedig megnyitotta az utat a globális digitalizációnak. Az emberiség közös *(globális) titka* –a gondolkodás- mára már technikai értelemben is globalizálódott.
A gondolkodásnak, speciálisan a tudomány és technika fejlődésének (mindenképpen ide kell értenünk a titkosítás tudományát is) megvannak a maguk törvényei. Ezek közül talán a legfájóbb és legigazságtalanabb, hogy minden korhoz hozzátartoznak a „látnok gondolkodók"*, akikből saját korukban* meg nem értett előfutárok *lesznek. Majd 10 … 100 év múlva eljön a megértő és befogadó utókor, amelyben a társadalom csupán azért lehet oly megértő, mert az előfutárok látnoki gondolatait, az „új felfedezők" képesek az új kor számára olyan nyilvánvaló formába önteni, ami már azokat is meggyőzi, akik addig értetlenül álltak e gondolatok előtt.*
Eme igen mély törvény elvezet a titok relativitási elvéhez, *amely már nem az azt birtoklók számához köti a titok (rejtély) lényegét:*

Minden megfejtetlen titok rejtély, ám a megfejtése után rejTénnyé válik.

A TitokTan Trilógia második kötetétől [TDT 2004-k], [TDT 2005-k][11] már e különös szóösszetétellel fejezem ki, azt az egész emberiséget végigkísérő örök kettősséget (nevezhetjük nyugodtan titok*nak), amely a rejtélyek és tények, a rejtett tények, a megfejtésre váró ismeretlen és a már felhalmozott ismeretek között feszül. A kettősséget, amely mindenhova elkísér, melyet csak egy egyszerű, közönséges T köt össze, amely mégis oly erősen egybeolvadt, hogy egy fogalom, egy szó lett belőle: RejTények.*

Láthatjuk tehát, hogy a *titok*, a *titkosítás* évezrede óta (mióta emberi társadalom létezik), rejtélyes fátyolként kíséri az emberek életét, olykor többet, máskor kevesebbet takarva el belőle. A 20. század az emberi életek tömegét rejtő *titkok*, a világháborúk és hidegháború durva fátylai által betakart kódok évszázada volt. A titkosítás alkalmazása soha nem látott méreteket öltött, ami egyúttal igazi kihívást jelentett a rejtjelzés és természetesen a rejtjelfejtés művelőinek. A titkosítás, a kódolás és kódfejtés, azaz a kriptográfia és kriptológia a tudomány és művészet ötvözeteként ostromolták az emberi agy teljesítőképességének határait.

„Milyen siralmas látni, hogy a tudományokat alig lehet megkülönböztetni a fegyverektől."
Jan Amos Komensky (Comenius 1592-1670)

Ha a 20. század utolsó évtizedeire az *információrobbanás* volt jellemző, akkor a 21. század első évtizedét nevezhetjük az *„információs láncreakció"* évtizedének. Az egyének, a legkülönbözőbb társadalmi csoportok, szervezetek egyre több szálon kötődnek eme globális (idő és térbeli korlátokat átívelő) e-rendszerekhez. Így az emberiségnek abban a bizonyos 15-20%-nyi kisebbségében kialakult az információ-függőség, hasonlóan a civilizált társadalmakban már létező „elektromosság-függőséghez". Azonban, míg az elektromosság fizikai létünket határozza meg alapvetően, addig az információ teljes személyiségünk, pszichikai, egzisztenciális létünk „digitális leképezésére képes", amelynek birtoklása soha nem látott hatalomkoncentrációt eredményez.

Észre kell venni tehát, hogy a 21. századi információalapú társadalom kulcsfogalma az információbiztonság, azaz a személyes és globális titkok tömegének jó elkülönítése, tárolása, továbbítása. Az e-kommunikáció dominanciája egyre jobban kizárja a hagyományos értelemben vett tapasztalatokon nyugvó ellenőrzést, így a legkülönbözőbb mesterséges azonosító eszközöket vagyunk kénytelenek alkalmazni. A mesterséges azonosításhoz egyre több titkos kód, jelszó, kulcs megőrzésére, tárolására kényszerülünk, hiszen ezek mindegyike számunkra, vagy más közös érdekeltségű csoportok számára értékes információkat takar (hitelkártyák, SIM kártyák, igazolvány-kártyák, jelszavas és biometrikus azonosítók, stb.). A titkolódzás az e-kommunikációban általánossá válik, kilép a titkosszolgálatok szűk világából és mindennapjaink része lesz.

EZ A MEGVALÓSULT, IGAZI NAGY TESTVÉR!
Ez a megvalósult, egész emberiséget behálózó globális titok és titkosítás!
Ide jutottunk a ***mecsoti*** gyermekien titkos fantázia világától!

Szinte napra pontosan, az ezredfordulóval, sűrű sötét fátyolként takarta be az emberiséget a 2001. szeptember 11-i terrortámadás réme. Azóta a titokról, a globális e-kommunikációról, az e-világ biztonságáról alkotott „egyértelmű" képet kényszerül az emberiség „átfesteni". A

[11] A két kötet címe: *Klasszikus RejTények*, és *Újkori RejTények*. A szóösszetétel, illetve a mögötte meghúzódó fogalom újdonságát mutatja, hogy általában a könyv ismertetőkben elírásnak értelmezik és korrigálják a „helyes" kifejezésre: *rejtvények*.

történelem dupla felkiáltójellel hívta fel mindannyiunk figyelmét arra, hogy a jövendő információalapú társadalmak kulcsa a biztonság legyen!

Igazán megfontolásra érdemes tehát L. J. Hoffman, a George Washington Egyetem professzorának mély gondolata, a mély titok*ról [HOFFMAN 1995]:*
„Az NSA[12]-nál bíznak valamiben, amit ők úgy neveznek, hogy mély titok. Ők a legértékesebb mély titkaikat legszívesebben rejtjelezve betennék egy bontásvédett chipbe, ezt egy lezárt irodában lévő páncélszekrénybe, amely iroda fegyveresen védett szögesdróttal körülvett épületben van egy katonai bázison. Közlöm veletek, hogy ***a világ legértékesebb titka a demokrácia****. Ezt a titkot a műszakiak és a politikusok kéz a kézben kell, hogy megvédjék.* ***Ez az, amit mély titokként kell védeni.”***

[12] Az USA 1952-ben alapított Nemzetbiztonsági Szolgálata, NSA (National Security Agency) , amely ma a Föld legnagyobb számítástechnikai, és szellemi kapacitásait tömörítő rejtjelfejtő intézménye. Egyben az ECHELON kémműholdas rendszer, a megvalósult NAGY TESTVÉR szellemi központja.

2. Két gondolkodási modell: *„Találd meg!" – „Találd ki!" (rejtés és rejtjelzés)*

„Ha az emberi agy olyan egyszerű lenne, hogy megérthessük,
akkor túl egyszerűek lennénk ahhoz, hogy ezt megtehessük."
(Edgar Allan Poe 1809-1849)

Manapság közismert fordulat, ha úgy kezdődik egy fontos fogalmat tárgyaló dolgozat, előadás, hogy *„Már az ókoriak tudták …"*, vagy *„Ez a fogalom az emberrel egyidős …"*. Az ember hajlamos saját szerepét túlbecsülni a természet színpadán. Különösen igaz ez a TITOK, a TITKOSÍTÁS esetében, ahol az ***élő természet sok millió évvel megelőzött bennünket!*** Ennek az *előnynek* a megismerésén fáradozik néhány ezer éve a tudomány. Tudatosan nem a *hátrány* kifejezést használom, mivel az emberi megismerésnek *nem hátrány*, hogy a természet évmilliókon át kipróbált mintákkal szolgál a titkosítás területén.

Az *evolúció* a legátfogóbb olyan jelenség, amelyben alapvető szerepet játszik a környezethez való alkalmazkodás, a *rejtőzködés*. Például a mimikri a környezetbe való beolvadás csodálatos példáit mutatja.[13] Charles Darwin (1809-1882) evolúciós elméletében a „struggle for life", azaz a „küzdelem az életért" (a faj fennmaradásáért), nem játék, nem afféle elmeélesítő rejtvény, szórakozás, hanem maga az *élő valóság*! Eme küzdelem eredményeképpen alakult ki a ma létező élővilág, s benne egyetlen fajként az EMBER. Ezzel azonban a biológiai evolúció nem fejeződött be, a küzdelem folytatódik ma, holnap, holnapután! Sőt a tudományos megismerés eredményeként, ma már tudjuk, hogy az evolúció általános törvényei megjelennek a társadalom színpadán is. A társadalmi evolúció során azonban a változások idő skálája nem évmilliós léptékű, így a jelenségek egy-egy emberi generációban is érzékelhetők. Valahogy úgy, ahogy az anyaméhben 9 hónap alatt, mint valamiféle gyorsított film, játszódik le a teljes törzsfejlődés.

Az EMBER az egyetlen faj, amely sokszor a természettől ellesett *rejtési módszereket* nem csak a fajok közötti versenyben, az emberi faj fennmaradásáért folytatott élet-halál küzdelemre, hanem saját faján belüli érvényesülésére használja fel. A társadalmi egyenlőtlenségek, a profitorientált gazdasági verseny, a hatalom koncentráció számos példát szolgáltat erre, amelyek közül legmegrázóbb szinte folyamatos történelmi aktualitás a HÁBORÚ !
Az *emberiség* rossz tanulónak bizonyul az evolúció iskolájában! Nem csak az évmilliós tapasztalatokkal rendelkező bölcs tanítótól, a természettől nem tanulunk elég alaposan, de az Albert Einstein által kiállított bizonyítvány szerint, saját történelmünkből sem: *„A történelem mindössze arra tanít meg bennünket, hogy az emberiség semmit sem tanul a történelemből."*
(A.Einstein)

Az 1. fejezetben megállapítottuk a TITOK fogalmának relativitását, vagyis, hogy bármely információ *csak valamihez képest* (valamely vonatkoztatási, viszonyítási alapot képező információkhoz képest) lehet TITOK. A *természetes rejtőzködés csodája* éppen abban áll, hogy a TITOK beleolvad környezetébe. Ez akkor is igaz, ha változik a környezet!
Az *élet elrejtése* az állat és növényvilágban *élet-halál* kérdése. Az ehhez szükséges módszerek évmilliók alatt tökéletesedtek és váltak az *evolúció egyik kulcsává*.

[13] A TitokTan Trilógia első kötete 4. fejezetének címe: *„Természetes" titkolódzás*. Ebben a szerző számtalan példával illusztrálva járja körül a rejtés, rejtőzködés és az emberi titkosítás kapcsolatát.

A gondolkodás kialakulásával *az EMBER magára maradt az élővilágban*. A ***gondolkodás ugyanis magányos műfaj.*** A *gondolat* mindig *egyetlen ember „tulajdona”*, míg kommunikáció útján át nem adja azt másoknak. *A GONDOLAT tehát még Franklin szélsőséges definíciója szerint is TITOK.* Ezzel a titokkal azonban az ember általában egyedül nem tud mit kezdeni. Talán éppen ennek köszönhető, hogy kialakult az *emberi társadalom*! Erre mutat rá Hermann Imre előző fejezetben idézett gondolata a TITOK-ról: *„…A titok elszigetelő ereje. Amíg titkomat magamban őrzöm, magányos ember vagyok.”* Az ember számára tehát szó szerint, létkérdés a *kommunikáció* (hangutánzás, gesztusok, mimika, mozgás, beszéd, írás)!

Darwin szerint az érzelmek kifejezésének túlélési értékük volt! Azaz ha a másik viselkedését időben, jól értelmezzük, akkor van esélyünk arra, hogy felkészüljünk a jó reagálásra, vagyis jól alkalmazkodjunk a helyzethez (amely esetleg éppen az életünket veszélyezteti).

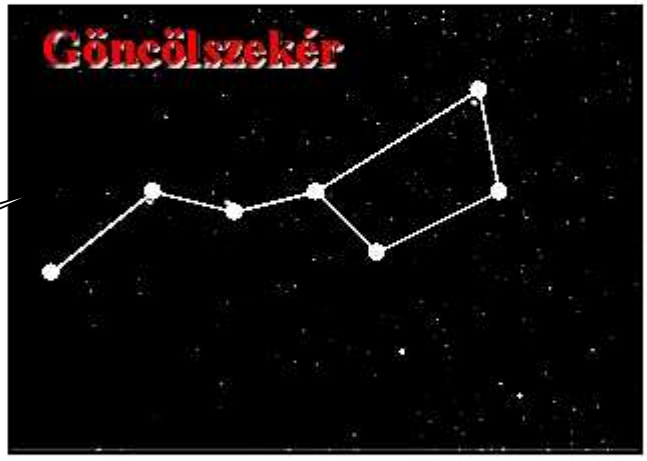
A *beszéd*, illetve a *beszédnyelvek* kialakulása a hatékonyabb kommunikációt segítette. Lényege, hogy egységes jelrendszerek alakultak ki. Az egymással kommunikáló emberek, azonos gondolati (fogalmi) egységekhez, azonos jeleket asszociáltak. *A nyelvi kommunikáció tehát lehetetlen a háttérben meghúzódó azonos fogalmi rendszer nélkül.*
Példaként képzeljük el, hogy el kell magyarázni valakinek, hogy mit jelent a *„csimbala”* szó. Ez csak akkor lehetséges, ha mindketten ismerjük a *„csimbala”* szó mögött rejtőzködő fogalmat. Ha ilyen közös fogalom nincs, akkor a megértés reménytelen még akkor is, ha egyébként mindketten azonos nyelvet beszélünk. Ugyanakkor könnyű a megfeleltetés például az angol *table* és a magyar *asztal* szó esetében, hiszen a szavak által jelképezett bútordarab mindkét nyelv fogalomrendszerében közismert.[14] Éppen ezért érdekes, de a tudomány számára is nehezen megválaszolható kérdés: Bár az emberiség egy fajhoz tartozik, *miért nem egy nyelvet beszélünk?*

A magyarázatot a rejtőzködő gondolat TITOK jellegében érhetjük tetten, melynek következtében a megismerés a titokfejtés jellegzetességeit mutatja. Illusztrációként átnyújtom a következő, bárki számára könnyen követhető gondolatkísérletet.
Földrajzi helytől és beszélt nyelvtől függetlenül, mindannyiunknak kedves emlék, amikor felnézünk az égre és a tiszta éjszakai égbolton fényes pontokként látjuk a csillagok óriási halmazát. Hogy mégis valamiféle „rendet teremtsünk”, különböző csillagképeket „látunk bele” a sok-sok különböző fényességű pontba, ami egészen addig TITOK, amíg másokkal meg nem osztjuk. Így válnak a csillagképek egy adott csoport, vagy akár az egész emberiség közös fogalmává, ami már nem titok, mivel ettől kezdve bárki felnéz a csillagos égboltra, a Göncölszekér „ott található”.
Pedig *nincs Göncölszekér* a világegyetemben, de még a látható égbolton sem! A csillagképeket az emberek alkotják, éppen azért, mert így strukturálni tudják az egyébként áttekinthetetlen csillaghalmazt! A 2.1.a. ábra azt a Nagy Medve csillaghalmazt mutatja, amelynek hét legfényesebb csillagához az emberi képzelet hozzárendelte a Göncölszekér képét (lásd 2.1.b. ábra). De ugyanazokhoz a fényesebb csillagokhoz az én képzeletem a 2.1.c. ábra *„küllő csillagképét”* asszociálta, így most ezt megosztom Önnel kedves Olvasó és ha egyszer személyesen találkozunk, számunkra a *„küllő csillagkép”* már nem lesz afféle értelmetlen *csimbala*.

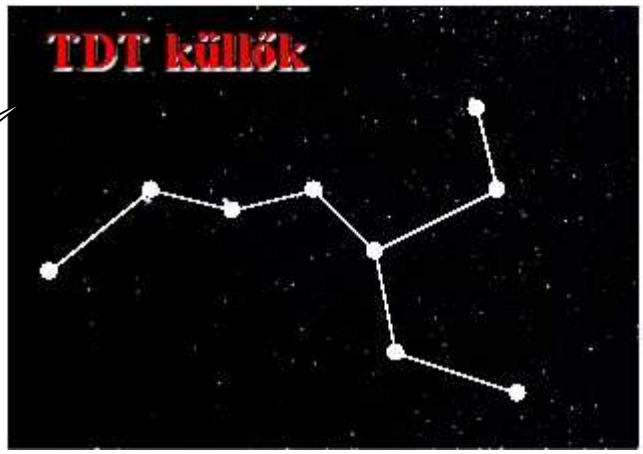
[14] Íme Comenius (1592–1670) cseh író és pedagógus bölcs vélekedése a nyelvekről: *„... a nyelvek bölcsességet nem nyújtanak, hanem csak arra valók, hogy szót érthessünk a földkerekség más-más lakóival, élőkkel vagy holtakkal.”*

Hasonlóan jártam el, amikor a Hubble űrteleszkóppal készített Omega Centauri csillaghalmazban, csupán a fényesség alapján kiszíneztem a fénylő pontokat és a legfényesebbekből alkotott alakzatot *„piramis csillagkép”*-nek neveztem el (lásd a 2.2.a.-d. ábrákat).

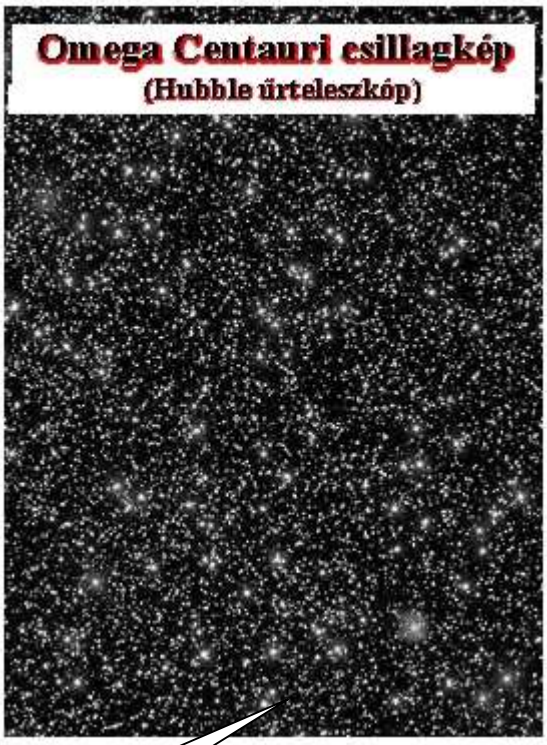
2.1.a. ábra



2.1.b. ábra



2.1.c. ábra

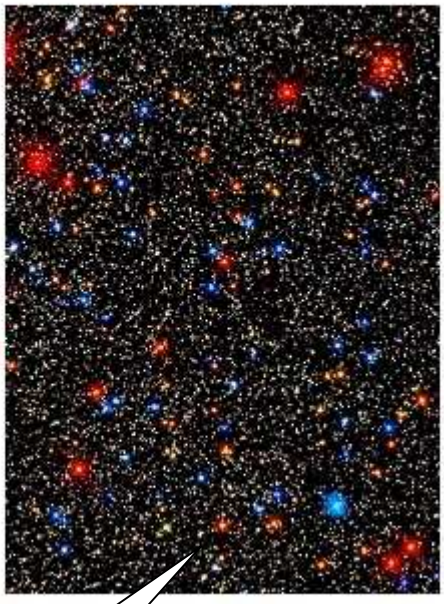


2.2.a. ábra

sűrítés

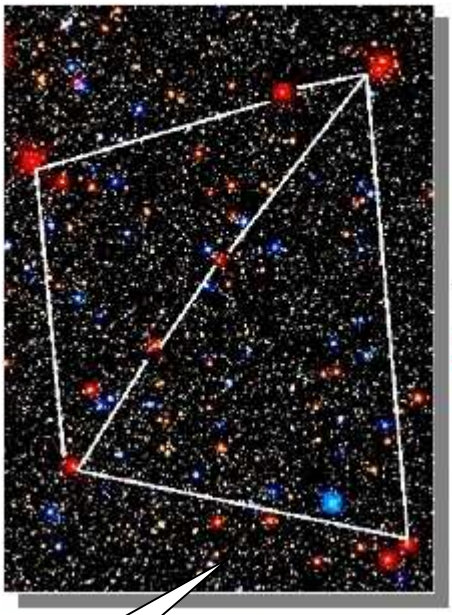
2.2.b. ábra

színezés



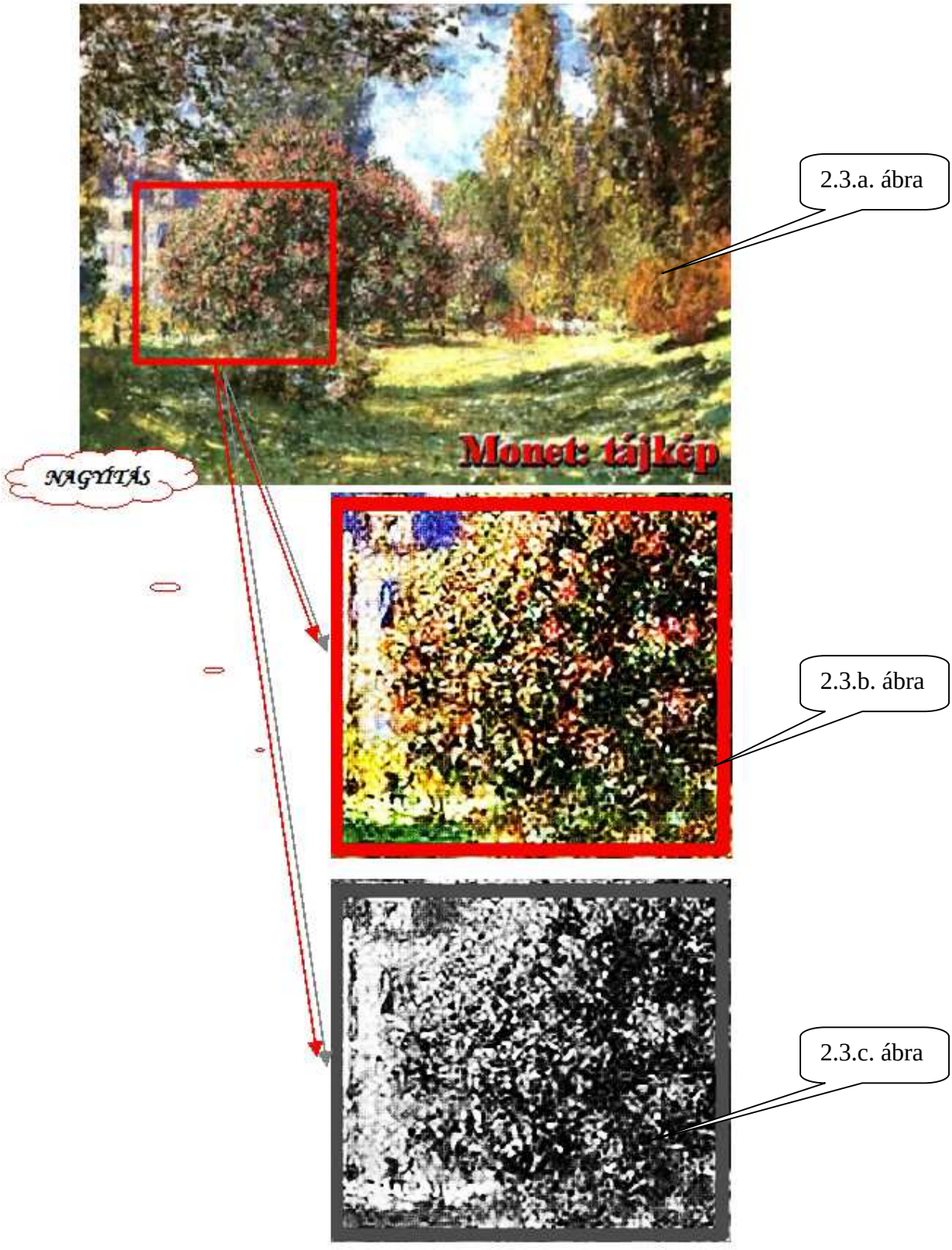
2.2.c. ábra

TDT piramis



2.2.d. ábra

A kutatók a tudomány nyomozói, a csillagászok hatalmas távcsövekkel igyekeznek minél közelebb kerülni a csillagokhoz, és igyekeznek megfejteni a *titkot*, akárcsak *kódtörő* a valóságból érkező temérdek információban keresi a *rendet*. Ez a kutatás, a megismerés rendje, amit a valóság, de sokszor maga az ember rejtett el.



Ezért mutattam be a saját *„piramis és küllő csillagképemet”*, mivel mindkettő ugyanolyan *„valóság”*, mint a *Göncölszekér*. Ezzel igyekeztem szemléltetni a megismerés, azaz a valóság

leképezésének szubjektív fázisát, a vonatkoztatási szempontok meghatározását. Így már nem nehéz észrevenni, hogy ez a folyamat pontosan az ellentettje a TITOK elrejtésének, amely különös módon kapcsolja össze a tudományt és művészetet. Ugyanis pontosan ez a fordított eljárás történt, amikor például Monet a 2.3.a. ábrán látható tájképének impresszióját kis színfoltokká képezte le, amelyek csak megfelelő távolságból nézve állnak össze alakzatokká („csillagképpé”, vagy éppen festménnyé)! A 2.3.b.-c. ábrákon igyekeztem szemléltetni, hogy a „nagyítás” és színezés folyamata éppen az Omega Centauri, vagy a Nagy Medve csillaghalmazokhoz hasonló ponthalmazhoz vezet, amelyben az emberi agy nem találja az eredendően benne foglalt rendet.

Mindez pontosan megfelel annak, ahogy a beszédnyelvben a betű és hangképeknek szavakat feleltetünk meg, amelyekhez teljesen szubjektíven társítunk „jelentést”, ami attól kezdve egy közösségben azonos asszociációval bír, így jön létre egy közösség kultúrája, például a beszédnyelve. A nyelvtani szabályoknak tehát nem az a lényege, hogy „csak úgy lehet beszélni, vagy írni, ahogy azt a szabályok diktálják”, hanem az, hogy az adott közösség számára egységes struktúrát teremtsen, ahogy a közlekedésben a KRESZ.

Richard Dawkins az 1970-es években a gén mintájára, bevezette a *mém = emlékmás* fogalmát. A biológiai örökítő anyag általánosítása (vagy éppen rivális fogalma) a kulturális átadás, a gondolati örökítés! Amely éppen a környezetébe maximálisan beépülve válik hosszú távon megőrizhetővé! *Az éntudat állandó, miközben 7 évente az összes sejtünk kicserélődik!* R.Dawkins szerint: *„Az ember halálakor két dolgot hagyhat maga után: géneket és mémeket.”*
DE amíg *leszármazottaink csupán 2-3 generáció távolában emlékeztetnek arcvonásaikban, hajuk színében, külső jegyeikben ránk,* addig *az emlékmásolatok, a mimika, a gesztusok, a viselkedés, de legfőképpen a gondolatok lényege sok-sok generáción át fennmaradhat!* Akkor is, amikor génjeink már régen feloldódnak az emberiség közös génkészletében.
Lehet, hogy Beethoven, Mozart, Darwin, vagy Einstein egy-két génje még létezik a világban, de *mémjeik szervesen beépültek kultúránkba!* Akárcsak Monet tájképe, vagy a Nagy Medve csillagkép részleteként a Göncölszekér, vagy éppen az Omega Centauriban a jelen szerző által „felfedezett” piramis csillagkép.

Az eddigiekből kiderül, hogy a TITKOK elrejtése, a rejtőzködés a természet, így az emberi gondolkodás ősi modellje, amelynek megfejtéséhez a megismerés *„Találd meg!”* módszercsaládja vezet. *Találd meg!* az óriási Nagy Medve csillaghalmazban a Göncölszekeret, az Omega Centauriban a piramis csillagképet, vagy Monet színes festékfoltjainak kavalkádjában a tájképet.

Az EMBER azonban a természet eme évmilliós ősi bölcsességével nem érte be. A beszédnyelvek fejlődésével kétkomponensűvé lett a kommunikáció:

- dominánssá vált a konkrét (célzott) üzenetet közvetítő funkciója,
- és másodlagos jellegűvé vált a metakommunikáció[15]

Tovább erősödött ez a tendencia az írás kialakulása során:

- *Képírás* (egész történeteket jelenít meg képi formában) *alig tömörít*, majdnem olyan, mint a beszéd

[15] Már elnevezésében is arra utal, hogy *„kommunikáción túlinak”* minősül.

- *Ideografikus (fogalom) írás***,** igyekszik a háttérben működő *egységes fogalom rendszert megragadni*
- *Szótagírás, kezd elválni a jel és annak jelentése*
- *Betűírás, teljesen elválik a jel és jelentése*. Tulajdonképpen visszajutottunk egy nagyon jól strukturált ősi állapothoz, a „hangutánzáshoz”, csak nem hanggal történik *az utánzás, hanem a hangoknak írásjeleket feleltetünk meg*, azaz KÓDOLUNK !

Az írásnál használt ABC tehát fogalomsűrítés és absztrakció útján kialakult jelkészlet. Használata nagyon kényelmes, gyorsan tanulható és rendkívül variábilis. A *titkosírások* tulajdonképpen ezt a variabilitást használják fel. Vagyis a szokásoshoz képest, *megváltoztatják a kódolási eljárást*!
Mindebből világosan kiderül, hogy a *titkosítás* nem azonos a *titkosírással*, bár a különbség mindössze egyetlen betű! E két szó a közgondolkodásban szinte meg sem különböztethetően összeolvadt[16], pedig a titkosírás csak a titkosítás egy nagyon speciális ága, ahogy maga az írás is a kommunikációnak.

A titkosírással tehát nem elrejtjük, hanem rejtjelezzük, vagyis egy másik jelrendszerbe átkódoljuk a TITKOT. Ekkor nem megtalálni kell a környezetében rejtőzködő titkot, hanem ki kell találni a kódolási (rejtjelzési) eljárást. Ezért nevezzük a rejtjelzett titok megfejtését *„Találd ki!”* gondolkodási modellnek.

E kötet további fejezeteiben megmutatjuk, hogy a két gondolkodási modell, egymást kiegészítve képezi a BIT, vagyis a Biztonságos Információalapú Társadalom alapját. A 21. századi digitalizáció mindkét módszercsaládnak új perspektívákat nyit, amelyeket jól alkalmazva már nem utópia az INFOSANCE kor, hanem *a jelen század reménye*.

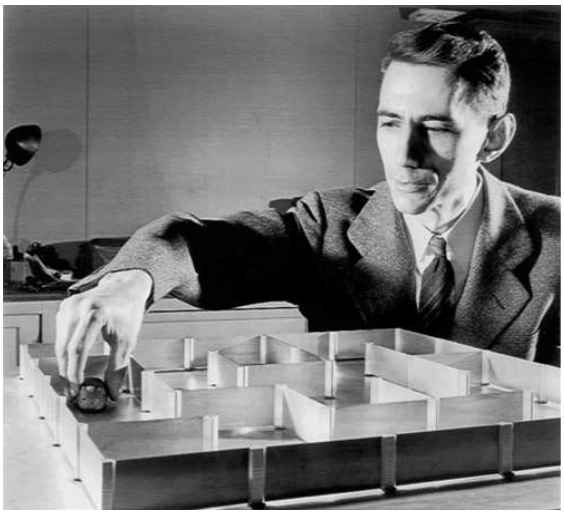
[16] 2003-ban előadást tartottam Marosvásárhelyen a Sapientia Erdélyi Magyar Tudományegyetemen. Előzetesen elküldtem előadásom címét: *Rejtés vagy rejtjelzés? (A titkosítás régi-új útjai)*, amely az egyetemi plakátokon így jelent meg: *Rejtés vagy rejtjelzés? (A titkosí**r**ás régi-új útjai)*

3. Az *információbiztonság titka* a *redundancia*

„Mindig elcsodálkoztam azon, hogy hogyan álltak össze a világ dolgai."
(C.E.Shannon 1916-2001)

3.1. C.E. Shannon[17] a modern információelmélet atyja

Vékony, egyszerű (60 kg és 178 cm), mégis különös ember volt, aki szerette a scifi-t, a jazzt, a sakkot, a matematikát, a bűvészkedést és más különös dolgokat, de leginkább szerette a változatosságot. Már életében legendává váltak különleges hobbyjai. Egy alkalommal a Bell Laboratórium halljában kifeszített kötélen járt fel-alá egykerekű kerékpárján, munkatársai legnagyobb megdöbbenésére. Ugyanitt konstruálta meg (egészen fiatalon) az első elektromechanikus „tanuló egeret", amelyik biztonságosan talált ki a legkülönbözőbb kísérleti labirintusokból. C.E.Shannon *Theseus[18] nevű elektromechanikus egere volt (1940-es években) az egyik legelső „tanuló gép"*.



C.E. Shannon és Theseus nevű elektromechanikus „tanuló" egere

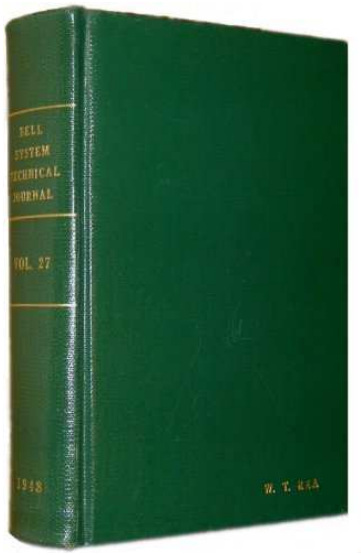
Figyelemre méltó volt sakkozó-gépe is, amely az 1940-es években nagy lépést jelentett a computer-építéshez vezető úton. Berendezését akkor sikerrel alkalmazták harcászati helyzetek kiértékeléséhez és az optimális stratégia kiválasztásához[19]. Shannon disszertációjában[20] a

[17] C.E.Shannon, akit az információelmélet "atyjának" is neveznek, 1916. április 30-án született a Michigan állambeli Petoskey-ben. 1936-ban a michigani egyetemen szerzett matematikus és elektromérnök diplomát, majd az MIT-n (Massachusetts Institute of Technology) szerzett doktori fokozatot. 1941-től több, mint 30 éven át a Bell Laboratórium matematikai osztályának vezetője, közben az MIT vendégprofesszora volt.

[18] Az „okos" egér elnevezése nem véletlen. Theseus ugyanis görög mondai hős volt, aki behatolt Minotaurus (félbika-félember) lakóhelyéül szolgáló útvesztőbe (labirintusba), hogy kegyetlenkedéseiért megölje őt. Theseus legyőzte a szörnyet, ám a labirintusból csak segítséggel tudott kijönni. A segítséget az a fonal jelentette, melyet a krétai király lányától, Ariadnétól kapott, s amely fonalat a labirintusba vezető útján maga mögé eregetett, így visszafelé csak ezt kellett követnie, hogy el ne tévedjen a labirintusban.

[19] Ebben az időben (az 1940-es évek első fele), a II.világháború vérzivataros éveiben természetesen a hadiipar, a hadászat jelentette a kutatás számára a legnagyobb kihivást. Tulajdonképpen az első elektronikus számítógép (az ENIAC) megépitése is ennek „köszönhető".

Bool-algebrára építve *megalapozta a digitális hálózatok elméletét*. Ennek napjainkig ható jelentőségét adja, hogy a digitális hálózatok képezik a modern számítógépes és telekommunikációs rendszerek alapját. Ő maga így emlékezett eme II.világháborús évekre:
„A Bell Laboratórium titkos rendszereken dolgozott. Én a kommunikációs rendszerekkel és a kriptológia[21] tanulmányozásával foglalkoztam. Gondolkozásomban annyira összeolvadt a kettő, hogy sokszor az egyik terület problémáján gondolkodva jutott eszembe az a megoldás, amit a másik területen lehetett alkalmazni. Egy idő után képtelen voltam elkülöníteni a két kutatási területet."



A Bell System Technical Journal 1948-as kötete, C.E. Shannon korszakos cikkével, amelyben lerakta az információelmélet matematikai alapjait

Így született meg 1948-49-ben két alapvető cikke a Bell System Technical Journal-ban, amelyekben elsőként sűrítette matematikai formába a kommunikációs rendszerekkel és ezek biztonságával kapcsolatos elméletét:

1. *A Mathematical Theory of Communication* [SHANNON 1948]
2. *Communication Theory of Secrecy Systems* [SHANNON 1949]

Az 1. cikket tekinthetjük a modern *információelmélet születésének*, míg a 2. cikk a kriptológia információelméleti megalapozása, amelynek szintén nagy jelentősége volt. Mégis Shannon alapvetően új gondolatai között vezető helyet foglal el a *redundancia* fogalmának bevezetése. Ez képezi ugyanis az alapját, a napjaink kommunikációs és számítástechnikai rendszereiben is *kulcsfontosságú kódolásnak*, különös tekintettel a hibajelző és hibajavító kódokra. A redundancia ugyanis a nyelvek, így a kommunikáció fontos jellemzője, amely lehetővé teszi a nyelvi „rejtőzködést", a TITOK elrejtését, illetve kódolását, ugyanakkor biztonságot is nyújt bizonyos szándékos, vagy akár véletlen torzítások felismerésénél. A redundancia tehát a *Találd meg!* és *Találd ki!* titkosítási modellek esetén is alapvető jelentőségű.

3.2. Redundancia az információelméletben

Shannon minden információval kapcsolatos fogalmat (jelenséget) számszerűsített, hogy azután a matematika eszközeivel egzakt tételeket, összefüggéseket fogalmazhasson meg. Így egy üzenet információmennyiségét (nem ismeret mennyiségét!), az üzenet váratlanságával jellemzi, amely tulajdonképpen egy valószínűségi típusú érték. Jellemzésére a kinetikus gázelmélet modell-analógiából származó *„entrópia"* fogalmat vezette be, melynek lényege a következő:

---

[20] Disszertációjának cime: *A Symbolic Analysis of Relay and Switching Circuits*
[21] A kriptológia a rejtjelekkel és rejtjelfejtéssel foglalkozó tudomány.

Adva van egy hírforrás, melyről a szimbólumok (más szóval: egy ABC betűi) előfordulási gyakoriságán kívül (ez végtelen hosszú, vagy végtelen sok üzenet esetén megfelel a szimbólumok valószínűségének) nem tudunk semmit. Ha minden szimbólumot két jelből álló jelsorozattal (0-1 bináris sorozat) akarunk leírni, akkor egy-egy szimbólum leírásához átlagosan milyen hosszú bináris sorozatra van szükségünk?

Shannon az alábbi, általa *entrópiának* nevezett matematikai összefüggést vezette le (*jelölése: H, p_i* az *i*-ik szimbólum előfordulási valószínűségét jelöli):

(3.2.1) $$H = -\sum_{i=1}^{n} p_i \cdot \log_2 p_i \quad \text{bit/szimbólum}$$

Mivel $\log_2 p_i$ mindig negatív érték, így az összegzés pozitív H értéket ad.

Az entrópia modell-analógia fontos tulajdonsága, hogy ahogy a fizikában csak zárt rendszerekre alkalmazható, úgy az információelméletben úgynevezett *teljes eseményrendszerekre érvényes*, amelyekben *n*-féle szimbólum, vagyis *n* elemű ABC esetén teljesül, hogy

(3.2.2) $$\sum_{i=1}^{n} p_i = 1$$

Ez szemléletesen azt jelenti, hogy minden esemény (üzenet) a megadott szimbólumokkal (az ABC betűivel) leírható. Hasonlóan ahhoz, ahogy például a Nagy Medve csillagrendszer csillagaiból képeztük a Göncölszekér, vagy éppen a TDT küllő csillagképeket.

Az entrópia és redundancia könnyebb értelmezhetősége érdekében tekintsük a „fej vagy írás” játékot. Első megközelítésben legyen teljesen szabályos a pénzérme, amellyel játszunk, így az F fej és I írás dobásának valószínűsége egyforma, azaz ½. Ekkor a H_{szab} entrópia így alakul:

(3.2.3) $$H_{szab} = -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1$$

Azaz 1 bittel leírható (0-1, igen-nem, fej-írás, stb.) minden dobásnál a keletkező esemény (üzenet) és mivel az események egyenlő valószínűségűek, így az információk váratlansága (bizonytalansága) a dobások során nem változik. Tehát erre az 1 bitnyi információra feltétlenül szükség is van, ha a dobás eredményét közölni akarjuk.

Most vizsgáljuk a „cinkelt” pénzérme esetét, ahol például az F fej dobásának valószínűsége ¾ , így az I írás valószínűsége ¼ . Ekkor a H_{cink} entrópia így alakul:

(3.2.4) $$H_{cink} = -\left(\frac{3}{4}\log_2\frac{3}{4} + \frac{1}{4}\log_2\frac{1}{4}\right) = 0.689$$

Azaz alig több, mint kétharmad bit elegendő lenne az így cinkelt pénzérmével való dobások eredményének közlésére, hiszen az események váratlansága (bizonytalansága) ebben az esetben nem olyan „meglepő” (a dobások többségénél ugyanis várható, hogy az F fej lesz az eredmény).
Általában az információelméleti entrópia akkor maximális, ha az alap ABC minden betűjének p_i előfordulási valószínűsége egyenlő (ez a valószínűség n betűs ABC esetén, éppen $\frac{1}{n}$), ekkor vagyunk ugyanis a legbizonytalanabbak abban, hogy milyen információ fog az üzenetben érkezni, míg ha az entrópia csökken, akkor bizonyos információkat nagyobb

valószínűséggel várhatunk, mint másokat. Az entrópia csak akkor nulla, ha egy kivételével minden p_i nulla, ami azt jelenti, hogy az üzeneteknek nincs „hír értéke”, hiszen mindig ugyabból a szimbólumból (betűből) álló jelsorozat (üzenet) érkezik, amelynek a valószínűsége így pontosan *1*, azaz minden üzenet előre tudható, biztos esemény. *Az információelméleti redundancia (jele: R)* definíciója:

(3.2.5) $$R=1-\frac{H}{H_{\max}}$$

azaz a relatív entrópiát *1*-ből levonjuk, ami *megadja, hogy az üzenetben szereplő jelsorozat hányadrésze hagyható el anélkül, hogy az az „érthetőséget” csökkentené.*

Fel kell hívni a figyelmet arra, hogy ebben az értelmezésben az „érthetőség”*-et információelméleti megközelítésben úgy kell érteni, hogy* „az üzenetet képező jelsorozat annak tartalmától függetlenül, szintaktikusan, azaz a nyelv formai szabályainak megfelelően beazonosítható”.

Az így értelmezett redundancia szerint (hosszú szövegeken végzett számítások alapján) az emberi nyelvek redundanciája átlagosan 50%, ami azt jelenti, hogy ha valamely üzenet betűinek körülbelül a felét elhagyjuk (természetesen véletlenszerűen kiválasztva a betűket), akkor a fenti értelemben, érthetetlenné válik a szöveg. Az előzőkben bemutatott pénzérmés példáinknál például a következő eredményre jutunk a redundancia kiszámításával.

A szabályos pénzérménél: $R_{szab}=1-\frac{H_{szab}}{H_{\max}}=1-\frac{1}{1}=0$

A cinkelt pénzérménél: $R_{cink}=1-\frac{H_{cink}}{H_{\max}}=1-\frac{0.689}{1}=0.311$

Tehát míg a szabályos érmével történő dobások esetén 0 redundancia mellett, minden információra szükségünk van, hogy az üzenetet „megértsük”, azaz egyértelműen tudjuk azonosítani (az üzenet itt a dobás eredménye), addig a cinkelt érme esetén, több mint 30% redundancia mellett, a bejövő információk majdnem egyharmada elhagyható.
Jó példa a tudatos információ sűrítésre a gyorsírás, ahol éppen a nyelvi redundancia minimálisra csökkentése a technika lényege. Ugyanakkor lényeges momentuma ennek az eljárásnak, hogy a gyorsírással rögzített szöveget, mihamarabb „gépbe írják”, mivel egy idő után az egyedi jelölések asszociációs tartalma már nem rekonstruálható.

Példaként álljon itt egy olyan mondat, amelyből először a betűk 21%-át, majd 39%-át hagytuk el, mégis mindkét esetben a szöveget több-kevesebb gondolkodás után el tudjuk olvasni és meg is értjük annak üzenetét (a mondatközi vonalkák a hiányzó betűket jelölik):
É-dekes -i-met -uta-tak be az e-mu-t -ap-kb-n. (21%-os tömörítés)
É-dek-s -i-m-t -út—t-k be -z e-mu-t -ap-kb-n. (39%-os tömörítés)

Mindennapjaink részévé váltak a képi információsűrítés szimbólumai, a piktogrammok, valamint játékos formában a szöveg és képsűrítés keverékei a képrejtvények. Digitális világunkban mindennaposak a tömörített kép, hang és videó file formátumok (jpg, mp3, mp4, …), amelyeket a legkülönbözőbb e-kommunikációs eszközökön továbbítunk és tárolunk.
A redundancia csökkentésével tehát rövidíthetjük az üzenetek átlagos hosszát, de kérdés, hogy mit tudunk kezdeni az így „optimalizált” üzenettel? A válasz meglepő!

A mesterséges (digitális) kommunikációs rendszerek szempontjából valódi előny, hogy a rövidebb üzenet gyorsabban átvihető és kisebb helyen tárolható. A kommunikáló felek

azonban teljesen védtelenné válnak mindenféle véletlen, illetve szándékos hibával, torzítással szemben.
Nulla redundanciára érzékletes példa a LOTTÓ húzás, ahol nem lehet közelítőleg eltalálni a főnyereményhez tartozó számokat, ellenben a beszédnyelvben megadhatunk egy szót közelítőleg, azaz hibásan, akkor is felismerjük (pl.: ha „borotva”, helyett a „barotva” jelsorozat érkezik). Fel kell hívni a figyelmet a beszédnyelv kihangsúlyozására, mivel ugyanez például a számítástechnikában alkalmazott programozási nyelvekre nem igaz. Ott az utasítások, formulák úgynevezett szintaxisát pontosan be kell tartani ahhoz, hogy a gép „megértse”.

Fontos, hogy az előzőkben vázolt információátviteli tulajdonságok, csupán a kommunikációnak a hírközlő csatornán (ez lehet írott, hang, kép átvitelére alkalmas technikai eszköz) átvitt, üzenet részére vonatkoznak.

Amint láttuk, az információelméleti redundancia csökkentése lerövidíti az üzenetet, de véletlen, vagy éppen szándékos hibák esetén megnehezíti, esetleg lehetetlenné teszi az üzenet megértését (azonosítását). Ennek kiküszöbölésére a $\frac{bit}{szimbólum}$ arány megnövelésével (kódhosszúság megnövelésével), úgynevezett *hibajelző (error detecting), illetve hibajavító (error correcting) kódok képezhetők*.

Neumann János (1903-1957) már az 1950-es években felvetette az önjavító, önreprodukáló gépek kérdését (lásd [NEUMANN 1972]), amelyre elméleti úton pozitív választ adott. Az információelméletnek ma már külön ága a hibajelző és hibajavító kódok elmélete, amely matematikai leírást ad olyan kódok létezésére és készítésére, amelyek megfelelő redundancia mellett, az üzenetben keletkező, meghatározott mennyiségű hibás jel kiszűrésére, illetve kijavítására alkalmasak. Enélkül a mai e-kommunikációs eszközök és hálózatok folyamatos, biztonságos működése elképzelhetetlen lenne.

PÉLDA
Anélkül, hogy részletesen kifejteném az elméleti hátteret, szemléltetésként bemutatok egy példát, *1* hibát jelző kódra. Legyen egy egyszerű ABC, amely mindössze négy betűből áll *(B,T,I,O)* és legyenek e betűk bináris kódjai a következők:

B = 100
T = 010
I = 001
O = 111

3.2.1. ábra

Ha üzenetünk például a *BIT* szó, akkor az átviteli csatornán az *100001010* bináris jelsorozatot küldjük el. Azonban, ha az átvitel során véletlen, vagy szándékos hiba keletkezik és a fogadó oldalon például a *000001010* jelsorozat érkezik meg, akkor a dekódolt üzenet a következő lesz: *000 I T*, amelyből rögtön kiderül, hogy az első karakter hibás.

Ugyanis az összes lehetséges három bitből álló kódok (számuk: $2^3=8$) a következők:

100	*011*
010	*101*
001	*110*
111	*000*

3.2.2. ábra

így e táblázatból világos, hogy az első oszlopban levő bármelyik kód egy bitjének megváltoztatásával, rögtön átkerül a második oszlopba, azaz a két oszlopban leírt kódok éppen kiegészítik egymást (komplementer viszonyban vannak!). Azonban két bit eltérést (pl.: *100* helyett *010*) nem képes ez a kód jelezni, hiszen ekkor csupán egy értelmes betű (*B*) helyett egy másik értelmes betűt (*T*) kapunk (azaz az azonos oszlopba tartozó kódok kicserélődése történik).

Pontosan ezt a tulajdonságot használják ki a rejtjelzésben alkalmazott „helyettesítéses" eljárások, melyeknek az a lényege, hogy az úgynevezett „nyílt üzenet" alap ABC-jének betűihez egyértelműen hozzárendelik az alap ABC, vagy egy másik ABC betűit. Az így keletkező üzenet természetesen az illetéktelen olvasó számára értelmetlen jelsorozat (szöveg), azaz titok.[22]
Ez a titok azonban ránézésre, alig-alig különbözik a véletlen hibák által létrehozott „zaj"-tól, amely az információs csatornák, mondhatni természetes velejárója. A *Találd ki!* rejtjelzési filozófiának, azaz a rejtjelzésnek pontosan az a célja, hogy a rejtjelzett üzenet minél inkább hasonlítson egy nagy entrópiájú, azaz véletlen jelsorozathoz.
Ennél jóval bonyolultabb a helyzet, ha a betű eltérés, egy értelmes szó helyett, egy ugyanolyan hosszúságú másik értelmes szót eredményez (pl.: *BIT* helyett *BOT*), azaz amikor a *Találd meg!* titkosítási filozófiát követjük.

Témánk szempontjából igen lényeges eme két probléma-típus felismerése, melynek lényege, hogy információelméleti eszközökkel az „értelmes", „érthető" fogalmak csak formálisan értelmezhetők, így a mesterséges kommunikációs rendszerről fel kell tételeznünk, hogy bizonyos mennyiségű „formális értelmetlenséget" produkál, ezáltal megkülönböztethető a természetes intelligenciával rendelkező, „értelmes" rendszerektől. Pontosan erre épül a következő fejezetekben bemutatásra kerülő Turing-teszt, amely szerint a nagyon jól utánzó gép, megkülönböztethetetlen a természetes intelligenciától.

3.3. Redundancia a kommunikációban

„Amióta információelmélettel foglalkozom, sokszor eltűnődtem azon,
hogy fér el néhány verssorban összehasonlíthatatlanul több információ,
mint egy ugyanolyan hosszúságú, maximális tömörségű táviratban."
(Rényi Alfréd 1921-1970, Ars matematica)

C.E. Shannon az információelméletet megalapozó [SHANNON 1948] cikkének első oldalán (a második bekezdésben) rögzítette, hogy nem akar foglalkozni az információ jelentéstartalmával:

[22] A *helyettesítéses titkosításokat* részletesen tárgyalja a Kódtörő ABC [TDT 2002-k].

„Az üzeneteknek gyakran jelentésük van; ez azt jelenti, hogy valamely – bizonyos fizikai vagy fogalmi dolgokkal jellemzett – rendszerre vonatkoznak, illetőleg aszerint korreláltak. A hírközlés elméletének e szemantikai vonatkozásai közömbösek a műszaki probléma szempontjából. A lényegi kérdés az, hogy a tényleges üzenet, egy sor lehetséges közül kiválasztott egyetlen üzenet."

Az információelmélet korlátai, azaz, hogy a kommunikáció nem csupán az üzenet, mint információ átvitelét szolgálja, hanem az üzenet által asszociált ismeret (jelentéstartalom) eljuttatását a fogadóhoz, a fenti mottó szerint a magyar matematika és információelmélet jelentős gondolkodóját, Rényi Alfrédot is foglalkoztatta.

A 20.század középső évtizedeiben alkalmazott információátviteli technikák mellett azonban eme gondolatokat háttérbe szorították, az akkor éppen csecsemő korban levő információelmélet meghökkentő lehetőségei, amelyek a híradás és számítástechnikában nyertek alkalmazást. Az információelmélet, majd a kódoláselmélet eredményei adtak alapot az információ tárolás és átvitel egy egészen új korszakának, a digitális technikának, amely lehetővé tette az *„információs bumm"* (információ robbanás) kialakulását. A 20.század utolsó harmada az információ tömegtermelésének kora, amely mint minden tömegjelenség, kezdte a „méregfogait" is kimutatni.
Az eltárolt temérdek információ dzsungelében egyre nehezebb lett az eligazodás (ahogy például a hatalmas csillag rendszerekben), így szükségessé vált az optimalizálás, amely a kor szellemének és az elméleti, valamint technikai háttérnek megfelelően, a mennyiségi paraméterekre vonatkozott. Hogy lehet az információt minél kisebb helyre tömöríteni, ezáltal minél gyorsabban átjuttatni az információs csatornán és végül minél kisebb helyen tárolni ?
A hardver eszközök térfogategységre jutó kapacitása exponenciálisan nőtt, azaz egyre nagyobb mennyiségű információt képesek tárolni, egyre kisebb helyen (lásd a ma már közforgalomban kapható laptop (táska), palmtop (marok) számítógépeket, sőt az úgynevezett okostelefonokat), míg ugyanez a növekedés a „gépek" architektúrájában és a felhasználó szempontjából létfontosságú gép és ember közötti kommunikációt szolgáló szoftverben egyáltalán nem jött létre. A napjainkban tömegesen alkalmazott asztali, laptop, palmtop számítógépek alapvető hardver architektúrája még mindig megegyezik a Neumann János által leírtakkal, sőt tulajdonképpen C.Babbage (1792-1871) 19. századi elképzeléseivel (lásd [TDT 2003-k]). Így a jelen globális kommunikációs rendszereiben, a felhasználó teljesen magára maradt, szuper teljesítményű, de „intelligenciáját" tekintve 19. századi digitális eszközeivel.

Napjainkra előállt tehát az a paradox helyzet, hogy a redundancia egyszerre vált „ellenséggé" és mint a fentiekben rávilágítottunk, az információbiztonságot támogató eszközzé. A racionális törekvések, a gazdasági, üzleti szempontok diktálta fogyasztói társadalomban mégis az előbbi irányba húztak, sőt a digitális technika térhódításával egyre erőteljesebb a redundancia „ellenség-képe".

A digitális technikával, ami napjaink és várhatóan a közeljövő uralkodó technikája, óriási számhalmazokká képezzük le egész környezetünket, az e-kommunikációban még gondolatainkat is, így valójában egy digitális világot építünk fel, amely bizonyos értelemben újraéleszti az ókori számmisztikát.
Püthagorasz és követői a püthagoreusok (i.e. 6.-5. század) alapvető világszemlélete volt, hogy *„A dolgok természete, lényege: a szám."*, de még a XIX. század végén Leopold Kronecker (1823-1891) is így vélekedett: *„Az egész számokat az Isten alkotta, minden más az embertől származik."*

A számmisztika legérdekesebb és talán legemberibb megnyilvánulása volt, mikor nem a számokat személyesítették meg, hanem a személyes (emberi) tulajdonságokat „számosították meg”, mint például a barátságos, vagy a tökéletes számok esetében, melyeknek titka a mai napig rejtve maradt, még a legnagyobb matematikusok előtt is. A számmisztika tehát a számok titokzatos, rejtett tulajdonságait tárta fel, ílymódon igazolva azt a szemléletét, hogy az emberi változatosság a számok tulajdonságaiban tetten érhető.

A digitális világ, azaz *napjaink számmisztikája* ettől lényegesen különbözik, mivel a digitalizált információ számdömpingjében éppen a számok „számtulajdonságait” hántjuk le és egyszerű „számkódok”-ként használjuk fel őket. A digitális számhalmazok így tulajdonképpen jelhalmazokká, kódhalmazokká válnak, amelyek semmiben sem különböznek a nem numerikus szimbólumoktól, ABC-ktől.
Illusztrációként figyeljük meg a *„123 darab könyv”* nyelvi üzenet esetét, amelynek ebben a formában majdnem egyértelmű jelentést tulajdonítanak a magyar nyelven értők. Az emberi intelligencia persze a nyelvi szokásjog alapján egyértelműnek tekinti azt is, hogy a *123* szám tízes számrendszerben értendő, így valóban *„százhuszonhárom”* darabnyi mennyiséget értünk az üzenetből. A *„123 db könyv”* sűrített üzenet a magyar nyelv rövidítéseiben járatos emberek számára még mindig egyértelmű (az előző kiegészítésekkel!). Mennyiségi leírásnak tekintve ugyanez mondható el a *„123 db”* üzenetről is. A *„123”* numerikus üzenet azonban már nem csupán nem hordozza önmagában e szám(ok) mennyiséget leíró tartalmát, hanem numerikus volta is kétséges! Hiszen még ha mennyiségi tartalmat feltételezünk, akkor is lehet bármely hármasnál nagyobb alapú számrendszerben felírt szám, amelyek mind-mind lényegesen eltérő mennyiségeket képviselnek. Például négyes számrendszerben a *„123*”=”huszonhét valami”, ötös számrendszerben a *„123”=”harmincnyolc valami”*, tízes számrendszerben a *„123”=”százhuszonhárom valami”*, míg százas számrendszerben a *„123”=”tízezerkétszázhárom valami”*. A *„123”* üzenet bizonytalansága azonban ennél jóval nagyobb, mivel az *1, 2, 3* jelek tetszőleges ABC betűit helyettesíthetik, azaz a *„123”* akár tekinthető ugyanolyan kódnak, mint az 3.2.1.ábra kódjai, csupán annyi bizonyos, hogy nem bináris kód.

A globális e-kommunikáció „fekete dobozában” tehát egyre nagyobb mennyiségű, mesterségesen elhelyezett, *„természetes értelmetlenség”* található! A globális kommunikáció „fekete doboza” pillanatnyilag úgy tekinthető, mint *a digitális világ Bábel tornya*, amelyben az emberi nyelvek különböző számkódokká keveredtek össze, melyeknek megértéséhez, azaz ahhoz, hogy az információk jel alakját ismeretté konvertáljuk, már egyáltalán nem elegendő csupán a nyelv ismerete.

Ebben a „természetes rendetlenségben” kell rendet teremtenünk, ha azt akarjuk, hogy „fekete dobozunk” hasonlítson a természetes intelligenciához. Ennek módja azonban csak a *Találd meg!* filozófián át vezet. Azaz éppen a racionális, gazdasági, üzleti megfontolásokból feleslegesnek tartott redundancia segítségével kell jelentést találni az információ (jel) tömegnek, majd (ha még mindig nem értelmes számunkra az üzenet), a *Találd ki!* séma alkalmazásával jutunk a számunkra is értelmezhető, azaz a természetes intelligencia számára befogadható ismerethez.
Az ismeretet itt általános fogalomként kezeljük, amely jelenti mindazt az asszociációt, amit az adott információ az üzenet fogadójából kivált. Így világossá válik, hogy míg az információ statikus, addig az ismeretre alapuló (jelentés tartalommal bíró) kommunikáció dinamikus jelenség!

Nem véletlen, hogy a természet a titkosításra inkább a rejtést használja (pl. mimikri), amely éppen a jelentős redundanciára épít. A rejtés optimumát ekkor nem a rejtőzködő, hanem a környezete határozza meg! Ha megváltozik a környezet, akkor ezzel együtt kell változni a rejtőzködőnek is. Ez tehát a *Találd meg!* titkosítási séma.

Kérdés tehát, hogy a *Találd meg!* séma kivitelezésére alkalmas-e az emberi (vagy egyéb) nyelv? Ez a sarkalatos kérdés, ahogy a későbbi fejezetekben látni fogjuk, a *„valódi vagy virtuális információ?”* megválaszolásával ekvivalens!

4. A rejtjelzés és rejtjelfejtés forradalma: *gépesítés a 20. században*

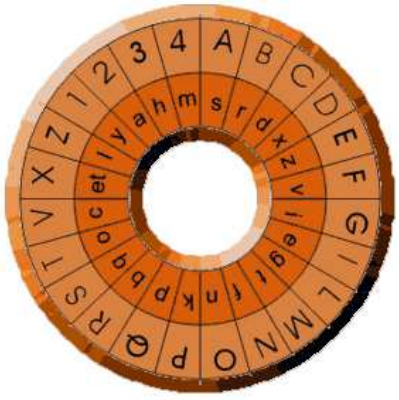
„Mialatt a világ termelése szédítő arányokban növekedett,
az emberiség felét éhhalál fenyegeti.
Pedig a fenyegető katasztrófát soha nem álmodott
jóléttévé lehetne átváltoztatni.”
(Magyar Miklós: Az ember és a gép harca, 1933.)

4.1. Rejtjelző kerék

A TitokTan Trilógia megírása során különös párhuzamra figyeltem fel. Ahogy a technika fejlődésének történetét meghatározta és napjainkig végigkíséri a *kerék „feltalálása”*, ugyanígy vezethető vissza a rejtjelzés és rejtjelfejtés gépesítésének története a *rejtjelző kerék* megalkotására. A két történet közötti lényeges különbség azonban, hogy míg általában a kerék „feltalálóját” nem ismerjük és a feltalálás időpontjáról is csak elképzeléseink vannak, addig a *rejtjelző kerék* története a 15. századi feltalálása óta pontosan követhető.
Érdemes e fél évezredes technikai törzsfejlődést, az anyaméhben történő embrionális egyedfejlődéshez hasonlóan, felgyorsított formában áttekinteni[23], hogy végül értő részesei lehessünk a 20. századi infokommunikációs bumm megszületésének.

Leon Battista Alberti
(1401-1472)

Leon Battista Alberti (1401-1472) a 15. századi kiemelkedő alakja, aki igazi reneszánsz gondolkodóként fogalmazta meg világszemléletét: *„Úgy kell tanulni a természettől, hogy megragadjuk a dolgok legfutólagosabb mozzanatait, azokat, amelyek többre indítják a néző képzeletét, mint amit lát.”* Csodálatos, ahogy egyetlen mondatba tömörítve írja le a természet törvényeibe rejtett titkok megismerése iránti olthatatlan emberi vágyat[24], és a megismerés részben szubjektív folyamatát. Az sem véletlen, hogy éppen Ő írta le elsőként a perspektíva törvényeit, a két szem szerepét a sztereo látásban: *„A kép úgy keletkezik, hogy a festő szemét és a lefestendő tárgyat egy sugárral kötjük össze, ahol ez a sugár a festő elé tett átlátszó síkot döfi, ott keletkezik a tárgynak megfelelő kép. … ha a festő megtartva a festendő kép síkját, de máshonnan nézi ugyanazt a tárgyat, akkor természetesen más képet kap.”*



4.1. ábra *L.B. Alberti rejtjelző korongja*

Talán éppen a nézőpont megváltoztatásának gondolata vezette Albertit a *korongos rejtjelző* megalkotására. A rejtjelző személy, aki lehet éppen a festő (emlékezzünk a Monet tájkép és a csillagképek analógiájára), gondolatban a korong középpontjában helyezkedik el, ahonnan a különböző sugárirányokba nézve, különböző „képét” látja ugyanannak a tárgynak, azaz a nyílt ABC és a

[23] E korszak részletes áttekintését adja a titkosítás szemüvegén át, a TitokTan Trilógia második [TDT 2004-k] kötete.
[24] Alberti több mint 500 éve megfogalmazta a *Találd meg!* gondolkodási modell lényegét, és reneszánsz polihisztorként ugyanabban az agyban kelt életre a *Találd ki!* modell forradalmian új rejtjelző eszköze, a *korongos rejtjelző*.

kód ABC változó megfeleltetéseit. Így írta le Alberti találmányát, a rejtjelző korongot: *„Rézlemezekből kivágok két korongot. Az egyik nagyobb, ez lesz a rögzített, a másik kisebb átmérőjű, ez lesz a forgatható. Mindkét korongot sugár irányban 24 egyenlő részre osztom. Ezeket a részeket celláknak nevezzük. A nagy korong celláiba beírom az ABC nagybetűit a szokásos sorrendben … a kis korong celláiba az ABC betűit véletlen sorrendben …”*[25]

Alberti e találmányával megteremtette a több ABC-s rejtjelzés alapjait, amely a későbbi modern kriptográfiának egyik alappilére. Rejtjelző korongjának alapelvét láthatjuk viszont évszázadokkal később a 18.-20. századi mechanikus, majd elektromechanikus (rotoros) rejtjező gépekben. Nem csupán a rejtjelző koronggal, de több korszakos találmányával[26], évszázadokkal megelőzte korát, így nem véletlen, hogy a *Nyugati Kriptográfia Atyja*-ként tartjuk számon.

Giovanni Battista Porta (1535-1615)

Minden bizonnyal az itáliai reneszánsz gondolkodást megtermékenyítő szellemének köszönhető, hogy a következő évszázad, a 16. század is olyan polihisztor óriásokat adott Európának, mint Girolamo Cardano (1501-1576)[27], vagy *Giovanni Battista Porta* (1535-1615). Porta nem csak húsz kötetes monumentális művével, a Magiae naturalis[28]-al alkotott maradandót, de megfogalmazta tevékenységének végső indítékát: *„Megvizsgálom azt, amit elődeink mondtak. Azután saját kísérleteimmel mutatom be, hogy igazak-e ezek vagy hamisak …”* Ez a gondolat négy évszázaddal előzi meg a 20. századi empirikus gondolkodást, így bátran választhatja minden mai kutató, tudós ars poéticául.

4.2. ábra Rokokó rejtjelző korong Porta kódtáblájának *jeleivel*

Porta kriptográfiai rendszerét a TitokTan Trilógia 2. kötetének 14. fejezetében részletesen tárgyalom, jelen kötet témája szempontjából az emelendő ki, hogy a Magiae Naturalis XVI. könyvében, Ő osztályozta elsőként a rejtjelzési módszereket a mai modern terminológiának megfelelően *helyettesítéses* és *keveréses* eljárásokra.[29] Ugyanebben a könyvben bemutatja a

[25] Alberti az Itáliában akkor használatos olasz és latin nyelvre alkalmazta rejtjelző korongját, ezért csak az azokban használatos betűket tüntette fel.

[26] Például a rejtjeles szövegek *betűstatisztikájának* vizsgálata, amely a 20. században vált a kriptológia alapvető eszközévé!

[27] Cardano neve a harmadfokú egyenlet megoldó képletével vonult be a köztudatba. Még a technika történet könyvek sem emlékeznek meg arról a technikatörténeti kuriózumról, hogy Ő találta fel a kardán-csukló alapelvét, amit 500 év után, ma is mindenki használ (változatlan formában!), aki autóba ül. Korának meghatározó polihisztor gondolkodójaként, a kriptográfiában is maradandót alkotott. Megalkotta az úgynevezett cardano-rácsot, amely a keverő rejtjelzési eljárások alapvető eszközévé vált.

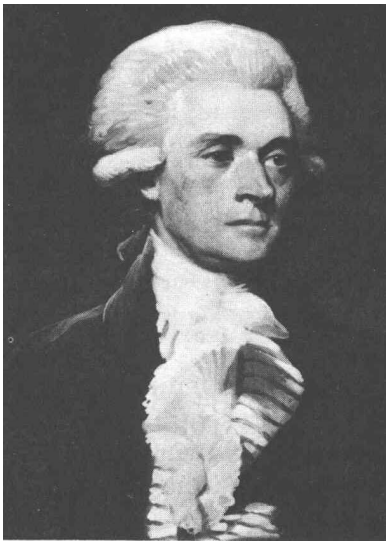
[28] Szó szerinti fordítása: *Természetes varázslat*, de a tartalmát pontosabban fedi a *„természet varázslata”*. Ezt tükrözi a húsz kötet címe és a teljes korabeli ismerethalmazt felölelő tartalma, Porta ma is korszerűnek tekinthető gondolataival szintézisbe foglalva. Különleges példaként említendő a II. könyv, amelynek címe: *Az élő fajok változatosságának bemutatása, ahogy keveredés és párosodás útján új, életképesebb fajok keletkeznek.* E kötet 22 fejezetében tulajdonképpen három évszázaddal előzte meg az evolúció elméletét.

[29] Ez pontosan megfelel a 2. fejezetben bemutatott *Találd ki!* és *Találd meg!* általános gondolkodási modelleknek.

rokokó néhány esztétikailag is különleges rejtjelző korongját, amelyek egyik legszebb példányát láthatjuk a 4.2. ábrán, amelyen felfedezhetjük Porta különös kódtáblájának jeleit.

4.2. Rejtjelző henger

A rejtjelző korong különböző megjelenési formákban még két évszázadon át a titkos szövegek rejtjelzésének alapvető eszköze volt Európában. A diplomáciai kapcsolatok élénkülése térben és időben is megnövelte a titkos kommunikáció mennyiségét, így szükségessé vált a kommunikáció biztonságának növelése. A 18. század utolsó évtizedéig ebben nem volt jelentős szerepe az amerikai földrésznek.



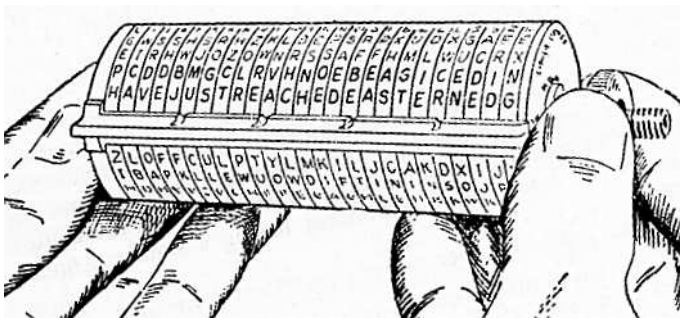
Thomas Jefferson (1743-1826)

Ekkor azonban éppen ezen a földrészen jelent meg egy nagy hatású reneszánsz gondolkodó *Thomas Jefferson*[30] (1743-1826) személyében. Jefferson nem csak a legújabb kori modern társadalmakra alapvető hatást gyakorló Függetlenségi Nyilatkozat megszövegezője volt, de a reneszánsz polihisztorokhoz hasonlatosan, sikeres politikusként és kísérletező tudósként is maradandót alkotott.

A ma is hatályban lévő 1787-ben elfogadott amerikai alkotmány szükségességét, így indokolta: *„A kormányzatok jogos hatalma a kormányzottak beleegyezéséből ered. Valahányszor a kormányzati mód veszélyezteti a természetből eredő jogaikat, a népnek jogában áll azt megváltoztatni vagy megsemmisíteni, s új alkotmányt teremteni, amely olyan elveken épül fel és olyan módon van megszervezve, mely legalkalmasabbnak látszik arra, hogy a nép boldogulását lehetővé tegye."*

Jeffersont különösen foglalkoztatta a különböző nyelvek használata a jelentős mennyiségű bevándorló és az indián törzsek kommunikációjában. Elkészítette indián-angol szótárát, azzal a nem titkolt céllal, hogy a katonatisztek az indiánokkal minél pontosabb kapcsolatba tudjanak kerülni.

Az 1780-as években kezdődő ipari forradalom Angliából futótűzként érte el Amerikát is. Ez nem egyszerűen a gőzgép feltalálását jelentette, amelynek az egész ipari és mezőgazdasági termelésre rendkívüli hatása volt, hanem egy merőben új szemléletmódot hozott a társadalmi gondolkodásban. Jefferson az alkotmányozással azonos jelentőségűnek tekintette a szabadalmi törvény létrehozását, amelynek szintén tevékeny részese volt. Személyiségére jellemző, hogy bár számos jelentős találmányt dolgozott ki, ezeket soha nem szabadalmaztatta. Aktív részvétele a diplomáciában, valamint nyelvekkel kapcsolatos kutatásai, keltették fel érdeklődését a titkosítás, a kriptográfia iránt. Maga is alkalmazta a kor általánosan elterjedt rejtjelzési módszerét, a kódkönyvet (lásd [TDT 2002-k]). Ennek előnyös tulajdonságai kapcsolta össze a rejtjelző korong dinamikusan és kényelmesen változtatható variabilitásával és



4.3. ábra *Jefferson rejtjelző (tárcsás) hengere (1790.)*

[30] George Washington és John Adams után 1801-1809 között az USA harmadik elnöke.

megalkotta a korszakos jelentőségű *tárcsás rejtjelző hengert*, amelyet a szellemi nagysága előtt tisztelegve, az utókor *Jefferson henger*-nek nevez.
A *Jefferson rejtjelző henger* 20 centiméter hosszúságú fa henger, amely 26 darab 5 centiméter átmérőjű tárcsából állt. A tárcsák közepe lyukas, így a lyukakon áthaladó fémpálca végén egy rögzítő csavarral lehetett összefogni. Minden tárcsa peremére az angol ABC 26 betűjét vésték. Így mindegyik tárcsa egy-egy állásánál az angol ABC egy sorrendjét állították elő, ami olyan mintha a henger palástján minden állásban egy Vigenére-tábla[31] lenne felkasírozva. Jefferson úgy alakította ki a henger méreteit, hogy a tárcsák beállításait gyorsan és kényelmesen el lehet végezni, az így létrehozható rejtjelzések számát a következő 27-jegyű szám írja le:

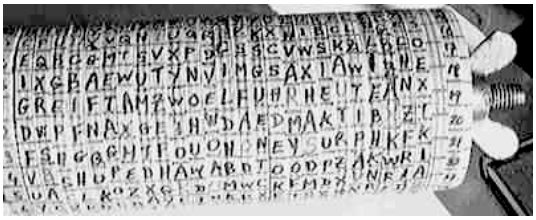
$$26 \cdot 25 \cdot 24 \cdot \ldots \cdot 3 \cdot 2 \cdot 1 \approx 403.291.461.126.605.635.584.000.000 \tag{4.1}$$

Ez az elképzelhetetlen variabilitás, valamint a *Jefferson henger* gyors és kényelmes használata, hordozhatósága messze túlmutat saját korán és megteremtette a 19-20. századi gépesített rejtjelzés alapjait. Joggal nevezhetjük Thomas Jeffersont az *amerikai kriptológia atyjának.*

Étienne Bazeries (1846-1931)

A technikatörténet érdekessége, vagy éppen fintora a Jefferson henger további sorsa. Részben Jefferson találmányával kapcsolatos visszafogottsága, részben titkos jellege következtében, a rejtjelző henger híre nem jutott el Európába. Így fordulhatott elő, hogy Étienne Bazeries (1846-1931) a francia hadsereg rejtjelfejtő őrnagya mintegy 100 évvel Jefferson után, ismét feltalálta a rejtjelző hengert. Készüléke nagyban hasonlított a Jefferson hengerhez, csupán ez 20 tárcsára épült és minden tárcsa peremére 25 betűs ABC-t írtak. Mivel kezelése is hasonló volt, így mondhatjuk, hogy Jefferson hengerének francia „reinkarnációjával" állunk szemben.

A történetnek azonban más érdekessége is van. Bazeries rejtjelző hengerének alkalmazását ugyanis a francia hadsereg elutasította. Mivel azonban Jefferson túlzott „szerénysége" következtében az Amerikai hadsereg nem használta a Jefferson hengert (valószínűleg száz év távolából a feledés homályába merült), Bazeries nem kis meglepetésére, 1922-ben az Amerikai hadsereg befogadta rejtjező hengerét és M-94 kódnéven alkalmazásba vette (1944-ig alkalmazta!). Ezzel kétszeresen bebizonyosodott a bölcs mondás igazsága, miszerint *„nem lehet senki próféta a saját hazájában"*!



4.4. ábra *Bazeries rejtjelző hengere (1901)*

4.5. ábra *Az Amerikai hadsereg M-94 rejtjelző*

[31] A Vigenére-tábla egy olyan 26x26-os táblázat, amelynek minden sorában az angol ABC egy-egy sorrendje szerepel. (Részletesen lásd [TDT 2004-k] 13. fejezetét)

A 20. század a titkos kommunikáció, a titkosítás fontossága szempontjából új korszakot nyitott a történelemben, nevezhetjük akár a *kódok évszázadának*. Talán e kor szellemének tudható be, hogy az I. világháború végén négy különböző országban, négy különböző feltaláló, szinte azonos időben, egymástól függetlenül[32] találta fel a rotoros (forgó tárcsás) rejtjelző gépet.
E gépek lényege, hogy a tárcsák (korongok) sorát, amely a forgórészt alkotja, bonyolult huzalozással kötik össze, így igen összetett algoritmusokkal helyettesíthetők az üzenet betűi a megfelelő rejtjeles betűkkel. A rotoros gépek tehát jóval erősebb rejtjelzést és jóval egyszerűbb kézi mechanikus, majd elektromechanikus kezelést (alkalmazást) tettek lehetővé.

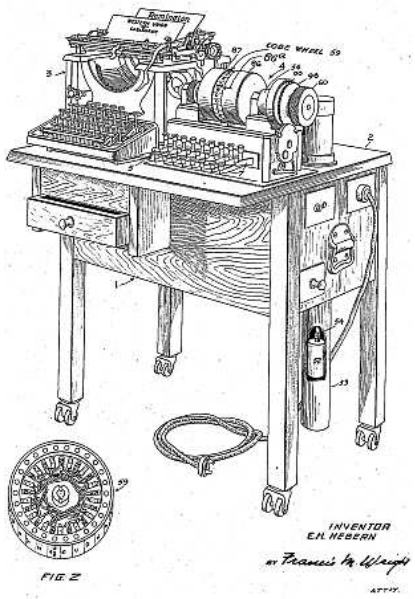
4.3. Rejtjelző gép

Edward Hebern (1869-1952)

Az első rotoros rejtjelző gépet *Edward Hebern* (1869-1952) az USA-ban találta fel. A találmány keletkezése szokatlan. Hebern építési vállalkozó volt, aki egy ló ellopása miatt 1908-ban börtönbe került. A kriptográfia iránt meglévő érdeklődését így volt ideje kiteljesíteni. 1912-1915 között több rejtjelző berendezést talált fel. A legfigyelemreméltóbb az 1917-ben elkészült elektromos írógép, amely egyben egytárcsás, 26-os huzalozású rotoros rejtjelzőgép is volt (lásd 4.6.-4.7. ábra).

További fejlesztései eredményeképpen 1921-ben már több tárcsás rejtjelző gépet épített. Erre a szabadalmára alapította a *Hebern Electric Code Company* nevű céget. Tehát elsőként hozott létre olyan gyárat (386.000 dollárból, 1.500 alkalmazottal), amelyben csak rejtjelző gépeket gyártottak. Megkezdődött tehát a rejtjelző eszközök gyártásának iparággá válása, ami az első lépés volt ahhoz, hogy maga a rejtjelzés, a titkosítás külön iparág lehessen.

4.6. ábra *Hebern első rotoros rejtjelző gépe (1917)*



4.7. ábra *Hebern első, elektronikus írógéppel összekapcsolt rotoros rejtjelzőgépének szabadalmi rajza*

[32] Akkor még globalizált világról nem beszélhettünk!

Hebern nem csak üzleti, de különös érzelmi kapcsolatban állt rejtjelző gépével, amit az *Óda a Hebern rejtjelző géphez* című költeményébe foglalt[33].

Óda a Hebern rejtjelző géphez
(Edward Hebern)

Marvelous invention comes out of the West
Triumph of patience, long years without rest
Solved problem of ages, deeper than thought
A code of perfection a wonder, is wrought

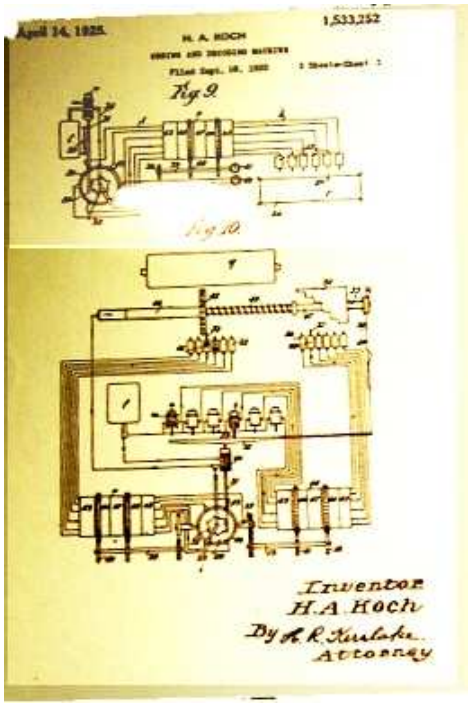
Of international scope, is the code electric
With merit so obvious, no nation can reject it
Result of deep study, when necessity goads
Hebern Electric, is the peer of all codes

Sphinx of the wireless, guardian of treasure
Brain of a nation, safety beyond measure
Heart of a battleship, preserver of lives
When brute force, against intellect strives

Keeper of secrets, of state and alliance
Inscrutable, wonderful, a mystery to science
Of depth so profound, brainy traitors, beware
Invisible around you, is the genii's snare

Conceived of the world war, in desperate need
Brains of all nations, competing in speed
Trained minds of the highest, seeking for might
An American achievement, is now brought to light

Történelmi időléptékkel mérve szinte Hebernel azonos időben, 1919. októberében jelentette be rotoros rejtjelző gépét a szabadalmi hivatalnál *Hugo Alexander Koch* (1870-1928) Hollandiában (lásd 4.8. ábra). Hebernel ellentétben, soha nem adott el egyetlen gépet sem, viszont 1927-ben eladta rejtjelző gépe jogait Arthur Scherbiusnak 600 guldenért. E nem túl jelentős összeget sem volt módja sokáig élvezni, mivel 1928. márciusában meghalt. Néhányan úgy gondolják, hogy Scherbius saját találmánya védelmében vásárolta meg Koch szabadalmát, mivel annak technikai megoldása nagyon hasonló volt az övéhez. A pontos történet máig nem tisztázott.



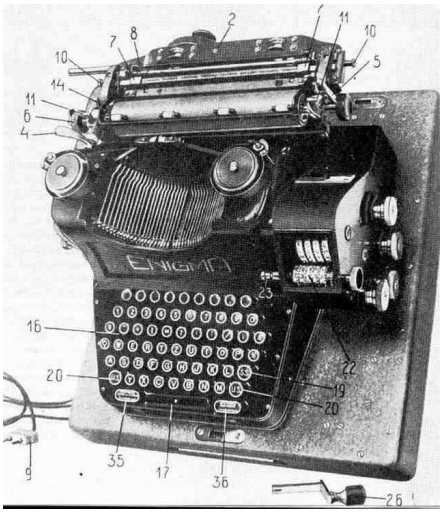
4.8. ábra H.A. Koch rotoros rejtjelző gépének szabadalmi rajza

[33] Mivel valódi költeményről van szó, nem vállaltam fel a műfordítás nemes terhét, így az eredeti angol szöveget adom közre. Örömmel fogadnám, ha a műfordítói vénával megáldott kedves Olvasók megörvendeztetnének e különös költemény fordításával és e kötet új kiadásában azt leközölhetném (természetesen a fordító megjelölésével).

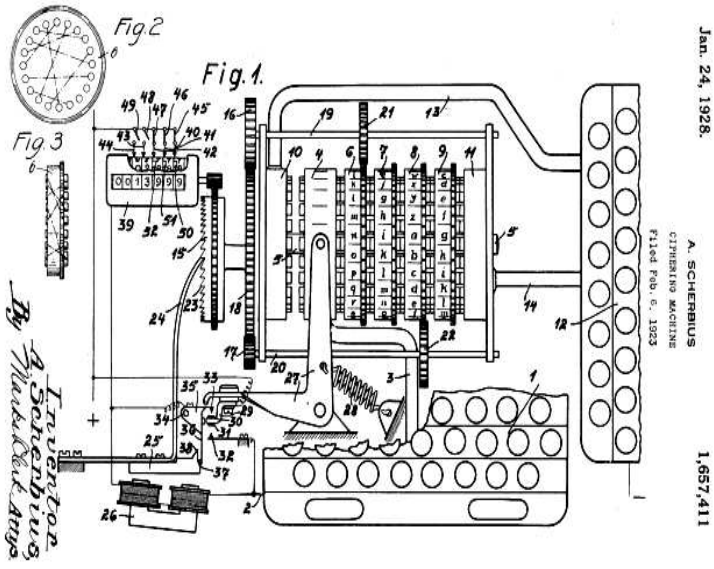
Arthur Scherbius
(1878-1929)

Az azonban tény, hogy néhány évvel Hebern után, *Arthur Scherbius* (1878-1929) német mérnök, 1923. február 6-án adta be Enigma elnevezésű, legendássá vált rotoros elektromechanikus rejtjelző gépének szabadalmát (lásd 4.9. ábra).

Hasonlóan a Jefferson henger tárcsáihoz, az Enigma tárcsáinak kerületén egy-egy mozgatható gyűrűn szerepeltek a számjegyek és betűk 1-től 26-ig, illetve A-tól Z-ig. A háromtárcsás gépen az üzenetet el lehetett indítani a kulcsciklus bármely pontján a három tárcsának a kívánt pozícióba állításával. Előzetes megállapodással, vagy szigorúan titkos üzenetben továbbított indikátor követésével az üzenet küldője és fogadója úgy állította be a tárcsáit, hogy a kiválasztott hárombetűs indikátort (pl. AZG vagy bármi más) lehessen látni a készülék tetején lévő ablakban. Az egyenként eltérő belső elektromos kötésű tárcsákat ki lehetett emelni a helyükről és más sorrendben visszahelyezni. Ez hat permutációt eredményezett: a három tárcsa bármelyike kerülhetett a bal oldali helyre, amivel két lehetőség maradt a középsőre, és az azután megmaradt tárcsa került a jobb oldalra, ez *3x2x1=6* lehetséges balról-jobbra tárcsakombinációt eredményezett. További permutációk létrehozásához újabb tárcsákkal lehetett kicserélni az egyik, vagy akár mindhárom tárcsát. Öt munkába állítható tárcsával már



Enigma író és rejtjelző gép
(az első típus)



4.9. ábra *Az Enigma rejtjelző gép szabadalmi rajza*
(Beadás: 1923. február 6.)

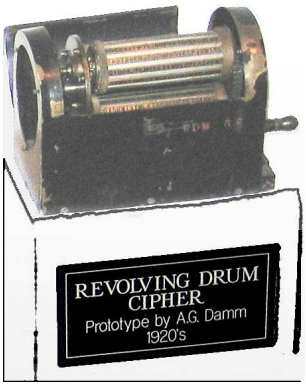
5x4x3=60 eltérő tárcsasorrendet lehetett létrehozni (általában 5 tárcsával használták az Enigmákat). Továbbá minden tárcsán új pozícióba lehetett állítani a léptető hornyot, mely a betűkkel ellátott mozgatható gyűrűn helyezkedett el és amely gyűrűt a tárcsától függetlenül el lehetett forgatni, mint gumiabroncsot a kerék körül. A gyűrűk ilyen módon történő

átállításával elmozdult az a pont, amelyiknél a tárcsa továbblépett, amivel további *26x26=676* lehetséges kombinációra osztotta az egyes kulcsszekvenciákat. Mivel változtatni lehetett a gyûrû beállítását, mindehhez még hozzájárult, hogy az adott indikátor esetében el lehetett rejteni a tárcsák tényleges kiindulópontját, hiába tudta az üzenet címzettje, hogy AZG-ből kell kiindulnia, ezzel az információval még nem dekódolhatta az üzenetet, csak ha azt is tudta, hogyan kell beállítania a tárcsákon a gyűrűket – amire *26x26x26=17.576* lehetőség adódott.

Az Enigma a rejtjelzés és a rejtjelfejtés szempontjából is történelmi jelentőségűvé vált, mivel mindkét területen -ahogy azt a következő oldalakon látni fogjuk-, új korszakot nyitott.
Mindezeknek a rejtjelzés biztonsága szempontjából a kor technikai lehetőségei mellett fantasztikus jótulajdonságok ellenére, az Enigma pályája eleinte nem sok jót ígért. Az egyik korai Enigma modellt kiállították Bernben a Nemzetközi Posta Unió 1923-as kongresszusán, ahol üzletembereknek kínálták, hogy titokban tarthassák táviratai tartalmát a konkurensek fürkésző tekintete elől. A mechanikai és matematikai szempontból egyaránt briliáns szerkezet azonban kereskedelmileg kész csődnek bizonyult.
Scherbius megpróbálta értékesíteni gépét a német katonai és kereskedelmi cégeknek, de nem volt rá igazi érdeklődés. 1926-ban kifejlesztette az Enigma C modelljét, amelynek súlya már az eredeti modell negyede volt (kb. 12 kg). Ezt a modellt 1926-ban megvette a német haditengerészet, majd 1928-ban követte a német hadsereg is.
Nem sokkal ezután 1929-ben Scherbius egy lovaskocsi balesetben halt meg, így nem élhette át azt az élményt, ahogy találmánya a 20. század középső évtizedeinek kulcsszereplője lett.

Arvid Gerhard Damm

A negyedik feltaláló *Arvid Gerhard Damm*[34] svéd mérnök és feltaláló. Eredetileg textilmérnök volt, és konstruktőr menedzserként dolgozott egy Finnországi textilgyárban. Ebben az időben hamis szertartás keretében (amit Damm barátja álpapként celebrált) kötött házasságot egy magyar nővel. Később, miután egy új romantikus kapcsolatra talált, Damm megpróbált elválni, azzal a valótlan állítással, hogy a nő kém volt, de kétszínűsége felszínre került, amit üzleti partnere Olof Gyldén fedett fel (akinek előléptetését igencsak mellőzték később a vállalatnál).



A.G. Damm rotoros rejtjelző gépe (1920)

Mindössze 3 nappal Koch után, 1919. október 10-én jelentette be rejtjelző gépének szabadalmát. Ő dupla tárcsás rotort alkalmazott, de készüléke nem működött megbízhatóan, így soha nem adott el egyetlen példányt sem. Azonban Damm megalapította az AB Cryptograph céget, amely a Crypto A.G. elődje volt. Két befektető, K.W. Hagelin és Emanuel Nobel (Alfred Nobel unokaöccse) látott fantáziát a rejtjelző gépben és befektetett Damm cégébe.

[34] Csak halálozási éve ismert: 1927.

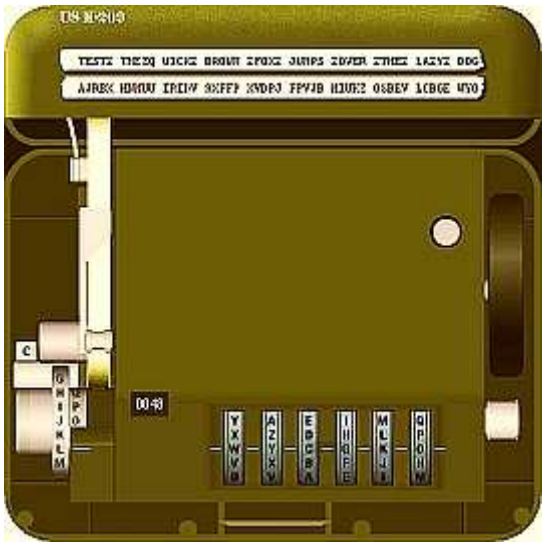
Boris Hagelin (1892-1983)

1922-ben Hagelin fia, *Boris Hagelin* (1892-1983) a cég fejlesztő mérnökeként kezdett foglalkozni Damm szabadalmával, így 1926-ban a svéd hadsereg nagyobb tételt vásárolt belőle. Az üzleti sikert azonban Koch esetéhez hasonlóan, Damm sem élvezhette sokáig, mert 1927-ben meghalt.

Boris Hagelin vette át a céget és új találmányokkal bővítette a kínálatot. Kifejlesztette a B-211 rejtjelző gépet, amely saját nyomtatóval rendelkezett, és a C-35 jelű kézi rejtjelző eszközt. Ennek továbbfejlesztett változata volt a C-38, amelynek licencét az USA megvásárolta és M-209 néven nagy sikerrel használták. A készülék sikerét jól jellemzi, hogy a II. világháború alatt 140 ezer példányt gyártottak belőle. Így lett Boris Hagelin az első, akit a rejtjelző gépek tettek milliomossá. A Hagelin cég az 1970-es években már 60 országban forgalmazta rejtjelző készülékeit.

Boris Hagelin tárcsás kézi rejtjező gépe és annak belső szerkezete.

HAGELIN M-209 CIPHER MACHINE (GVG / PD)



A nagy sikerű M-209-es, amely Boris Hagelint milliomossá tette. Jobbra az USA-beli új formatervezéssel.

E négy párhuzamos (siker)történet közül a legmaradandóbb, a szó valódi értelmében történelem formáló, napjainkig ható nyomot az Enigma hagyta. Ma már tudjuk, hogy ennek oka a II. világháború rejtjelzésében és rejtjelfejtésében betöltött szerepe. Mindkét szálon korszakváltást indított el. Az egyik szál, a „tökéletesen biztonságos” rejtjelzés, az egyetlen elméletileg bizonyítottan megfejthetetlen algoritmus, a *végtelen átkulcsolás (one-time-pad)* kidolgozása. A másik szál az elektronikus rejtjelfejtő gépek megépítése, amelynek elméleti és technikai alapjaiból az *elektronikus számítógép* és az egész *számítástechnika* kinőtt.

A dugaszoló aljzattal (stekkerrel) szerelt Enigma rejtjelző gép

Az Enigma későbbi modelljeiben dugós csatlakozók (steckerek) biztosították az újabb keverési lehetőséget, és további permutációk milliárdjait generálták a kulcsszekvenciákban. A dugaszolt Enigma gépek esetében a billentyűzetet és a lámpákat nem közvetlenül a bemeneti gyűrűhöz kötötték, hanem közbeiktattak egy harminchat pár dugós csatlakozóval ellátott kapcsolótáblát.

A régimódi telefonközpontokban használatosokhoz hasonló dugós végű kábelek összeköttetést létesítettek a kiválasztott betűk között. Tíz kábel 150 milliószor millió ilyen permutációt tett lehetővé!

Ha történetesen az ellenséghez jut egy gép, azzal még szinte semmi nem kerül a rejtjelfejtő kezébe, amivel továbbléphetne. Az Enigma által generált egyedi kulcsszekvenciák óriási száma, az a mód, ahogy ezeket a kulcsokat naponta, vagy akár gyakrabban meg lehetett változtatni, az egyes kulcsok hosszúsága, mindezek minimális valószínűségűvé tették, hogy két üzenetet ugyanazzal a kulcs-betűsorral generáljanak, így tökéletesen alkalmazhatatlanná váltak a rejtjelfejtés szokásos matematikai eszközei.

Ez inspirálta a történelem talán legtitkosabb projectjének, az angol ULTRA projectnek létrehozását, amelynek célja az Enigma megfejtése volt. Az ULTRA project tevékenységével és annak történelmi, tudomány és technikatörténeti hatásaival foglalkozik *Titkos-számítógép-történet* című kötetem [TDT 2003-k], amelynek jelen témánk szempontjából fontos rövid összefoglalására kerül sor a következő fejezetben.

Az ipari forradalom 18. századi kezdetei óta különös kettősség jellemzi a gépek, a társadalmi méretű gépesítés megítélését. Egyrészről a gépek az ember barátai, amíg életüket kényelmesebbé, gazdaságukat termelékenyebbé teszik, másrészről az ember ellenségei, amikor sokak munkáját, munkahelyét teszik feleslegessé. A 20. században a gépesítés fejlődése rohamosan felgyorsult, találó Magyar Miklós 1933-ban megjelent könyvének címe (Az ember és a gép harca [MAGYAR M. 1933]) és egyáltalán nem véletlen a könyvéből vett idézet, amelyet e fejezet mottójában idéztem. Az idézet a fenyegető munkanélküliség réme után, mégis a remény lehetőségével zárul: *„Pedig a fenyegető katasztrófát soha nem álmodott jóléttét lehetne átváltoztatni.”*.
Nos, a biztonság (és ennek részeként a *titkosítás*) gépesítése éppen ebbe a remény kategóriába tartozik, mivel ebben az esetben pontosan fordított törvényszerűség érvényesül:

maximális biztonság = minimális emberi tényező

Bár a rejtjelzés, illetve az információbiztonság még matematikailag is nehezen definiálható[35], e törvényszerűség alapján biztosan állíthatjuk, hogy a 20. századi gépesítési tendencia a biztonság növekedése irányába hatott. Ennek legszebb példája, hogy az eddig ismertetett elektromechanikus rotoros rejtjelző gépek fejlődésével párhuzamosan, már az I. világháború idején megjelent az egyetlen ismert, matematikailag bizonyíthatóan megfejthetetlen rejtjelző eljárás, a *végtelen átkulcsolás (one-time-pad, rövidítve: OTP).*

A végtelen átkulcsolás a nyílt szöveget betűnként (vagy betűcsoportonként) kódolja át. Ennek során az eredeti szöveget a hírközlő csatorna bemenetére alkalmas ABC szerinti sorozattá kódolják át. A kódoláshoz kulcsként egy fizikai véletlen (vagy álvéletlen) sorozatot használnak[36], amelyet a szövegtől teljesen függetlenül, előre generálnak, az egymás utáni kulcsbetűket is egymástól függetlenül választják meg, mégpedig úgy, hogy minden kiválasztásra kerülő kulcsbetű egyenlő valószínűséggel lehet az ABC bármelyik betűje. A kulcssorozatot a *küldő* és a *fogadó* egymás között abszolút biztos csatornán előre kicseréli. A rejtjelzés az egymás utáni nyílt- és kulcsbetű összeadásával történik, mégpedig a konkrét üzenettől független, állandó Boole összeadó tábla szerint. A Boole összeadás (+) szabályai:

(4.2) $$0(+)0=0,\quad 0(+)1=1,\quad 1(+)0=1,\quad 1(+)1=0$$

PÉLDA a végtelen átkulcsolással történő rejtjelzésre:

REJTJELZÉS		
Nyílt üzenet		*10110101*
Kulcs		*00101101*
Rejtjeles üzenet (Bool összeg)	(+)	***10011000***

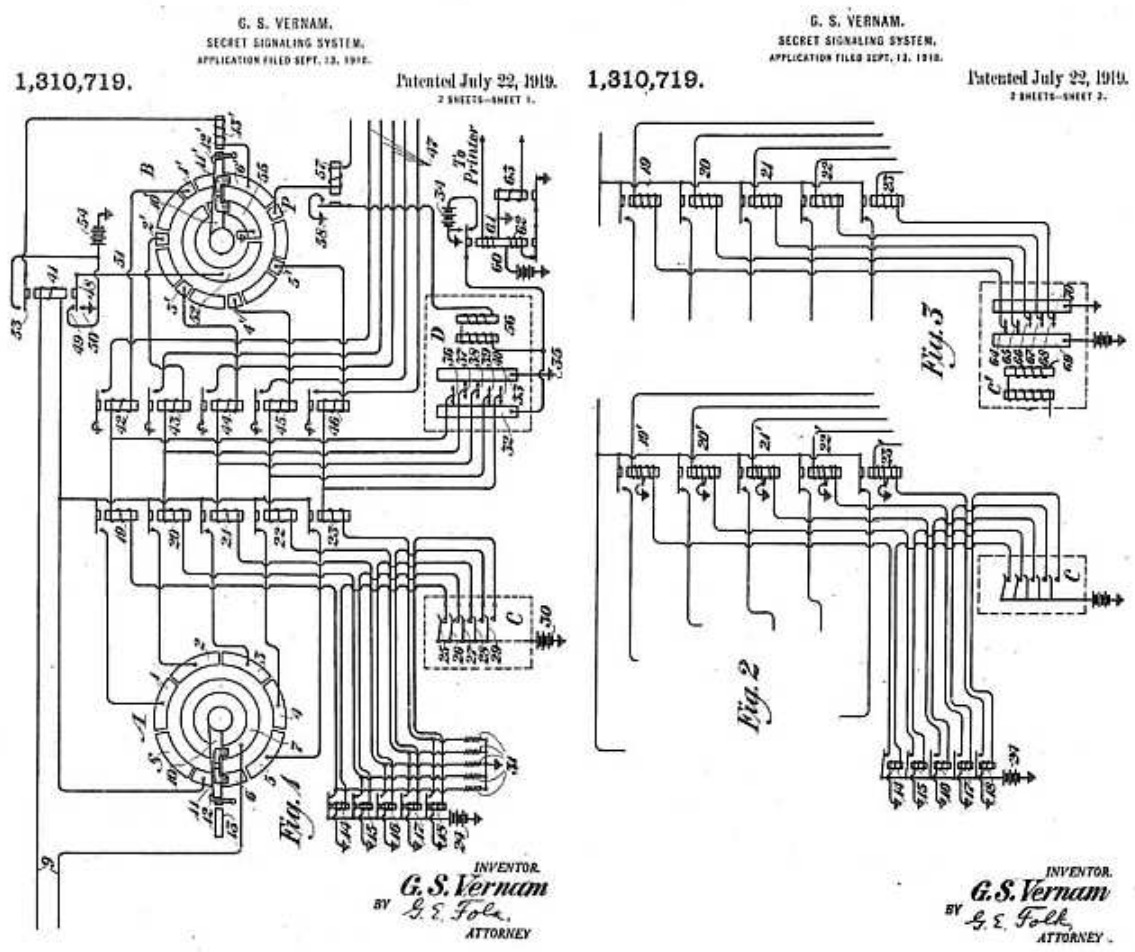
MEGFEJTÉS		
Rejtjeles üzenet		***10011000***
Kulcs		*00101101*
Nyílt üzenet (Bool összeg)	(+)	*10110101*

[35] A matematika talán legfiatalabb ága, a *bonyolultság elmélet* vizsgálja az ezzel kapcsolatos problémákat. Az információbiztonság szempontjából alapvető jelentőségű, hogy a problémákat osztályokba sorolja és kimondja, hogy van olyan problémaosztály amelynek feladatai a ma ismert matematikai eszközeinkkel, emberi léptékkel mérve reális időn belül nem megoldhatók. Ugyanakkor ezen feladatok egy részénél maga a „nem megoldhatóság” elméletileg nincs bizonyítva, csak annyit tudunk, hogy eddig nem sikerült az eszközeinkhez, számítógépeinkhez mérten jó eljárást találni a megoldásukra. Ez tehát azt jelenti, hogy mai információbiztonságunk alapvetően „gép függő”, vagyis a gépesítés fejlesztése a 21. században egyre inkább szükséges a biztonság növeléséhez.

[36] A *fizikai véletlen* számokat az különbözteti meg az álvéletlen számoktól, hogy az elsőnél egy fizikai véletlen folyamat bizonyos paramétereit rögzítjük (pl. szabályos pénz feldobás eredményei), míg az *álvélelen* sorozatot egy matematikai képlet alapján számítjuk ki, amely azonos kezdőértékek esetén azonos sorozatot állít elő.

Gilbert S. Vernam
(1890-1960)

A végtelen átkulcsolás alkalmazásához tehát annyi kulcselem kell, amennyi a továbbítandó üzenet (szöveg) hossza, ezért e rejtjelzés kulcsellátása igen bonyolult, és költségigényes. Ugyanakkor a rejtjelzés manuális elvégzése nagyon munkaigényes, így hatékony alkalmazásához elengedhetetlen volt a gépesítés. Ezt a problémát oldotta meg *Gilbert Sandford Vernam* (1890-1960) az American Telephone and Telegraph Company (AT&T Comp.) mérnöke. A végtelen átkulcsolást végző elektromechanikus rejtjelző gépének szabadalmát 1919. július 22-én adta be, amit 1.310.719 számon tartanak számon az USA-ban.



4.10. ábra *G.S.Vernam végtelen átkulcsolást végző rejtjelző gépének szabadalmi rajza (1919)*

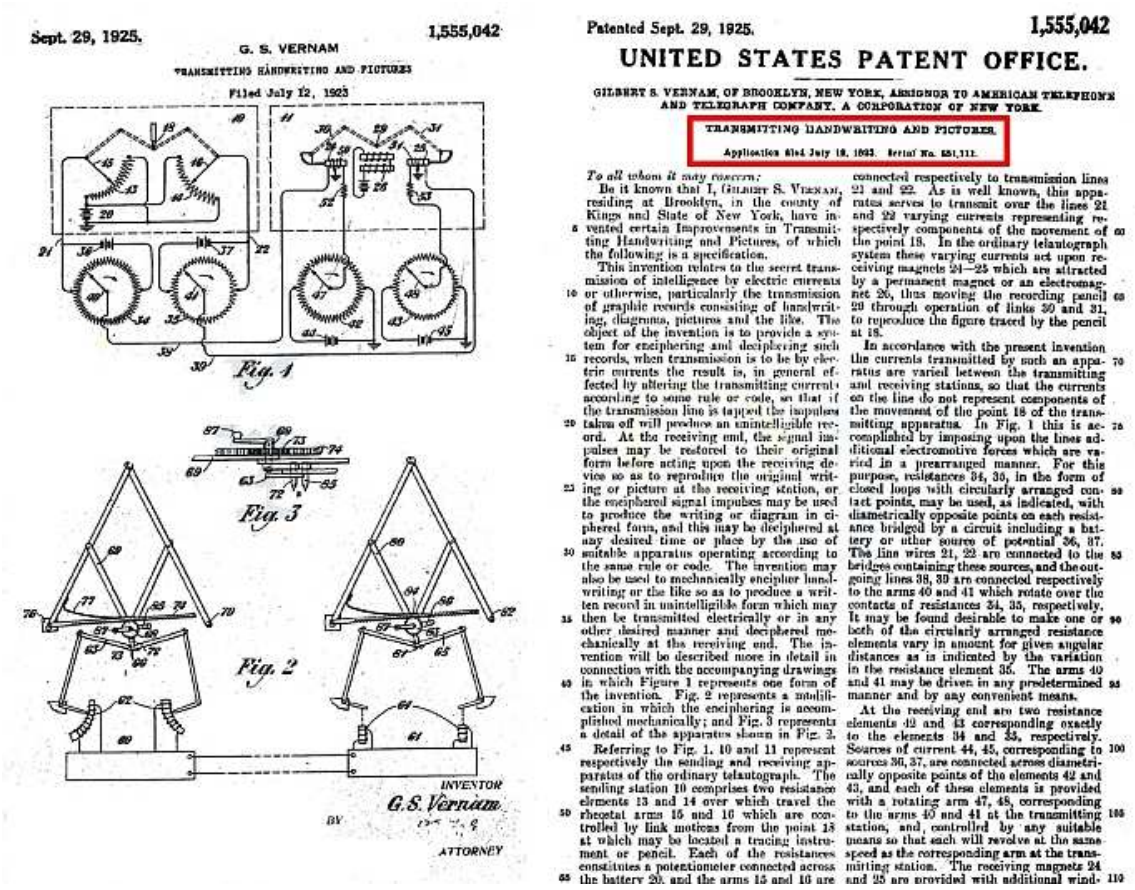
Vernam rejtjelző gépe a távgépíró elvén alapult és a kulcsot lyukasztott távírószalag formájában készítette el. Az impulzusokat a szalagon levő lyukak képviselték, amelyeket önműködően adtak hozzá a nyílt szöveg távíróimpulzusaihoz. A vevőnél azonos kulcsszalagú gép vonta ki a kulcsimpulzusokat a rejtjelzett szöveg impulzusaiból (lásd a fent bemutatott Bool összeadás példát). Ez a gép volt az első, amely egyetlen művelettel automatikusan végezte a rejtjelzés és a jel továbbítás munkafázisait. Automatikus jellege kitűnően alkalmassá tette arra, hogy a végtelen hosszú véletlen kulccsal megbirkózzék. Illetéktelen személy csak úgy fejthette meg a rejtjelzett üzenetet, ha a kulcsszalagot is a megszerezte.
A végtelen átkulcsoláson alapuló rejtjelzés maximális biztonsága tette alkalmassá a Vernam-típusú berendezést arra a különleges feladatra, hogy az 1960-as évek elején létrehozott Washington/Moszkva, azaz a két nagyhatalom elnöke közötti „forróvonalon” (hotline)[37] a titkosított kommunikációt folyamatosan biztosítsa.

Vernam-típusú rejtjelző berendezés az üzenetet és a végtelen átkulcsolást tartalmazó lyukszalagokkal

Az ETCRRM típusjelű rejtjelző gép, amely a Washinton/Moszkva „forródrót” kommunikációját biztosította

Vernam jóval saját korát megelőzve észrevette, hogy különböző típusú információkra is lehet azonos rejtjel-rendszert alkalmazni. Elmélete alapján megtervezte új berendezését, a kézírás, és képek átvitelére alkalmas rejtjelző gépet, amelyre 1923-ban 1.555.042 számon szabadalmat szerzett (lásd 4.11. ábra). Lényegében ezzel feltalálta a *titkosított faxberendezést*.

[37] Közismert nevén: „forródrót”



Sept. 29, 1925. 1,555,042

G. S. VERNAM

TRANSMITTING HANDWRITING AND PICTURES

Filed July 12, 1923

Fig. 1

Fig. 3

Fig. 2

INVENTOR
G. S. Vernam
BY
ATTORNEY

Patented Sept. 29, 1925. 1,555,042

UNITED STATES PATENT OFFICE.

GILBERT S. VERNAM, OF BROOKLYN, NEW YORK, ASSIGNOR TO AMERICAN TELEPHONE AND TELEGRAPH COMPANY, A CORPORATION OF NEW YORK.

TRANSMITTING HANDWRITING AND PICTURES.

Application filed July 12, 1923. Serial No. 651,111.

To all whom it may concern:

Be it known that I, GILBERT S. VERNAM, residing at Brooklyn, in the county of Kings and State of New York, have invented certain Improvements in Transmitting Handwriting and Pictures, of which the following is a specification.

This invention relates to the secret transmission of intelligence by electric currents or otherwise, particularly the transmission of graphic records consisting of handwriting, diagrams, pictures and the like. The object of the invention is to provide a system for enciphering and deciphering such records, when transmission is to be by electric currents the result is, in general effected by altering the transmitting current according to some rule or code, so that if the transmission line is tapped the impulses taken off will produce an unintelligible record. At the receiving end, the signal impulses may be restored to their original form before acting upon the receiving device so as to reproduce the original writing or picture at the receiving station, or the enciphered signal impulses may be used to produce the writing or diagram in ciphered form, and this may be deciphered at any desired time or place by the use of suitable apparatus operating according to the same rule or code. The invention may also be used to mechanically encipher handwriting or the like so as to produce a written record in unintelligible form which may then be transmitted electrically or in any other desired manner and deciphered mechanically at the receiving end. The invention will be described more in detail in connection with the accompanying drawings in which Figure 1 represents one form of the invention. Fig. 2 represents a modification in which the enciphering is accomplished mechanically; and Fig. 3 represents a detail of the apparatus shown in Fig. 2.

Referring to Fig. 1, 10 and 11 represent respectively the sending and receiving apparatus of the ordinary telautograph. The sending station 10 comprises two resistance elements 13 and 14 over which travel the rheostat arms 15 and 16 which are controlled by link motions from the point 18 at which may be located a tracing instrument or pencil. Each of the resistances constitutes a potentiometer connected across the battery 20, and the arms 15 and 16 are connected respectively to transmission lines 21 and 22. As is well known, this apparatus serves to transmit over the lines 21 and 22 varying currents representing respectively components of the movement of the point 18. In the ordinary telautograph system these varying currents act upon receiving magnets 24—25 which are attracted by a permanent magnet or an electromagnet 26, thus moving the recording pencil 29 through operation of links 30 and 31, to reproduce the figure traced by the pencil at 18.

In accordance with the present invention the currents transmitted by such an apparatus are varied between the transmitting and receiving stations, so that the currents on the line do not represent components of the movement of the point 18 of the transmitting apparatus. In Fig. 1 this is accomplished by imposing upon the lines additional electromotive forces which are varied in a prearranged manner. For this purpose, resistances 34, 35, in the form of closed loops with circularly arranged contact points, may be used, as indicated, with diametrically opposite points on each resistance bridged by a circuit including a battery or other source of potential 36, 37. The line wires 21, 22 are connected to the bridges containing these sources, and the outgoing lines 38, 39 are connected respectively to the arms 40 and 41 which rotate over the contacts of resistances 34, 35, respectively. It may be found desirable to make one or both of the circularly arranged resistance elements vary in amount for given angular distances as is indicated by the variation in the resistance element 35. The arms 40 and 41 may be driven in any predetermined manner and by any convenient means.

At the receiving end are two resistance elements 42 and 43 corresponding exactly to the elements 34 and 35, respectively. Sources of current 44, 45, corresponding to sources 36, 37, are connected across diametrically opposite points of the elements 42 and 43, and each of these elements is provided with a rotating arm 47, 48, corresponding to the arms 40 and 41 at the transmitting station, and, controlled by any suitable means so that each will revolve at the same speed as the corresponding arm at the transmitting station. The receiving magnets 24 and 25 are provided with additional wind-

4.11. ábra *Vernam kézírásos szöveg és kép titkosított átvitelére alkalmas berendezésének szabadalmi leírása (1923)*

Vernam nem csak saját korát előzte meg berendezéseivel, hanem gondolati íve megerősíti napjaink titkosítási szakembereit is, akik a matematikailag bizonyított megfejthetetlenséget preferálják (a statisztikus biztonsággal szemben) és ennek megfelelően a végtelen átkulcsolás modern változatában látják a jövőt.

Nem véletlen, hogy a legnagyobb titkosságú katonai, diplomáciai információ átviteli rendszereken kívül (lásd például „forródrót”) infokommunikációs korunkban nem alkalmazzák a Vernam-típusú készülékeket. Az egyik kritikus problémát az jelenti, hogy a végtelen átkulcsoláshoz *óriási mennyiségű fizikai véletlen szám szükséges*.[38]

A másik kritikus probléma, az átkulcsoláshoz szükséges *kulcsok szinkronizált eljuttatása* a felhasználókhoz és azok *biztonságos őrzése*, amely a hagyományos módon megoldhatatlan feladat elé állítja a konstruktőröket.

A legújabb technikai eredmények alapján azonban a 21. században eme problémák reálisan megoldhatók. Egy lehetséges elvi konstrukció a következő:

Híradástechnikai műholdon elhelyezett fizikai véletlen szám generátorral egy folyamatosan kibocsátott véletlen szám sorozatot maximális sebességgel bocsát ki a Földre. Ebből az *A*

[38] Az USA-ban jelenleg egy óra alatt a rejtjelzett üzenetek száma körülbelül a II. világháború alatt rejtjelzett üzenetek számával egyenlő.

felhasználó a *B* felhasználóval szinkronizáltan, annyit tölt le, amennyi az *A* által küldendő nyílt szöveg rejtjelzéséhez szükséges.

Az üzenet váltása során a kulcsokat meg kell semmisíteni (ez könnyen biztosítható a mai számítástechnikai rendszerekben). Ezt az eljárást alkalmazni lehet bármilyen digitális átvitelnél (írott szöveg, hang, kép, videó, stb.), sőt a mobil hírközlésnél is (megfelelő okos telefonok ma már rendelkezésre állnak).

5. A számítástechnika gyökerei a rejtjelfejtésben fogantak

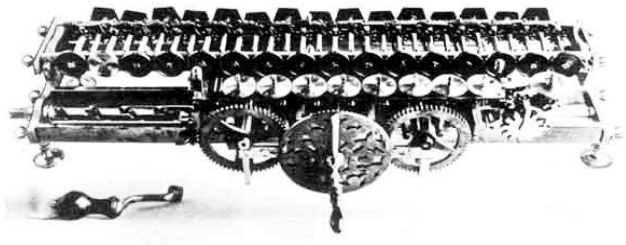
„Mivel a Colossus létezése is titok volt,
a világ úgy tudja, hogy az 1946-ban
megépített ENIAC volt az első
elektronikus számítógép.”
(T.Dénes Tamás: Titkos-számítógép-történet)

5.1. Összekapcsolt korongokból számológép

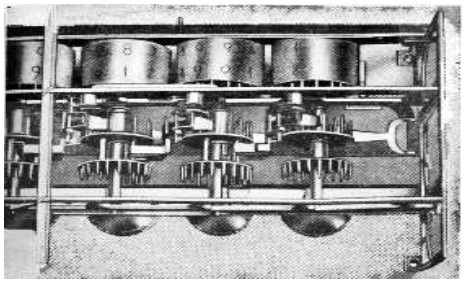
Gottfried Wilhelm Leibniz
(1646-1716)

Már a 17. században elindult az összekapcsolt rejtjelző korongok (kerekek) alkalmazásának egy másik irányzata. *Gottfried Wilhelm Leibniz*[39] (1646-1716) olyan szerkezetet alkotott, amelyben a kerekek nem egyetlen tengelyen helyezkedtek el, hanem több egymással fogaskerekekkel összekapcsolt kerék rendszerből épített olyan mechanikus gépet, amely alkalmas volt aritmetikai műveletek elvégzésére és az eredmény kijelzőn jelent meg.

Leibniz összeadó és szorzógépét 1671-1673 között készítette el. Ez az úgynevezett *Leibniz-kerék*, két részből állt, az egyik az összeadás (kivonás), a másik a szorzás (osztás) elvégzésére volt alkalmas, ugyanakkor a kettő össze is kapcsolódott. Ez a gép a technikatörténet során elsőként közvetlenül végezte el az osztást és a szorzást, valamint kiegészítő művelet nélkül a kivonást. A szorzás automatizálását Leibniz gépe ismételt összeadásokkal hajtotta végre (gépét Stepped Reckoner-nek, azaz Lépcsős Számláló-nak nevezte). Gépével tehát mind a négy alapműveletet el lehetett végezni.[40]



Leibniz összeadó és szorzógépe, a Leibniz-kerék



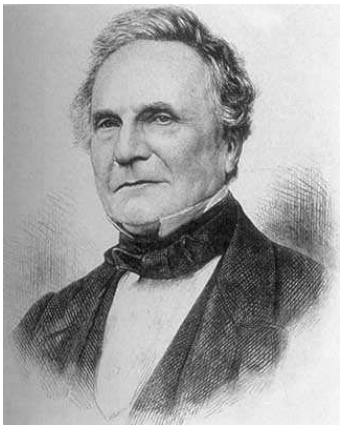
A Leibniz-kerék eredmény kijelzője

[39] Leibniz korának egyik polihisztora és kiváló matematikusa volt, így hát nem csodálkozhatunk, hogy behatóan foglalkozott a rejtjelzés és rejtjelfejtés tudományával. Lineáris egyenletrendszer alkalmazásával megfejtette például a kor nagy rejtélyét, az alkímista „rózsakeresztesek” titkosírását, amelyet a társaság alapítója Valentin Andreä (1586-1654) a *Christian Rosencreutz kémiai mennyegzője* című könyvében rejtett el.

[40] A számítógépek történetének eddig nem közismert rejTényeit mutatja be a [TDT 2003-k] kötet, amelyben Pascal és Leibniz számológépeiről és ezek belső felépítéséről is pontos képet kaphat az Olvasó. Különösen részletes leírások és képek találhatók ezekről a számítástechnika kezdeteit jelentő gépekről [TARJÁN 58]-ban. Az elmúlt évszázadokból felidézett gépek képei nem csupán a 21.század centrikus gondolkodásból zökkenthetnek ki egy pillanatra, hanem egyúttal olyan esztétikai élményt is nyújtanak, amely ma már az ipari termékekkel kapcsolatban nem igen tapasztalható.

A Leibniz-kerék lelke (a rotoros rejtjelző gépekhez nagyon hasonlóan!) az a fogazott henger volt, amelyet egy balra-jobbra mozgó másik henger működtetett, amely a helyiértékek átváltását is elvégezte. 1673-ban készülékét a legnagyobb érdeklődéssel fogadta mind az *Académie des Sciences* (Francia Tudományos Akadémia) Párizsban, mind a londoni *Royal Society* (Királyi Természettudományi Társaság).

Az ember és gép viszony humánus és egyben a társadalom szempontjából racionális megközelítését Leibniz több mint 300 éve így fogalmazta meg: *„Kiváló emberekhez valóban nem méltó, hogy rabszolga módra órákat vesztegessenek el olyan számítások elvégzésével, amelyeket bárkire nyugodtan rá lehetne bízni, ha gépet használna."*



Charles Babbage
(1792-1871)

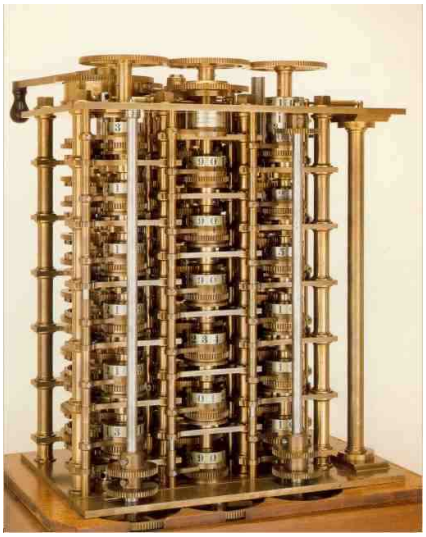
Leibniz eme napjainkig ható gondolata szinte rímpárként jelent meg a 19. században. *Charles Babbage* (1792-1871) angol matematikus és kriptográfus, akinek jelenősége a számítógépek keletkezéstörténetében csak ahhoz hasonlítható, ahogy Newton egészen új fizikai világképet teremtett. Azonban, amíg Newton (az anekdota szintjén) a tömegvonzás felfedezését egy almának köszönhette, addig a számítógép Babbage-féle elvét a csillagászati táblázatoknak köszönhetjük. Babbage így emlékezett vissza az inspiráló gondolatának megszületésére:
„Egy este Cambridge-ben, az Analitikai Társaság helyiségében üldögéltem, a fejemet, némileg álmodozva az asztalra hajtottam, ahol egy nyitott logaritmus táblázat hevert előttem. Amint a Társaság egy másik tagja bejött a szobába és meglátta, hogy félig alszom, odaszólt: — "nocsak, Babbage, miről álmodik?" amire azt válaszoltam, hogy — "azon gondolkodtam, hogy ezeket a táblázatokat géppel is ki lehetne számítani".

Babbage fantáziáját tehát ugyanúgy megmozgatta a már Leibniz óta halmozódó csillagászati táblázatok áttekinthetetlen tömege, ahogy az 1. fejezetben a *Találd meg!* gondolkodási modellel igyekeztünk megérteni a csillagképeket a hatalmas csillagrendszerekben. Ugyanez a rendszerező *Találd meg!* gondolkodás inspirálta Babbage gondolatait az automatikus számítógép kifejlesztésére.

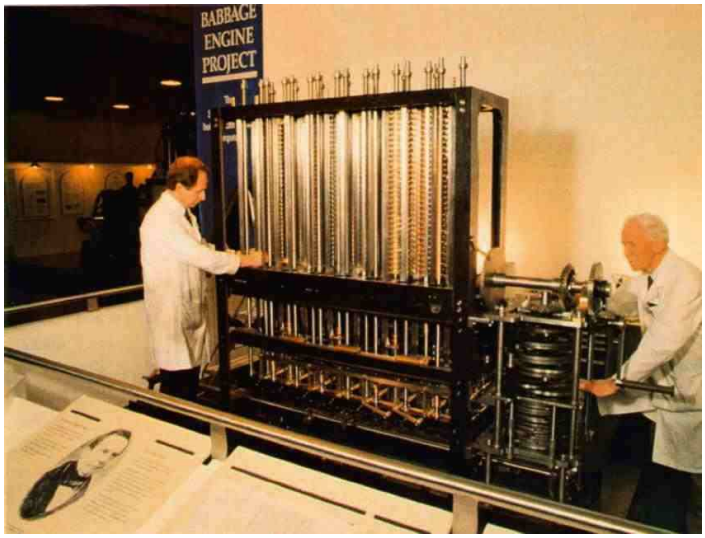
1822-ben levelet írt Sir Humphry Davy-nek, a Royal Society akkori elnökének, melyben közölte, hogy a matematikai és hajózási táblázatok kiszámításának fárasztó monotonitásáról és ennek az elviselhetetlen munkának az automatizálásáról ír egy értekezést *„On the Theoretical Principles of the Machinery for Calculating Tables"*[41] címmel, melynek elkészültével felolvasást tartana e témáról a Királyi Csillagászati Társaságban. A királyi kincstárhoz fordult anyagi támogatásért, amit a pénzügyminiszter 1823-ban jóváhagyott. Babbage azonban nem mérte fel a vállalt feladat nagyságát és 1827-ben egészségileg összeroppant. Gyógykezelésre külföldre utazott, majd hazatérve gyógykezeléséből újabb kincstári szubvenciót kért és kapott, amiből folytatta a *Defference Engine*-nek nevezett gépe építését.
Ám 1833-ban abbahagyta a munkát, és soha nem is fejezte be.[42] A Difference Engine azonban még így is képes volt nagy számtáblázatok automatikus elkészítésére, ami méltán váltotta ki a

[41] *„Táblázatok kiszámítására alkalmas gépek elméleti alapelveiről"*
[42] Ilyen abbahagyott formájában állították ki az 1862. évi Világkiállításon.

korabeli csillagászok elismerését. Babbage 1824-ben elsőként kapta meg a Royal Astronomical Society aranyérmét, melynek kapcsán Henry Thomas Colebroke így méltatta Babbage érdemeit: *„Nincs olyan tudományág, ahol ez a felfedezés oly rendkívüli haszonnal kecsegtetne, mint a csillagászatban... Nincs olyan tudomány, ami nehezebb számításokat igényelne a csillagászatnál; nincs olyan, amihez több segédtáblázatra lenne szükség; nincs olyan, amiben a számítási hiba olyan károkat okozna. ... Babbage úr találmánya a csillagász munkájának legfárasztóbb részét könnyíti meg, és új lendületet ad a csillagászati kutatásnak.”*



Babbage 1833-ban félbehagyott Difference Engine mechanikus számítógépének 2.000 alkatrészből álló részegysége (a teljes gép 12.000 alkatrészből állt volna)



Babbage születésének 200. évfordulójára, 1991-ben az angliai Science Museum (Kensington) elkészítette a Difference Engine egy komplett példányát, Babbage hátrahagyott rajzai alapján. A szerkezet méretarányait jelzi a Science Museum két munkatársa, akik a készülék mellett állnak.

A Difference Engine építésével Babbage rengeteg tapasztalatra tett szert, ezekre alapozva, még nagyratörőbb vállalkozásba fogott: egy általános mechanikus számítógép megtervezésébe, amelynek az Analitikus Számolómű (Analitical Engine) nevet adta. Ennek még a részletes tervei sem készültek el soha, csak tanulmányok, résztervek és makettek sokasága született 1834. és 1871. között.
Az Analitical Engine nem csak elvi konstrukcióját tekintve, de technikai megvalósításában is messze túlmutatott a 19. századi lehetőségeken. Az 1000 tengely és az 50 helyiértékes számokhoz tartozó fogaskerékrendszer (összességében mintegy 200 ezer alkatrész!) kivitelezése olyan technikai precizitást és gyártási kapacitást igényelt, amelyre az akkori ipar képtelen volt.

Napjaink számítástechnikába és digitalizációba született generációinak, amikor Neumann-elvű számítógépekről[43] beszélnek, érdemes a történeti hűség és Babbage szellemi nagysága előtt tisztelegve, megismerni az Analytical Engine szerkezeti felépítését!

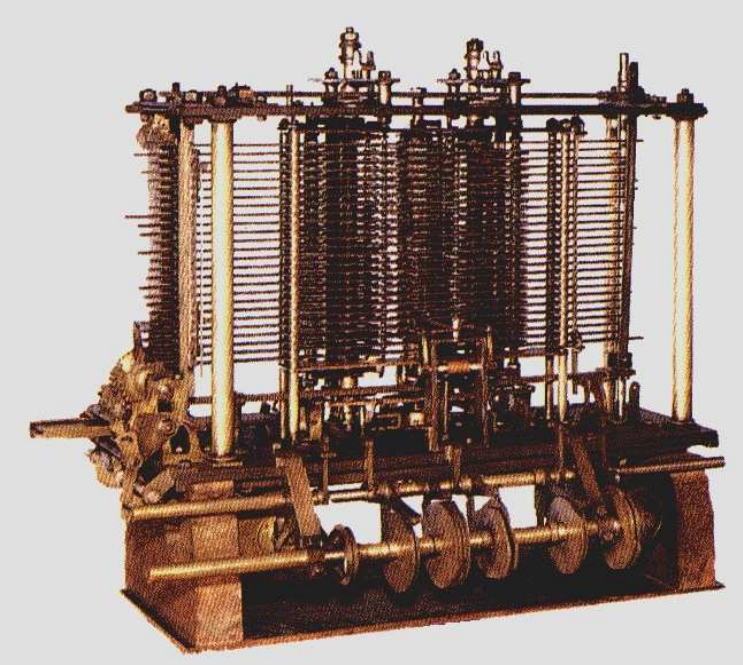
[43] Neumann-elvű számítógépnek, a programvezérlésű, program és adatok tárolására alkalmas memóriával rendelkező számítógépeket nevezik.

Az Analytical Engine két részből állt:

1. A *tárolóból*, ahol azok a változók helyezkedtek el, amelyekkel a műveleteket kellett elvégezni, valamint a más műveletek eredményeként keletkező numerikus értékek.

2. A *malomból*, amelybe mindig azokat az értékeket vitték be, amelyeken éppen valamilyen műveletet kellett végezni.

Minden formula, amelyet az analitikus géppel ki lehetett számíttatni, bizonyos algebrai műveletekből állt, amelyeket megadott betűkön lehetett végrehajtani, továbbá bizonyos módosításokból, a szóban forgó betűkhöz hozzárendelt numerikus értékektől függően. Ennek érdekében két kártyacsomagot kellett előállítani. Az első a végrehajtandó műveleteket határozta meg, ezeket Babbage *műveleti kártyáknak* nevezte, míg a második meghatározta azokat a speciális változókat, amelyeken az előzőeknek a műveleteket végre kellett hajtani, ezeket *változó kártyáknak* nevezte el.
Ebben az elrendezésben, ha bármilyen formulát ki akart számítani, a műveleti kártyacsomagot úgy kellett összerendezni, hogy a kártyák a műveleteket olyan sorrendben tartalmazzák, ahogy azok a formulában előfordultak. Ezután egy másik kártyacsomagot is össze kellett állítani, amely a változókat behívta a malomba, abban a sorrendben, ahogy dolgozni kívánt velük. Minden művelet elvégzéséhez így három kártyára volt szükség: kettő azon változókat és konstansokat, illetve ezek numerikus értékeit tartalmazta, amelyekre az előző műveleti kártya hatással volt, a harmadik pedig jelezte azt a változót, amelyben a művelet számszerű értékét el kellett helyezni. A gép a mozgó kartonszalagon tárolt utasítássort tapogatókarok segítségével olvasta le és így hozta működésbe a malmot és a tárolót.



Az Analytical Engine, amely teljes egészében sosem épült meg

Mély főhajtással kell elismernünk, hogy Babbage Analytical Engine gépe szerkezeti elemeit, azaz architektúráját tekintve (aritmetikai egység, operatív tár, vezérlő egység), pontosan megfelelt a napjainkban is használt, úgynevezett Neumann-elvű számítógépeknek. És íme a programvezérlés, sőt a program tárolás elvének (és gyakorlatának) leírása, amely annyira modern, hogy ha az elektromosság és egyéb technikai feltételek biztosítottak lettek

volna, Babbage nem csak a számológépek, hanem az egész modern számítástechnika atyjaként vonult volna be a történelembe. Mindez szinte pontosan 100 évvel Neumann János előtt![44]
Babbage gépe nem csak a programozhatóság elméleti lehetőségét rejtette magában, hanem *Ada Byron* (1815-1852), Lord Byron költő lánya (a későbbi Lady Lovelace) írt is programokat rá. Így őt tekinthetjük az első programozónak.[45]

Érdekes gondolatkísérletre és a számítástechnika kezdeteinek alapos átírására inspirál, ha elképzeljük: mi lehetett volna, ha a fizika és a technika fejlődésének órája csupán néhány évtizeddel jobban siet és Ampére, Faraday, Maxwell nem éppen Babbage kortársai, ha Edison nem az 1870-es 80-as években, Babbage halála után „néhány történelmi pillanattal" nyújtja be az elektromosság alkalmazására vonatkozó szabadalmait![46]

5.2. A gépi rejtjelfejtés kezdete

Babbage máig ismeretlen oknál fogva „titkos" kriptológus volt, ugyanis erre vonatkozó tevékenységét sosem publikálta, azt azonban fennmaradt jegyzeteiből és korabeli feljegyzésekből tudjuk, hogy a kriptológia tudományában is bámulatos eredményeket ért el. Ez a tevékenysége és számítógépeinek konstrukciói kölcsönösen hatottak egymásra.
Elsőként alkalmazta a matematikai formulákat és jelöléseket a rejtjelfejtésben. Megadta az általános megfejtését a polialfabetikus rejtjelzésnek, amely abban az időben már 300 éve a „le chiffre indéchiffrable" (a megfejthetetlen rejtjel) kitüntető elnevezést hordozta.

Önéletírásában, *Passages from the Life of a Philosopher* (Szemelvények egy filozófus életéből) írta ezt a kriptográfusok körében ma is gyakran idézett gondolatot: *„Alapelvként fektethető le az, hogy nem érdemes annak megfejthetetlen rejtjel készítésével foglalkozni, aki maga nem fejtett meg már nehéz rejtjelet."*

Egészen újszerű volt, hogy Babbage az algebrát alkalmazta a kriptológiában. Sok jegyzetében találhatók olyan formulák, amelyekkel igyekezett rejtjeleket megfejteni és amelyek átláthatóbbá tették a rejtjel struktúráját. A képletekben alkalmazott betűk, kódtáblázatokban szereplő értékeket jelöltek, amelyeket Babbage táblázatkezelő gépei igen gyorsan tudtak kezelni, a köztük definiált aritmetikai műveletekről nem is beszélve. Ezen a ponton világossá válik a gépi rejtjelfejtés és a számítástechnika kölcsönhatása.

---

[44] Babbage munkásságát, Nagy Károllyal és Ada Byronnal való kapcsolatát, tehát a számítástechnika valódi gyökereit részletesen tárgyalja [TDT 2005-k] 10. fejezete és a rejtjelfejtéssel való kapcsolatát a [TDT 2003-k] kötet.

[45] Ennek tiszteletére róla nevezték el az Ada programnyelvet.

[46] Az első működő differenciagépet Babbage gépének egyszerűsítésével 1853-ban készítette el Pehr Scheutz és fia Edvard Scheutz. Ez a gép harmadrendű differenciákat és 15 jegyű számokat kezelt. Christel Hamann tovább tökéletesítette a berendezést, és segítségével 1910-ben tízjegyű logaritmustáblázatot jelentetett meg. Differenciagépeket egészen az 1940-es évekig használtak matematikai táblázatok készítésére. Már az 1820-as években, Babbage eredeti elképzelései szerint, gépe a számítások eredményeit pontozóval közvetlenül a nyomda által használható fémlemezbe írta volna. Babbage eme terve óriási jelentőségű volt, hiszen a nyomdai kézi szedés teljes kiküszöbölését jelentette volna, ami rendkívül felgyorsítja a nyomdai munkafolyamatot és ami ennél is lényegesebb, elkerülhetővé teszi a szedési hibákat. E gondolata is másfél évszázaddal megelőzte korát, mivel a számítástechnika fejlődése csupán az 1980-as évek óta produkálja azokat a hardver és szoftver eszközöket, amelyek alkalmasak arra, hogy a szövegszerkesztő, vagy táblázatkezelő programok eredményeit közvetlen nyomdai „levilágításra" alkalmassá tegye.

Érdekes párhuzam figyelhető meg: ahogy Thomas Jefferson rejtjelző hengere óriási lendülettel indította útjára a rejtjelzés gépesítését, úgy hatottak Babbage gépei a rejtjelfejtés gépesítésére. Tulajdonképpen a 19. és 20. századi kriptográfia és kriptológia óriási léptékű gépesítése, ezeknek a berendezéseknek a kisebb-nagyobb továbbfejlesztése.

A távíró és a morze ABC elterjedésével az üzenetek nagyon gyorsan jutottak el a címzetthez, de mivel az a távírókezelők kezén futott át, az üzenetet először titkosítani kellett, és csak utána továbbítatni. Ez rákényszerítette a rejtjelezőket a bonyolultabb, de megbízhatóbb több ábécés Vigenére rejtjelzés[47] alkalmazására. A 4. fejezetben bemutattuk, hogy pontosan ez a felismerés inspirálta a rejtjelzés gépesítését.

Babbage 1854-ben általános elméletet és módszert dolgozott ki az addig megfejthetetlennek tartott Vigenére rejtjelzés megfejtésére[48], de az eljárását nem publikálta. Felfedezésére csak a 20. században derült fény, mikor néhány tudós átvizsgálta Babbage bőséges jegyzetanyagát. Időközben tőle függetlenül rátalált a módszerre a porosz hadsereg egyik nyugállományú tisztje, Friedrich Wilhelm Kasiski (1805-1881) is. Korszakos felfedezését 1863-ban Die Geheimschriften und die Dechiffrir-kunst (A titkosírás és a rejtjelfejtés művészete) című dolgozatában publikálta, így a módszer azóta az Ő nevéhez kapcsolódik.
Mai fejjel gondolkodva, igazán érdekes kérdés, hogy „Babbage vajon miért nem tette közzé e zseniális eredményét?"
Pontos információk hiányában csak az ismert tények mozaikjaiból rakhatjuk össze azt a felettébb izgalmas gondolatsort, mely szerint ez a módszer tökéletesen illeszkedett Babbage differencia és analitikus gépeinek logikájához. Így jogosan feltételezhetjük, hogy 1854-től kezdve nem okozott problémát az akkori viszonyok között elképzelhetetlenül rövid idő alatt megfejtenie tetszőleges polialfabetikus (Vigenére) titkosítással rejtjelzett szövegeket. Most már örök titok marad, de az angol titkosszolgálatok történetében nem egyedi eset[49], hogy korszakos felfedezések maradtak hosszú időn át teljes titokban, így szolgálva hazájuk érdekeit az üzleti, esetleg politikai presztizs érdekekkel szemben[50]. Lehetséges tehát, hogy Babbage a brit hírszerzés nyomására tartotta titokban munkáját?!

5.3. Az Enigma megfejtése, avagy a modern számítástechnika születésének titka

Ahogy a Vigenére rejtjelzésről 300 éven át, úgy az Enigma rejtjelző gépről is a német vezérkar azt hitte, hogy megfejthetetlen. Ezt a túlzott biztonságérzetet táplálta például az osztrák rejtjelfejtő szolgálat vezetőjének, Figl ezredesnek 1926-ban megjelent nyilatkozata, amelyben az Enigmáról, mint abszolút biztos, megfejthetetlen berendezésről ír. Figl véleményét később 1942-ben Safford az amerikai tengerészet rejtjelfejtő szolgálatának

[47] Blaise de Vigenére (1523-1596) talán minden idők leghíresebb, úgynevezett több ábécés rejtjelző rendszerét dolgozta ki. Általános elméleti megfejtése három évszázadon át reménytelennek tűnt. (lásd [TDT 2004-k] 13. fejezet)
[48] Ezen a ponton fel kell hívni a figyelmet arra, amit a „megfejthetetlenség" téveszméjének álbiztonsága jelent. Ahogy Babbage és Kasiski több évszázad után szétzúzta a Vigenére rejtjelzés megfejthetetlenségének mítoszát, ugyanígy bekövetkezett (jóval rövidebb idő alatt) ugyanez az Enigmával és lehet, hogy nem kell évszázadokat várni a napjaink információbiztonságának alapjául szolgáló RSA rejtjelzés általános megfejtésére.
[49] Erre a 20. századi történelemben, így a RejTények több későbbi fejezetében is döbbenetes példákat talál a kedves Olvasó (pl. az Enigma megfejtése, a Navajo kódbeszélők).
[50] Ennek ékes példája a számítástechnika története, amelynek kettős értelemben vett titkosságát fedi fel jelen szerző Titkos-számítógép-történet című kötetében.

vezetője is osztotta. Ez annál is pikánsabb, mert 1942-ben az angolok már folyamatosan fejtették az Enigmát.

Alan Mathison Turing (1912-1954)

A modern számítógép történet kezdetét nyugodtan nevezhetjük „titkos", vagy akár „angol vonalnak", amely *Alan Mathison Turing* (1912-1954) nevéhez köthető és kísértetiesen hasonlít 100 évvel korábbi elődjének C. Babbagenek a titkos rejtjelfejtési munkásságához.

1937-ben megjelent [TURING 37] cikke nagy feltűnést keltett. Ebben a cikkében vezette be az *absztrakt gép* fogalmát, amelyet máig is *Turing-gépnek* neveznek. A Turing-gép tulajdonképpen „egy darab absztrakt matematika", és bár elnevezése erre utal, nem technikai eszköz. A Turing-gép, mint minden igazán zseniális elképzelés, könnyen leírható:

Képzeljünk el egy automatát, amely végtelen hosszú szalagból, egy ettől független vezérlőegységből és egy olvasó–író fejből áll. A szalag egymás melletti mezőkre van felosztva, mindegyiken egy-egy jel áll; ezek a jelek egy véges ábécé elemei és véges sok kivétellel minden mezőn az a speciális jel található, ami az „üres" mezőt jelöli. (A jelek egyike annak a jelölésére szolgál, hogy az illető mező után következő valamennyi mező üres.) Az olvasó–író fej minden lépésben a szalag egyik mezeje fölött áll, kezdetben a szalag legelső mezeje fölött. A vezérlőegység véges sok állapot valamelyikében van, kezdetben a START állapotban; mindegyik lépésben a fejjel leolvastatja az éppen alatta lévő mező jelét és attól, valamint saját állapotától függően a következőket teszi:
átkerül egy másik állapotba, felülíratja az aktuális mezőt és a fejet az attól eggyel jobbra vagy balra álló mező fölé állítja vagy helyben hagyja. A gép akkor áll meg, amikor vezérlőegysége a STOP állapotba jut.

Ebben az absztrakt definícióban benne van a jelek hosszabb jelsorozatokká való összeláncolásának és így tetszőleges bonyolultságú utasítások végrehajtásának, valamint a végrehajtás közben keletkezett jelek (adatok) tárolásának lehetősége. A Turing-gép tehát valóban egy absztrakt automata, amit mai szemmel nagyjából úgy képzelhetünk el, mint egy végtelen nagy tárolókapacitással rendelkező (és bármilyen hosszú ideig futni tudó) „célszámítógépet", mellyel egyetlenegy „gyárilag beépített" program hajtható végre. Ebből azt is gondolhatjuk, hogy minden, intuitív értelemben vett „programnak" megfelel egy Turing-gép (és viszont). Ez a sok tapasztalattal és elméleti eredménnyel valószínűsített és ezért általánosan elfogadott elképzelés a *Church-tézis*. Ennek értelmében tehát a Turing-gép tökéletes modellje a program fogalmának. Ugyanekkor Turing definiálta a „kiszámítható számot", mint olyan valós számot, amelynek akárhányadik tizedesjegye előállítható egy alkalmas Turing-géppel, az üres szalagból kiindulva.
Turing gépekkel kapcsolatos munkásságának legnagyobb jelentősége, hogy megelőzte saját korát, hiszen leírta a modern számítógép lényegét jóval azelőtt, hogy annak technikai feltételei ebben az időben reálisan adottak lettek volna.[51] Turing 1936 és 1938 között játszott a gondolattal, hogy tervez egy működő számítógépet. Ezidőtájt azonban tevékenysége egészen új fordulatot vett, ugyanis kapcsolatba került a *Government Code and Cypher School*-al (az

[51] Tulajdonképpen Babbage analitikus gépével is ez történt.

angol titkosszolgálat rejtjelfejtő szolgálata), akik felkérték, hogy segítsen a német Enigma rejtjelző rendszer feltörésében.

Hitler ugyanis elkezdte Németország újrafelfegyverzését, és a Wehrmacht kriptológiai szakértői úgy döntöttek, hogy az Enigma kellő garanciát nyújt a titkosításban, ezért elkezdték ellátni vele az egyre terjedő hálózatukat. A II. világháború alatt az Enigma egy hordozható, elemes, lámpás, fadobozos, írógép méretű és súlyú változata szolgálta Németország hadseregét, légi- és tengeri erejét. Becslések szerint 1942 végére a németek legkevesebb 100.000 Enigmát gyártottak le. Valamennyi katonai parancsnokságon, Luftwaffe-támaszponton, hadihajón, tengeralattjárón, kikötőben, nagyobb vasútállomáson, SS-osztagnál és Gestapo-központban volt belőle. Soha, egyetlen nemzet sem bízta még addig titkos rádiótávirat-forgalmának ekkora részét egyetlen rejtjelező szerkezetre.
Ahogy azt a 4. fejezetben megmutattuk, az Enigma-t nem kevesebb, mint 1.054.560•150 billió módon lehetett beállítani a rejtjelezést megelőzően. Az Enigma eme beállítási variabilitása olyan biztonságérzetet sugárzott, hogy a németek még az 1960-as, 1970-es években is nyugodtan használták az Enigmákat, mivel továbbra is megfejthetetlennek hitték. Ne felejtsük el, hogy ezekben az időkben egyáltalán nem voltak mai értelemben számítógépek!

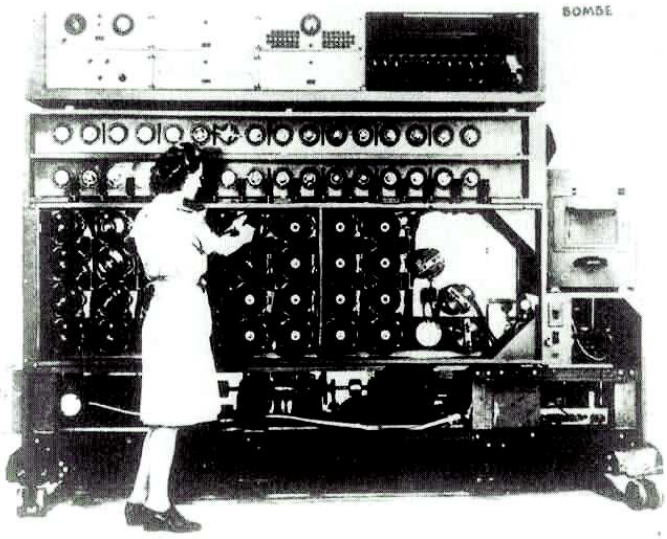
Különös paradoxon, hogy amíg az Enigma a német rejtjelzés, addig a megfejtés az angol rejtjelfejtés, az ULTRA project (az angol rejtjelfejtő szolgálat minden idők legtitkosabb projectje) sikertörténete. A megfejtés koncepciója és az ehhez szükséges nagy kapacitású gépi háttér, amely egyben egy egészen új számítógép kifejlesztéséhez vezetett, A.M. Turing nevéhez fűződik.

Lengyelországban a korai kutatások az Enigmával kapcsolatban már 1928-ban elkezdődtek, szinte a német hadrendbeállítással egy időben. A Lengyel Kriptológiai Hivatal három fiatal matematikusra bízta a feladatot (*Marian Rejewski, Jerzy Rozycki, Henryk Zygalski)*, akik 1932. szeptember 1-jén kezdték el a munkát a Kriptologiai Hivatalnál Varsóban. Segítségül kaptak egy régi üzleti célú Enigmát, ami jóval kevesebbet tudott, mint a katonai verzió.
Mindezek ellenére az analízis 1933. januárjában teljesen befejeződött. A vizsgálatok eredményeként megállapították, hogy az Enigma rejtjelző rendszerének megfejtése két részből áll. Az egyik magának a kódoló-gépnek az elméleti felépítése. A legfontosabb a belső huzalozás megállapítása, ezután a komplex egymásrahatások vizsgálata az egyes szerkezeti egységek között (rotorok, dugaszoló-tábla stb...). A megfejtés második része az, ahogyan a beállításokat közlik az üzenet fogadójával (mai szóhasználattal ez a „kulcscsere"). Az elméleti modell kipróbálásához, a temérdek variáció teszteléséhez azonban a lengyeleknek nem volt megfelelő méretű számítási kapacitásuk, így az igazi megfejtés félbe maradt.
A három lengyel rejtjelfejtő matematikus a német megszállás elôl Franciaországba menekült, majd Franciaország megszállása előtt Angliába. Az angol rejtjelző szolgálat megszervezte az addigi idők legnagyobb, legjobban szervezett és legmélyebben rejtett titkos projektjét ULTRA néven, amelynek célja az Enigma megfejtése volt (lásd [HODG 83],[WINT 96],[ENEV 94]) és működési helyéül egy külön birtokot választottak Londontól 40 mérföldre, ez volt a mára híressé vált Bletchley Park.

Az angoloknak 1939. július 25-én egy titkos megbeszélésen a lengyel fél átadott egy Enigma másolatot. A Bletchley Parkot álcázásként elnevezték *„Goverment Code and Cyper School"*-nak (viccesen „Golf Cheese and Chess Society"-nek hívták – Golf Sajt és Sakk Társadalom). Matematikusokat, sakkmestereket, nyelvészeket toboroztak egész Nagy Britanniából,

legtöbbjük a Cambrige University-ről jött. A „hut”-okban (barakkokban) folyó tevékenység három fő részből állt: *forgalom-analízisből, irány-meghatározásból és megfejtésből.*

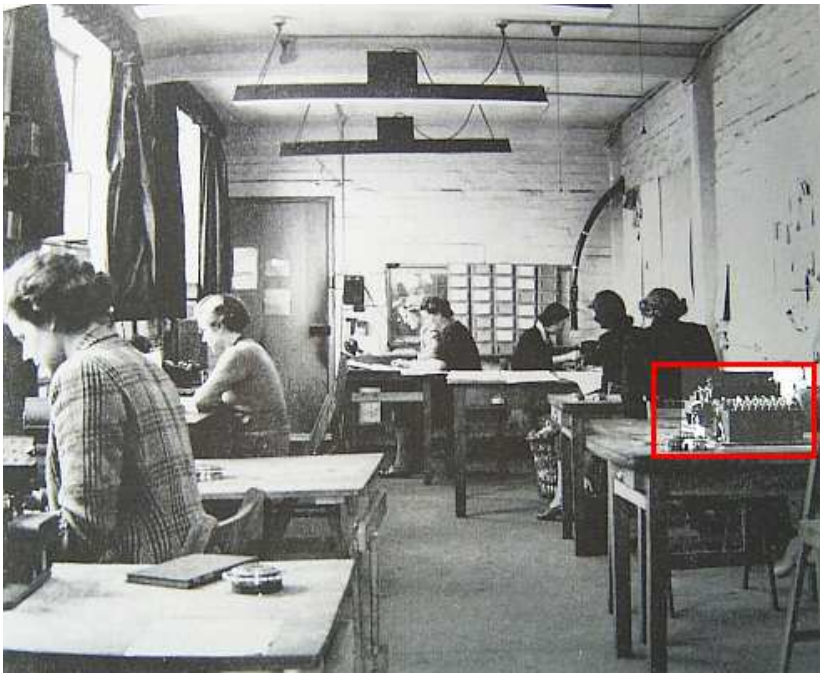
Amikor 1939-ben kitört a II. világháború, Turing azonnal teljes idejét a Bletchley Park-nak szentelte. Briliáns ötletei a kódok megfejtésében és az elektronikus rejtjelfejtő gép kifejlesztésében nagyban hozzájárultak az Enigma rendszer feltöréséhez.
Először 1940-ben fogott el az angol rendőrség egy Enigma titkosító géppel kódolt német rádióüzenetet. Több hónapos kitartó, intenzív munka után a kódtörők sikeresen megfejtették a titkosított üzeneteket, noha tudjuk, hogy magát a gépet 1939. nyarán látták először. Az egyes üzenetek kézzel történő dekódolása azonban minimum hat hetet vett igénybe, így mire megfejtették az üzenetet, az már teljesen érvényét vesztette.
Turing a „lengyel csoport” korábbi munkájára alapozva megtervezte azt a rejtjelfejtő gépet, amely 1940 nyarától dekódolta az összes üzenetet, amelyet a német légierő az Enigmával rejtjelezve küldött. Ezt a berendezést *Bombe*-nak nevezték el.



A Bombe rejtjelfejtő gép (1940)

A sikerben rendkívüli szerepet játszott a párhuzamos aritmetika[52], amelyet Turing ebbe az óriási gépezetbe tervezett. A Bombe méretei hasonlítottak Babbage rekonstruált gépéhez. Ebből az 1 tonnás, 2,1 méter széles, 2 méter magas és 0,6 méter mély gépezetből körülbelül 200 darab készült a II. világháború öt éve alatt.
1941. közepén Turing módszere az elfogott rejtjeles üzenetek feldolgozásával lehetővé tette a német haditengerészet rejtjeles üzeneteinek megfejtését, gyakorlatilag a német vezérkarral egyidőben. Ekkor a Bletchley Parkban szigorúan titkos körülmények között már majdnem 10 ezer embert foglalkoztattak. A gigantikus mennyiségű elfogott (főleg rádió) üzenet előkészítését a gépi feldolgozáshoz, a gépek kezelését és számtalan rutin feladatot kézi munkával végeztek.

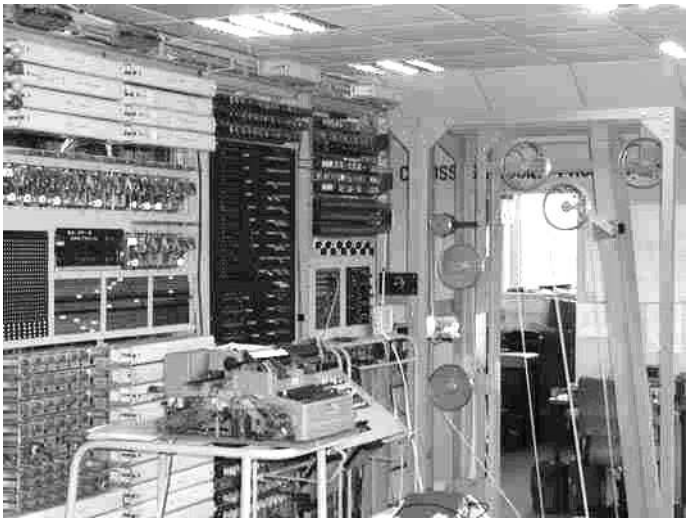
[52] A párhuzamos aritmetika az emberi asszociációhoz hasonlóan, bizonyos műveleteket (pl. két számsorozat összehasonlítása) egyszerre, azaz párhuzamosan végez. Ezzel ellentétes a szekvenciális működés, amely egymásutáni elemi léésekre bontja fel a műveleteket. Így működnek a napjainkban széles körben elterjedt, úgynevezett Neumann-elvű számítógépeink.



Munka a Bletchley Park egyik kódfejtő helyiségében. A jobboldali asztalon egy Enigma rejtjelző gép látható (bekeretezve)

A Bombe sikeres rejtjelfejtési alkalmazása és a tömegesen megfejtett titkos üzenetek tapasztalatai, Turing tervei alapján, a világ valóban első elektronikus számítógépének, a *Colossus*-nak a létrehozásához vezettek. *Max Newman* matematikus és *Tommy Flowers* mérnök 1943. márciusában kezdték el a Colossus kivitelezési terveit és még abban az évben fel is építették a gépet, 1944 januárjában beüzemelték a Bletchley Parkban és azonnal sikeresen dekódoltak vele egy valódi német rejtjeles üzenetet. A Colossus segítségével órák alatt fejtették meg azokat az üzeneteket, melyeken korábban hetekig dolgoztak. Így az angolok a lehallgatott és szinte a németekkel egyidőben dekódolt rádió-üzenetek birtokában szervezhették hadi tevékenységüket. A háború végén már tíz, továbbfejlesztett Colossus dolgozott az üzenetek dekódolásán, és a német vezérkar 63 millió karakternyi titkosított üzenetét fejtették meg a háború alatt.

Mégis az a szűkszavúság, amely ezt a sikertörténetet fedte, annak köszönhető, hogy a Colossus megtervezése, létrehozása és főleg üzemeltetése (szinte csak rejtjelzési és rejtjelfejtési feladatokra használták!) szigorúan titkos körülmények között történt.
Ma már tudjuk, hogy a Colossus 1500 elektroncsövet tartalmazott és 5 kHz órajellel dolgozott, így másodpercenként 25000 karaktert tudott feldolgozni. A háború után mindegyiket megsemmisítették, a gépek közül nyolcat helyben szétszereltek, kettőt pedig Londonba, majd Cheltenhamba vittek. 1960-ban még a gépek tervrajzait is megsemmisítették. Akkoriban még létezésük ténye is titoknak számított, sőt műszaki leírásukat a haditermékekre vonatkozó törvény alapján 50 évre titkosították. Mivel ezt a titkot az angolok lelkiismeretesen megtartották, ennek természetes következménye, hogy pontosan a kezdeti ötven év vált homályossá a modern számítástechnika történetében.



A Colossus számító és rejtjelfejtő gép, már 1500 elektroncsövet tartalmazott (1944)

Turing gépei az akkori viszonylatban óriási kapacitásukat szinte kizárólag a rejtjelzett német üzenetek megfejtésére használták, tökéletes titoktartás közepette. Hogy az ULTRA projectben résztvevôket milyen titoktartás övezte arra jellemző, hogy például Henrik Zygalskiról, aki a University of Surrey (Guildford) tanára lett a háború után, még az 1970-es években sem tudták kollégái, hogy részt vett az ULTRA-ban. Hogy mi értelme volt jóval a háború után is e szigorú titkolódzásnak? Ugyanaz, ami a háború alatt.

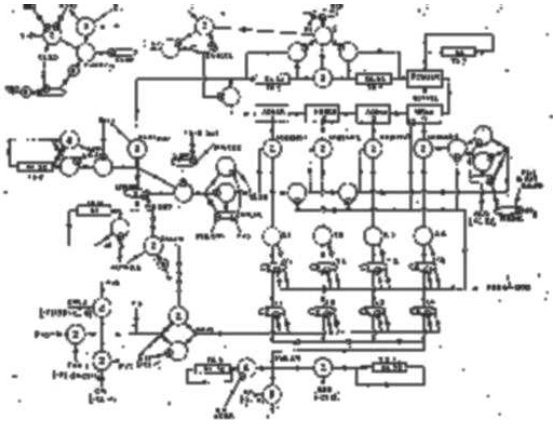
A szövetségesek sikere ugyanis éppen abban rejlett, hogy a németek számára semmilyen jel sem utalt arra, hogy a „megfejthetetlen" Enigmával rejtjelzett üzeneteiket az angolok már régóta rutinszerűen fejtik. Így ezt a titkosító „csodafegyverüket" egészen az 1970-es évek elejéig használták, ami persze az angol titkosszolgálatnak igen előnyös volt. A Colossus terveit a titkosítás elrendelésének megfelelően csak a háború befejezését követő fél évszázad elteltével hozták az angolok nyilvánosságra.

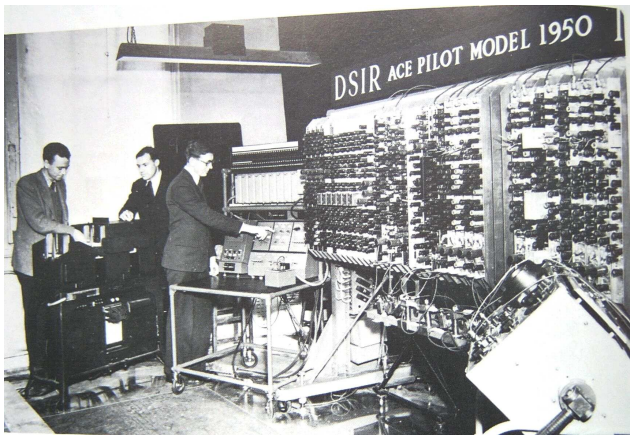
Mivel a Colossus létezése is titok volt, ma a világ úgy tudja, hogy az 1946-ban az USA-ban megépített ENIAC volt az első elektronikus számítógép, noha a Colossus (amint az előzőkből kitűnik) nemcsak korábban épült meg, de nagyobb kapacitással és párhuzamos aritmetikával is bírt, így felépítését tekintve is jóval előremutatóbb volt.

Meg kell állapítanunk, hogy az 1940-es évek, azaz a II. világháború elején egyedül A.M. Turing látta át a számítások megújításának lehetőségét: az univerzalitás, a programozhatóság, a tárolt program kihasználása, a nem numerikus alkalmazások, a mesterséges intelligencia fontosságát. Az olyan gép elképzelése, amely e követelményeknek mind megfelel, nagyon idegen volt 1945-ben az egész világon. Ám tíz évvel később, 1956-ban Howard Aiken, a harvardi egyetem számítógép főkonstruktőre így írt:
„Ha kimondjuk, hogy egy olyan gép logikai alapjai, amelyek differenciálegyenleteket oldanak meg, azonosak annak a gépnek a logikájával, amely törvénytervezeteket készít a minisztérium számára, ezt úgy tekintem, mint a legbámulatosabb egybeesést amellyel valaha találkoztam." De tényleg, hogyan mondhattuk ezt ki? E bámulatos, bár közel sem véletlen egybeesés

következik abból az alapelvből, amelyet Alan Turing már 1936-ban leírt, vagyis az „univerzális Turing-gép” konstrukciójából.”

1945-ben Turing a London külvárosában levő National Physical Laboratory (NPL) felkérésére tervet készített egy elektronikus számítógépről, a project neve: *Automatic Computing Engine* (ACE). A Colossus megépítésekor nyert tapasztalatainak birtokában részletekbe menő és számos rajzmelléklettel illusztrált dokumentációt készített rövid idő alatt, amelyet 1946. márciusában elfogadtak. Minden úgy nézett ki, hogy az ACE meg is valósul. Azonban mégsem így történt.





Turing Automatic Computing Engine (ACE) számítógép tervrajzának részlete és az 1950-ben beüzemelt számítógép

Turing terve ugyanis, mai terminológiával élve 6 kbyte memóriát tartalmazott, és ez túl nagyratörő elképzelésnek bizonyult. 1946 vége felé az NPL nyilvánosságra hozott egy sajtóközleményt, amely tisztázta, hogy Turing terve egy igen fontos nemzeti project és kiemelkedő találmány.

New N.P.L. Wonder

ELECTRIC BRAIN TO BE MADE AT TEDDINGTON

34 YEARS-OLD DESIGNER TALKS TO *SURREY COMET*

£100,000 A.C.E. WILL BE OBSOLETE BEFORE COMPLETED

SOME of the feats that will be able to be performed by Britain's new electronic brain, which is being developed at the N.P.L., Teddington, were described to the SURREY COMET yesterday by Dr. A. M. Turing, 34 year-old mathematics expert, who is pioneer of the scheme in this country.

The machine is to be an improvement on the American ENIAC, and it was in the brain of Dr. Turing that the more efficient model was developed.

A sajtóközlemény magyar fordítása: „Hőstettet voltunk képesek véghezvinni a Brit elektronikus agy révén, melyet az NPL-ben fejlesztettek ki, Dr. A.M. Turing 34 éves matematikus úttörő terve alapján. A gép tökéletesebb, mint az amerikai ENIAC, és mindez Dr. Turing agyában született meg.”

A NPL menedzsmentjének merev álláspontja miatt sem 1947-ben, sem 1948-ban nem épült meg Turing számítógépe. Ennek következtében az ACE csak 1950-ben, tehát 4 évvel az

ENIAC megépítése után készült el, annak ellenére, hogy Turing zseniális tervei jóval előbb készen voltak (amint arról a fenti újságcikk is tanúskodik).[53]
Egy másik tényező az volt, hogy a rejtjelfejtésről szóló titoktartás miatt Turing egyáltalán nem adhatta ki az erre vonatkozó temérdek és korszakos jelentőségű tapasztalatait. Hiszen ô a nyilvánosság előtt mint egy elméleti egyetem egyszerű matematikusa jelent meg (akárcsak Zygalski!). A továbbiakban Turing nem reklámozta a számítógépre vonatkozó elképzeléseit, csupán 1947-ben írt egy cikket *The Theory and Practice of Computing* címmel, amely tartalmazta az új elképzeléseit (de ezzel csupán a szakmai hírnevét gyarapította). Ebben az időszakban nagyon nyomasztotta és mérgesítette az NPL döntése és az, hogy elveszített egy „futamot" az idővel való versenyben.1947-ben visszatért Cambridge-be, ahol olyan, a számítógépektől és a matematikától látszólag távoli területeket kezdett tanulmányozni, mint a neurológia és a pszichológia. De nem felejtkezett el a számítógépekről sem és számítógépes programozási „kódokat" készített.

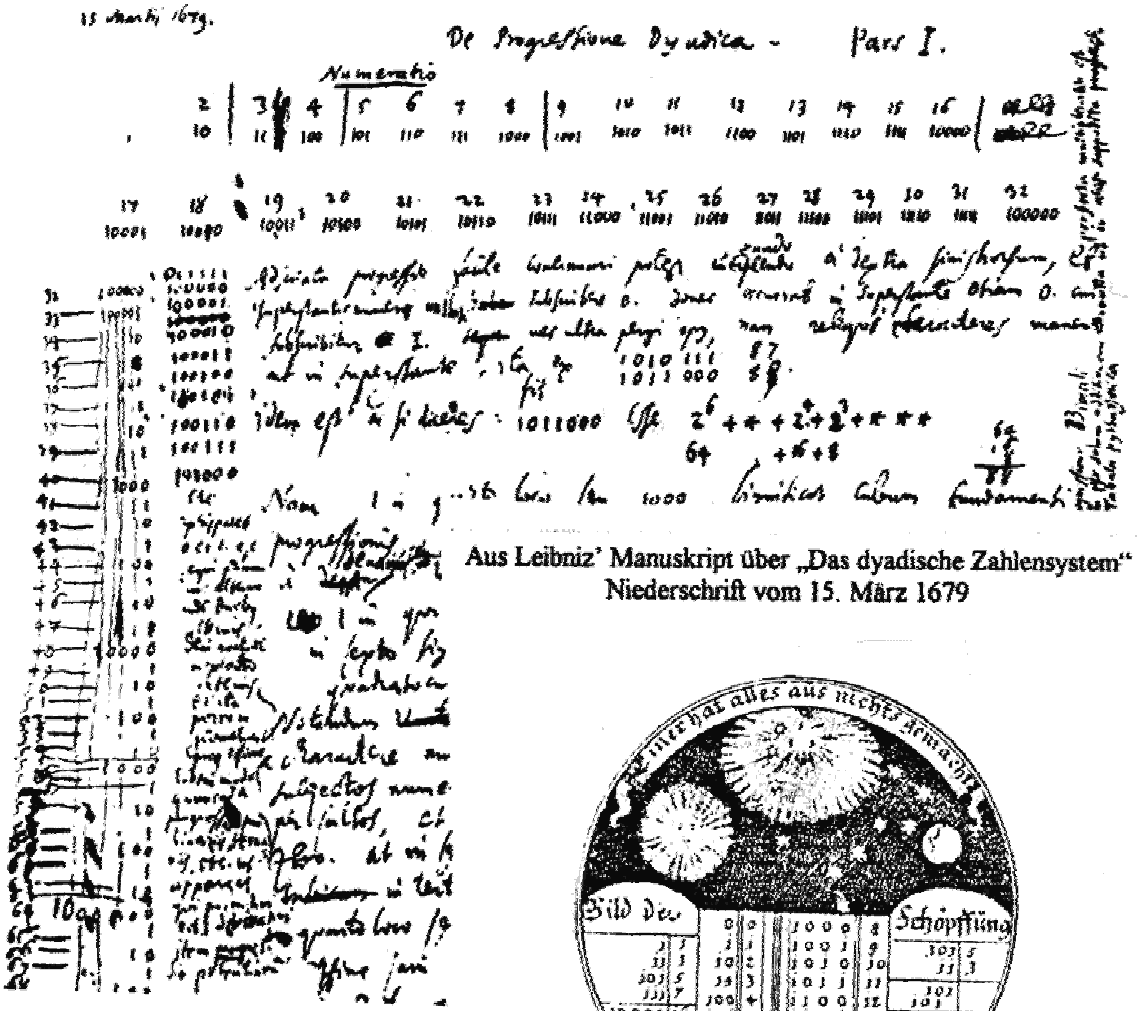
Az ACE-t valójában sohasem számolásra, inkább az emberi agy utánzására képzelte el. Turing így írt erről: *„Csak egyszer kell kitalálni, hogy miként működjön, aztán elfelejteni, hogy valójában mi történik odabenn."*
Látszólag minden lépéssel az emberi agy működését utánozta, de ki tudta akkor, hogy az agy hogyan működik? (Ez még a mai napig is helytálló kérdés.) Turing technikai javallatán túl lefektette filozófiai látomását, amely végképp túlmutat egy olyan gép építésén, ami sok, bonyolult összegzést végez. Erről a Turing-teszt fejezetben részletesen szó lesz.

Nem csak a modern számítástechnika gyökerei táplálkoznak Turing munkásságából, de a napjaink e-kommunikációs társadalmának és e kötet címében jelzett Globális titoknak *az alapját képező internet is Turing gondolataiból bújt elő!*
Ugyanis Turing már az 1946-os ACE jelentésében felvetette, hogy az ACE számítógép alkalmas távoli felhasználók összekötésére telefonkapcsolattal. Tehát ő előre látta a számítástechnika és a telekommunikáció összekapcsolását, jóval előbb, mint mások. Turing sajnos korai halála miatt, már nem tudott e korszakos gondolatának megvalósításával foglalkozni, de egyik NPL-beli kollégája, *Donald W. Davies* lett a *csomagkapcsolás"* alapelvének úttörője és így az első csomagkapcsolt hálózat, az ARPANET kifejlesztője, amely a mai internet kezdetét jelentette.

[53] Az ACE dokumentációja ma a londoni Science Nuseum egyik féltve őrzött anyaga.

5.4. Vissza Leibnizhez, akit megbabonázott a 2-es számrendszer

Leibniz a mennyiségek általános tudományában, a matematikában is a még általánosabbat kereste, és megjósolt egy még ma is csak részben megvalósult tudományt, amely már nem a mennyiségek, hanem a minőségek tudománya lesz. Ezt a szimbólumokkal leírható, a minőségek (struktúrák) kapcsolatait kifejező matematikát a kombinatorikában vélte felfedezni, azaz a „kombinatorikus művészet" a sorrend, a viszony, a hasonlóság, általában a szimbólumokkal kifejezhető minőségi kapcsolatok tudományában. Ezt képzelte az évezredek óta a mennyiségeket tárgyaló matematikát magában foglaló, új matematikának.
Leibniz főleg azért foglalkozott matematikával, hogy abban meglelje a gondolkodás legáltalánosabb törvényeit, ezért természetesnek tűnik, hogy a 2-es számrendszert is igyekezett beilleszteni filozófiai-teológiai rendszerébe.

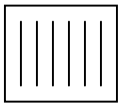


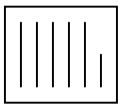
Leibniz kéziratának egy lapja, amelyben a 2-es számrendszer „teológiáját" írja le

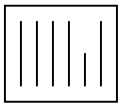
Csodás párhuzamot látott abban, hogy amint az összes mennyiség számokkal történő felírásához csak az *„egy"* és a *„semmi"* szükséges, ugyanúgy a Biblia teremtéstörténete szerint Isten a világot a semmiből teremtette. Tehát Leibniz szerint csak két ősprincípium

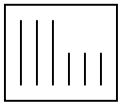
létezik: *Isten és a Semmi*, ezekből jött létre a *Minden (Mindenség)*, pontosan úgy, ahogy az *1* számjegy a nullával (a semmivel) létrehozza az összes számot.

Ezt az analógiát kifejtve, elragadtatással írta 1696-ban kelt levelében Rudolf Ágost hercegnek a következőt: *„Essentiae rerum sunt sicut numeri.”*[54] De hiszen ez pontosan a pütagoreusok több mint 2000 évvel korábbi, számmisztikát megalapozó filozófiája! Ma már a legtöbben csak mosolygással gondolnak a számmisztika tanaira, de ki gondolná, hogy sok más matematikai eredmény mellett a napjaink e-társadalmának technikai alapját képező 2-es számrendszer is egy ilyen „téveszméből” fogant. Egy évvel később, 1697-ben Leibniz egy Joachim Bouvet nevű jezsuita hittérítővel váltott levélből értesült az i.e. 8-7. században Kínában keletkezett nevezetes *Öt könyv* létezéséről. Az *Öt könyv* közül a kínai kultúrára legnagyobb hatással volt az *I Csing* (*Az átváltozások könyve*), melyben egy hosszú és rövid vonalakból álló különös jelképrendszer szerepelt (lásd).

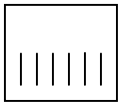

$= 000000_2 = 0_{10}$


$= 000001_2 = 1_{10}$


$= 000010_2 = 2_{10}$


$= 000111_2 = 7_{10}$


$= 010101_2 = 21_{10}$


$= 111111_2 = 63_{10}$

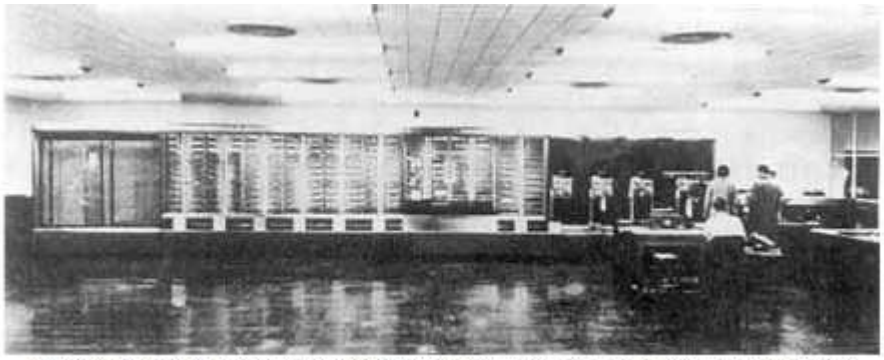
Az *I Csing* jelrendszerének ábráit (kódját) meglátva Leibniznek, akit abban az időben megbabonázott a 2-es számrendszer és a hozzá kapcsolt filozófiája, rögtön a helyiértékes 2-es számrendszert juttatta eszébe. A hosszabb vonalaknak a nullát, a rövidebbeknek az 1-est feleltette meg, így ezekből az 5.1. ábra szerinti módon előálltak a 2-es számrendszerben felírt számok.
Ebből Leibniz arra következtetett, hogy az ókori Kínában 2-es számrendszerben írták a számokat, de ez tévedés volt, mivel ekkor a kínaiak a 10-es és 100-as alapú számrendszert használták. Így a 2-es számrendszer valódi felfedezőjeként Leibnizet tarthatjuk számon.

5.1. ábra *Az I Csing jelképrendszere, valamint a megfelelő kettes és tízes számrendszerbeli számok (lásd az alsó indexeket)*

[54] „A dolgok lényege a számokban lakozik.”

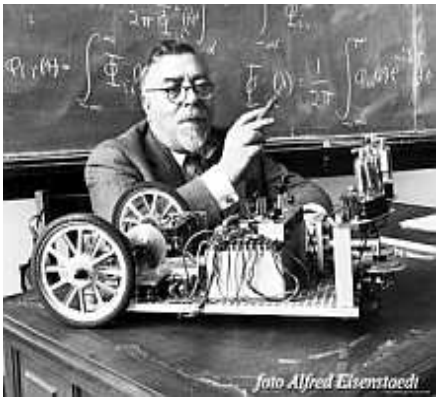
5.5. Mégis Neumann-elvű napjaink számítógépe?

Az elektromosság alkalmazása felgyorsította a számológépek fejlődését és a 20. század elején mind tökéletesebb elektromechanikus gépeket készítettek. Az Amerikai Egyesült Államokban *Howard Hathavay Aiken* elkészítette a MARK-I és MARK-II elektromechanikus analitikus számítógépeket, amelyekben egy összeadáshoz 0.3-0.5 sec, egy szorzáshoz 5-6 sec, míg egy osztáshoz 15 secundum kellett. Mindehhez (mint az a képen látható) egy hatalmas teremre volt szükség.



H.H.Aiken által tervezett MARK I elektromechanikus analitikus számítógép

Norbert Wiener 1940-ben megfogalmazta *a korszerű számítógépek "5-parancsolatát":*



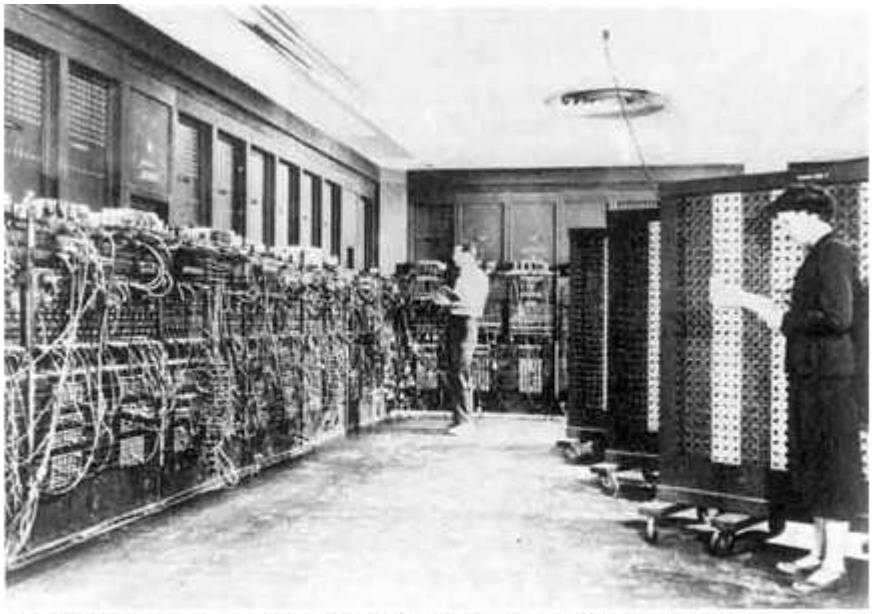
Norbert Wiener (1894-1964)

1. *A számítógép aritmetikai egysége numerikus legyen.*
2. *A mechanikus és elektromos kapcsolókat fel kell váltani elektroncsövekkel.*
3. *Az aritmetikai műveletek elvégzésére a 2-es számrendszert kell alkalmazni.*
4. *A műveletsort a gép, emberi beavatkozás nélkül, automatikusan végezze úgy, hogy a közbenső logikai döntéseket is be kell táplálni.* (Mai szóhasználattal, ez a program.)
5. *Legyen lehetőség az adatok tárolására, könnyű előhívására és törlésére.*

A II. világháború alatt rohamosan fejlődő hadiipar sorra vetette fel a rengeteg számolást igénylő feladatokat (például a nagy hatótávolságú lövedékek lőelemtáblázatai, lövedékek gyors röppályaszámítása, az atombomba kísérletek számításairól nem is beszélve), amelyek sürgették a "számítógépek 5-parancsolatának" gyakorlati megvalósítását.[55]
Így készült el Neumann János és Herman H.Goldstine tervei alapján 1943-1946 között az első elektronikus számítógép, az *ENIAC (Electronic Numerical Integrator And Calculator),* a philadelphiai Pennsylvania Egyetemen.[56]

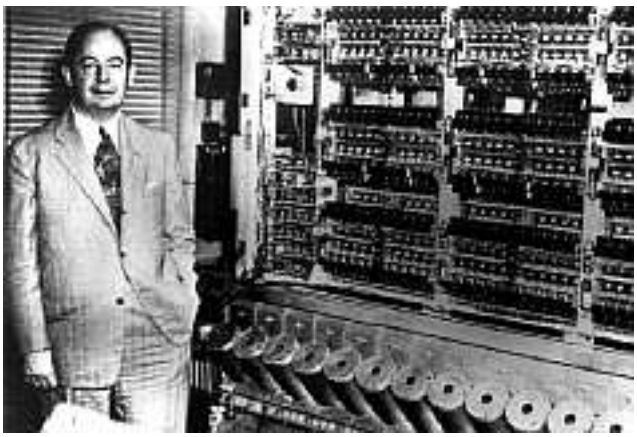
[55] Érdekes párhuzam, hogy Babbage számológépeit is az óriási számolás igényű csillagászati számítások inspirálták.
[56] Ma már tudjuk, hogy Turing gépei, a Colossus és az ACE is jóval az ENIAC előtt megszületett. De Turinggal méltánytalanul bánt a sorsa, mivel a Colossus-t a szigorú titoktartás, az ACE gépet pedig az NPL bürokratikus hozzáállása helyezte az ENIAC árnyékába!

Az ENIAC egy elektronikus kolosszus volt, amely 30 tonnát nyomott, egy több mint 30 méter hosszú terem kellett az elhelyezéséhez és a 18.000 elektroncső 100-150 kWó energiát fogyasztott (ezért a hűtése igen nagy problémát jelentett).



A Neumann János és H.H.Goldstine tervei alapján készült első elektronikus számítógép, az ENIAC

Az ENIAC még nem felelt meg egészen a Wiener "számítógépek 5-parancsolatának", hiszen aritmetikája 10-es számrendszerben működött. Számítási teljesítménye azonban a MARK-I és MARK-II gépekéhez viszonyítva lenyűgöző volt, az összeadást és kivonást 10 tizedes pontossággal 0.0002, a szorzást 0.0023 secundum alatt végezte el. Memóriájában mindössze húsz darab tízjegyű számot lehetett tárolni, így program tárolására nem volt alkalmas, a programozását egy huzalos dugaszoló tábla tette lehetővé.
Ezen adatok ismeretében még nagyobb tisztelettel kell adóznunk C. Babbage száz évvel korábbi teljesítménye előtt és egyáltalán nem csodálkozhatunk azon, hogy annak megvalósítása akkoriban kudarcba fulladt.



Neumann János (1903-1957)

Neumann János és *H.H.Goldstine* az 1940-es évek elejétől foglalkoztak a számítógépek elméleti és gyakorlati problémáival. Kutatásaik eredményét egy bizalmas jelentésben foglalták össze 1948-ban, amely először tartalmazta az univerzális, belső programvezérlésű, elektronikus, digitális számítógép tervét. Ebben egyértelmű érvekkel alátámasztva állást foglaltak a már Leibniz által ajánlott bináris számrendszer mellett, valamint megoldották a programtárolás módját is. Így lehetővé vált az adatok és részeredmények tárolásán kívül, a végrehajtandó utasítások tárolása is a számítógép memóriájának egy erre

fenntartott részében. Az ENIAC tapasztalatait felhasználva, már ezen elveket valósította meg, az 1948-1949-re elkészült *EDVAC (Electronic Variable Automatic Computer)*, amelyet tervezője *Neumann János* tiszteletére *"Johnnyac"*-nak is hívtak.

6. Tömeges információ + globális kommunikációs hálózat = globális e-társadalom

„A tipikus amerikai világban az információ sorsa az,
hogy áru lesz, venni és eladni lehet. Nem az én dolgom,
hogy azon akadékoskodjam, hogy ez a kereskedői álláspont
erkölcsös-e vagy nem, durva-e vagy finom.
Az én dolgom az, hogy kimutassam:
ez az álláspont az információ és a vele kapcsolatos
fogalmak, félreértéséhez és félrekezeléséhez vezet."
(Norbert Wiener 1894-1964 [WIENER 74])

És valóban, … az élet színpadán a valóság (mint legjobb rendező) mindig egyensúlyt teremt. Míg Turing tevékenységének a 20. század első felére volt történelemformáló hatása, addig mérnöki pontossággal a század közepére „időzített" korai halálával, a 20. század második felét napjainkig ható, látnoki gondolatainak megvalósulása töltötte be.
Turing, mint a kultúrtörténet óriásai Michelangelo, Leonardo, Mozart, Beethoven, vagy Einstein, egyszerűen a vezetéknevével él ma is a közgondolkodásban. A Turing-gép, a Turing-teszt köznyelvünk részévé vált, de valódi gondolati mélységeit a jelen 21. század globális e-társadalmában csak most kezdjük megérteni, amikor az Enigma megfejtése már csak a történelemkönyvek egy-egy jeles oldala. Mondhatjuk tehát, hogy Turing gondolati kortársunk. E kötettel is szeretnék megemlékezni, születésének éppen 2012-ben aktuális 100. évfordulójáról.

Turingra áttételesen szinte érvényes lehetne Madách örökérvényű gondolata, mely szerint

„Be van fejezve a nagy mű, igen.
A gép forog, az alkotó pihen.
Évmilliókig eljár tengelyén,
Míg egy kerékfogát ujitni kell."

De ma már tudjuk, hogy bár az alkotó valóban pihen, alkotásával, a „nagy művel" éppen egy lavinát indított el, amely egyre növekvő sebességgel, egyre nagyobb görgeteggé dagad.

Az előző fejezetből kiderül, hogy a 20. század közepén a „nagy mű", a számítástechnika készen állt az információk tömeges, soha nem látott sebességű feldolgozására. Ez volt az alapja egy egészen új iparág, az információ ipar kialakulásának. Nem véletlen tehát, hogy éppen ekkor (a 20. század második felében), az „információrobbanás" az emberi társadalmakban -akárcsak az ősrobbanás a világegyetemben- elindított egy visszafordíthatatlan folyamatot, ez az információalapú társadalmak kialakulása. Mivel a folyamat kezdete történelmi léptékkel mérve néhány másodperce zajlik, ugyanakkor az exponenciális léptékű változások az emberek mindennapi életét alapvetően meghatározzák, így könnyen válik ez az egész jövőnket meghatározó jelenség, és főleg ez az új iparág, valóban az üzleti vállalkozások és a napi politika martalékává.

Norbert Wiener
(1894-1964)

Norbert Wiener (1894-1964) fenti mottóban idézett gondolata nem csupán az információra, hanem az információn alapuló információs társadalomra is igaz. Vagyis egyet kell értenünk abban, hogy a

létrejövő információalapú társadalom (melynek kialakítása ma még általunk kormányozható) nem lehet üzleti vállalkozás.

A további fejezetekben azt szeretném tudatosítani az Olvasóban, hogy az információalapú társadalomban legnagyobb közös kincsünk, *globális titkunk*, a társadalomban (lavinaszerűen) felgyülemlő információ, amely az egyéneken keresztül ismeretté, majd a társadalmat fenntartó tudássá válik. Az információ birtoklásával és feldolgozásával kapcsolatos, Norbert Wiener által jelzett *„félreértések”* tehát társadalmi méretekben végzetesek lehetnek.

6.1. Valóban információt termel az információipar?

Ahhoz, hogy az információalapú társadalom alapvető értékéről, a biztonságról beszélhessünk, pontosítanunk kell a kulcsfogalmat: *az információt*. Mit is jelent az információrobbanás, az információfüggőség, mit is gyárt az információipar?

A 3.2. fejezetben láttuk, hogy az információ C.E.Shannon absztrakt értelmezésében, valamely jelkészletből előállítható jelsorozatok halmazán értelmezett függvény. Ez az értelmezés pontosan az információipar azon igényét volt hivatott kielégíteni, hogy magát az információt és minden vele kapcsolatos fogalmat számszerűsíteni lehessen. Így az információt annak *jel* értékével azonosítjuk és üzeneteink jelentés nélküli jelsorozatokká egyszerűsödnek. Ennek az értelmezésnek eredményeképpen Shannon a 6.1. ábrán látható modellel definiálta a kommunikációs rendszert.

6.1. ábra *A kommunikációs rendszer általános modellje CE..Shannon 1948-as cikkében*

Ugyanakkor a valóságban a jelek, jelsorozatok minden ember számára érzékelhetők *(rögzíthetők), míg azok csak bizonyos vonatkoztatási rendszer (értelmezési rendszer, dekódoló rendszer) birtokában* értelmezhetők. *Ugyanazon információ tehát az egyik embercsoport számára jelentéssel bíró ismeret, míg mások számára értelmetlen jelsorozat (adat). Néhány példa szemléletessé teszi az információ és az ismeret közötti jelentős különbséget.*

PÉLDA:
Gondoljunk például magára a beszédnyelvre. Eme szöveg, melyet most Ön éppen olvas, csak annak számára bír jelentéssel, aki ismeri a magyar nyelvet, mások számára csupán egy ABC betűiből készült jelsorozatok értelmetlen halmaza (ez Shannon tudatosan leszűkített értelmezése).

Még szemléletesebb egy fénykép, vagy videokép, amely valójában nem más, mint világos és sötétebb, vagy akár különböző színű pontok összessége.[57] A pontsorozat (jelsorozat) az információ, a kép az ember számára jelentéssel bíró ismeret. Azaz *továbbítjuk és tároljuk a pontokat, de a képet nézzük!*

A terminológia tehát pontos, az *információipar* valóban *információt* (Shannoni értelemben vett jelet, adatot) *termel tömeges mennyiségben*. Ez tehát az információsnak nevezett társadalom alapja?

Rényi Alfréd
(1921-1970)

A példákban felvetett paradoxon lehet a kulcsa ama gondolatnak is, amely a magyar matematika és információelmélet egyik legjelentősebb alakját *Rényi Alfrédot* (1921-1970) is foglalkoztatta. Évtizedekkel ezelőtt már így írt *Ars matematica* című könyvében [RÉNYI 73]:

"Amióta információelmélettel foglalkozom, sokszor eltűnődtem azon, hogy fér el néhány verssorban összehasonlíthatatlanul több információ, mint egy ugyanolyan hosszúságú, maximális tömörségű táviratban."

Mivel az emberiség számára évezredek óta az információk rögzítése, továbbítása technikai nehézségeket jelentett (szöveg nyomtatás, később hang-kép rögzítés, terjesztés, tárolás, stb.), így elődeink hozzászoktak ahhoz, hogy csupán az új ismeretek közvetítésére, átörökítésére korlátozták tevékenységüket.

A tömegtermelés -mint sok más területen is- megtette hatását és az információ ma már technikailag könnyen előállítható jel formáját, alapvetően elválasztotta annak jelentés tartalmától. Azaz exponenciális sebességgel termeljük a jeleket (adatokat), de nem áll ugyanez az ismeretek gyarapodására.

Ez a jelenség teszi az információrobbanást korszakhatárrá.

[57] Pontosan ez történik digitális világunkban, amikor minden információt elemi információ kvantumokra (bitekre) bontunk fel, amelyekhez számértékeket rendelünk. Így a tárolásra, továbbításra és feldolgozásra egyaránt azok a berendezések (gépek) lesznek alkalmasak, amelyeknek kifejlődését az előző fejezetekben bemutattuk. A 21. század fejlődési tendenciája, hogy azt a mély felismerést, miszerint a különböző típusú digitális információkat (szöveg, kép, hang, videó, stb.) azonos módon lehet feldolgozni a számítógépekben, úgy hasznosítsa, hogy a különböző infokommunikációs feldolgozó eszközöket minél kisebb méretben egyesítse.

6.2. Információrobbanás az információs társadalom kezdete?

Az információipar, mint a 20. század második felének új és egyre hatalmasabb ágazata, megkezdte és rohamos méretekben folytatja az információ tömegtermelését. Ezen új ágazat alapanyaga, félkész és végterméke is az *információ*. S mint a fogyasztói típusú társadalmak működési törvényei ezt diktálják, ez az ágazat is visszafordíthatatlan versenyfutásba kezdett önmagával, amelynek eredménye a ma már mindenki által hangoztatott *információrobbanás.*
Mint jeleztük, ezzel valóban egy egészen új korszak, új társadalmi forma vette kezdetét, amelynek jövője még ismeretlen, törvényszerűségeiről azonban modell analógia segítségével mégis sokat tudhatunk.

Az információipar működésének eszközrendszerét (és főképpen hajtóerejét!) az *információtechnológia* soha nem látott ütemű fejlődése teremti meg. Az információtechnológia mindenekelőtt az információ nagy tömegű tárolásának lehetőségét biztosítja.
Az írásbeliség kialakulása volt talán az első nagy hatás, ami a társadalmat az információipar részéről érte. Később -ahogy megjelent a távíró, telefon, kábel nélküli információ átvitel, majd ezek újabb és újabb változatai, végül belépett a számítástechnika- az információtechnológia alkalmassá vált az *idő* után a *tér áthidalására* is.

Az információ (adat, hír) mennyisége exponenciálisan növekszik. Ugyanez vonatkozik az információ technológia fejlődési ütemére is, míg mindezekkel fordított arányban csökken az információ átviteléhez szükséges idő, így az elérhető távolságok (a világegyetem tágulásával ellentétben) összezsugorodnak. Ez a helyzet a számítástechnika, digitális és műholdas adatátvitel végleges beépülésével az információiparba, magában rejti a Föld egyetlen globális társadalommá zsugorításának lehetőségét.
Az emberiség (egy része!) elérkezett egy olyan társadalmi modell beteljesedéséhez, amelynek középpontjában az információ áll, legnagyobb hatású ágazata az információipar, ez az információalapú társadalom. A mai valóságot még jobban fejezi ki az adat-hír dömping társadalom elnevezés.

Ahogy a fejlett országokban az elektromosság nélkülözhetetlenné vált az élet minden területén és kialakult a teljes elektromos függőség a társadalomban, úgy vagyunk szemtanúi annak, ahogy kialakulóban van az információfüggőség (ezen belül is egyre nagyobb teret hódít az elektronikus információ!) az e-társadalomban.
A számítógépes helyi, nemzeti és világhálókon óráról-órára tömegesen szaporodnak az adatok, üzenetek, az emberek milliói számára percek alatt elérhető információk. A sajtó, a tömegkommunikáció, a médiák, a reklámhordozók ontják az üzeneteket, adatokat, híreket és álhíreket. Kezdenek tehát kialakulni az *információfüggőség* tünetei, bár a fentiek alapján a valóságot talán jobban fejezi ki az *adat-hír függőség* elnevezés.

A világegyetem ősrobbanása és az információs társadalom kezdetét jelentő információ robbanás összevetése nem csak nyelvi játék.
A fizikai világban elismert alaptörvény az energia-megmaradás törvénye, melynek modern megfogalmazása: *„Zárt rendszer energiája állandó. Entrópiája csak növekedhet.”*
Ez bizonyos absztrakció segítségével átvihető a társadalomra, mint rendszerre is, ahol az emberek közötti viszonyokat az információ birtoklása és áramlása határozza meg. A társadalmi energia ezen viszonyokban (struktúrákban) testesül meg.

Az entrópia növekedése a rendezetlenség növekedésének, vagyis egy rendezettebb állapotból egy kevésbé rendezett (kevésbé kiszámítható) állapotba való átmenetnek felel meg.
Nos, a fizikai világban a rendezettebb állapotot a fizikai közelség képviseli, így az állandó tágulás entrópia növekedéssel jár, tehát megfelel a fenti törvénynek.
Az információs társadalomban (e-világban) a rendezetlenebb, kevésbé kiszámítható állapotot az információk szabadabb elérhetőségének közelsége jelenti, a zsugorodás tehát entrópia növekedéssel jár, ami szintén megfelel a fenti törvénynek.

A továbbiakban egzakt eszközökkel is megmutatjuk, hogy a fenti törvény a társadalomra, mint rendszerre is érvényes és ennek folyományaként két paradoxonra hívjuk fel a figyelmet.

6.3. Globális társadalom paradoxon

Az előzőkben kifejtett gondolatmenet egyenesen vezet ahhoz a konklúzióhoz, hogy *az információs társadalom globális társadalom.*
Fel kell hívni a figyelmet azonban a „globális társadalom" fogalomban rejlő paradoxonra. Induljunk ki Farkas János szociológus professzor társadalom definíciójából, miszerint ([FARKAS J. 1999] 1472.oldal): *„A társadalom szóval az egymással együttműködő emberek kultúrateremtő tevékenységére gondolunk. Ebben a jelentésében a különböző generációk közötti értékek és tapasztalatok átörökítését jelenti."*

A két gondolat összevetéséből adódik, hogy a globális társadalom csak akkor valósulhat meg, ha képesek az ebben résztvevő emberek *globális kultúrát* teremteni. Ehhez az eddig létrejött kultúrák tapasztalatai szerint, több ezer év lenne szükséges úgy, hogy ezalatt az ebben résztvevő emberek valóban együttműködnek egy közös cél érdekében. Igazán vonzó jövőkép. Vonzóbb, mint a SCIFI irodalom által felvázolt eltorzult, amorf-robotok jövőképe.
Ugyanakkor e globális kultúra lehetőségének van egy szépséghibája, ez pedig pontosan a megvalósulás reménytelensége.
A közös, globális kultúra ugyanis pontosan a több ezeréves létező kultúrák beolvadását (megsemmisülését) jelentené, ami a különböző kultúrák képviselőit eleve ellenérdekűvé teszi, így lehetetlenné válik az együttműködésük. Hiszen nem lehet közös cél a saját (nemzeti) kultúrák beolvasztása egy nehezen értelmezhető „közös kultúrába".
Mi sem bizonyítja jobban a globális kultúra megvalósulásának lehetetlenségét, mint az, hogy még a vallást sem sikerült az elmúlt több ezer év alatt egységesíteni. Sőt a történelem során (napjainkat is beleértve!) a háborúk, viszálykodások többsége éppen a vallások ellentéteiből fakadt.
Hogyan tudnának az emberek egy globális kultúra (mint közös cél) megteremtésében békésen együttműködni, ha a hit univerzalitása sem elegendő összekötő kapocs az egyes vallásoknak ahhoz, hogy közös célnak tekintsék. *Több ezer év alatt hol található meg a megvalósult globális vallás?! Még ha elvi támogatottsága lenne is, mekkora esélye van egy globális kultúra megvalósulásának?!*

6.4. Biztonságos információs társadalom paradoxon

A személyiséggel kapcsolatos jogok informatikai, számítástechnikai veszélyeztetésével kapcsolatos problémáknál elsősorban attól tartottak, hogy az automatikus nyilvántartó rendszereket használó szervezetek több kényes adatot tudnak majd összegyűjteni az egyénekről mint korábban és ezeket az adatokat könnyebben át tudják adni egymásnak. Ez a veszély pedig növekszik, ahogy személyes és munkavilágunkba egyre jobban belép a számítástechnika, az információipar. Még riasztóbb a biztonságérzetünk, ha a kommunikációs hálózatok összekapcsolódására gondolunk.
Ennek a problémának orvoslására sok országban alkottak olyan törvényeket, amelyeknek az a feladata, hogy szankcionálják (esetleg megakadályozzák) a központilag tárolt adatok téves, vagy rosszindulatú felhasználását.
Ez tehát azt sugallja, hogy általában nincs oka az egyénnek aggodalomra mindaddig, amíg a nyilvántartó rendszerek lehetővé teszik az érintett személy (adatalany) számára, hogy ellenőrizze adatainak helyességét és folyamatosan információt kapjon azok felhasználásáról (legalábbis azok többségéről). Ugyanakkor az információs technológiák elérték azt a fokot, amikor már elősegítik az egyéni viselkedés közvetlen nyomon követhetőségét, vagy az e viselkedésre vonatkozó, tárolt adatok hozzáférhetőségét. Például szolgálhatnak az ismert utcai, banki megfigyelő kamerák, illetve a számítógépen tárolt egészségügyi adatoknak rendőrségi hozzáférése.[58]

Feltehetjük a kérdést, hogy vajon George Arthur Orwell 1949-ben megjelent *Ezerkilencszáznyolcvannégy* című regénye napjainkban valóban utópiának tekinthető, amelyben ezt írja: *„Az embernek annak tudatában kellett élnie, hogy lehallgattak minden hangot, amit kiadott, s a sötétséget leszámítva minden mozdulatát megfigyelték.”*

A választ 50 évvel később, napjaink világméretű felismerése adja meg, amely hosszú titkolódzás után került nyilvánosságra: Földünket műholdakból álló lehallgató rendszer veszi körül, amelyek öt ország (USA, Kanada, Ausztrália, Nagy-Britannia, Új-Zéland) közreműködésével működnek. Hosszú ideig a nyilvánosságot a megtévesztő „kém műhold” elnevezéssel vezették félre, mondván, hogy ezek a műholdak csak katonai célokat szolgálnak. Azonban a 2000. év világszenzációja, vagy éppen világbotrányaként került napvilágra, hogy ez az ECHELON nevű rendszer, a ma már globális (egész Földet behálózó) kommunikációs rendszerek (telefon, fax, internet, stb.) teljes lehallgatására nem csupán alkalmas, hanem folyamatosan teszi is. Az ECHELON rendszer tehát, amelyet „NAGY FÜLEK”-nek is mondanak tökéletesen megvalósította Orwell „utópiáját”!**[59]**

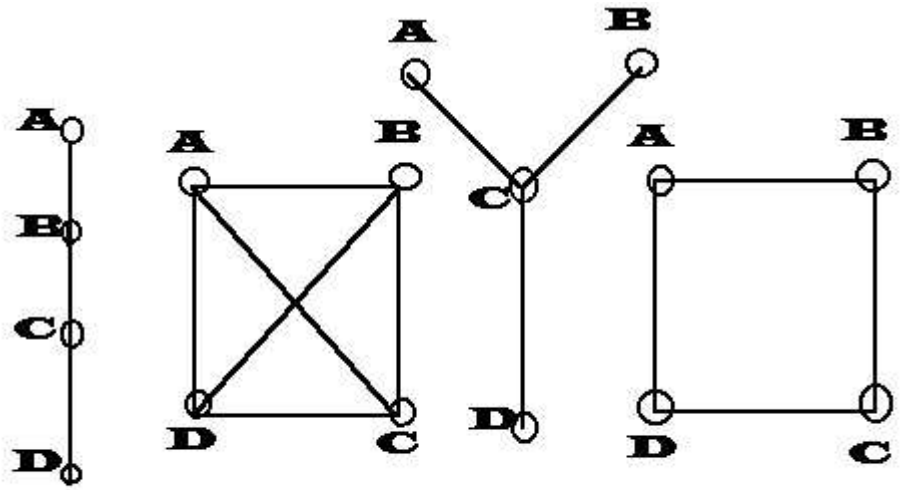
Az egyénről tehát egyre több személyes információ tárolódik, ugyanakkor az egyén számára egyre áttekinthetetlenebb az a hatalmas mennyiségű információ, amely számára idegen formában, virtuálisan áll rendelkezésére a hatalomnak.
Ez a virtualitás, az információ-szolgáltatók fokozódó elszemélytelenedése a forrása az egyén elszigetelődésének. Az elszigetelődés elbizonytalanodást is jelent, egy áttekinthetetlentől, a láthatatlantól való függés félelmét. Rendezettebb társadalmi struktúrákban tehát nagyobb az átláthatóság, a kiszámíthatóság, azaz a *biztonság*. Röviden:

BIZTONSÁG = KISZÁMÍTHATÓSÁG (rendezettség)

---

[58] Mindezeket részletesen tárgyaljuk az Információbiztonság fejezetben.
[59] Az ECHELON rendszerrel és annak hatásával, veszélyeivel a szabadságjogainkra és az információbiztonságra, foglalkozunk a NAGY TESTVÉR fejezetben.

A társadalmi relációk bonyolultsága (nem a mennyisége!) növeli a rendezetlenséget (entrópia növekedés!), így csökken a biztonság. Tehát ha társadalmi struktúrában fogalmazunk, akkor egy abszolút hierarchikus társadalom a legrendezettebb, így elméletileg ebben a legnagyobb a biztonság, míg a nyílt társadalmakban nagyobb a rendezetlenség, így elméletileg ezekben kisebb a biztonság.
Az alábbi 6.2.-6.5. ábrákon úgynevezett gráf modellekkel ábrázoljuk a társadalmi struktúrák (pl. kommunikációs hálózatok) alaptípusait. A betűkkel jelölt pontok egyedeket, csoportokat, objektumokat jelölhetnek, míg a közöttük létrejövő viszonyokat (relációkat) az őket összekötő vonalak jelölik.



6.2. ábra 6.3. ábra 6.4. ábra 6.5. ábra

Mindenki számára könnyen látható, hogy bár mindegyik ábra négy pontot tartalmaz, a 6.2., 6.4. struktúrák bejárhatósága sokkal kiszámíthatóbb, átláthatóbb, mint a 6.5. és főleg a 6.3. ábráé. Az előzőkben leírtak alapján azt is mondhatnánk, hogy a 6.2., 6.4. struktúrák biztonságosabbak, mint a 6.3., 6.5. struktúrák. Az ábrákkal illusztrálni szerettem volna azt az alapvető jelentőségű állítást, mely szerint:

> *Nem a társadalom alkotóelemei közötti viszonyok (relációk) száma, mennyisége az ami meghatározza a biztonságot, hanem eme relációk struktúrája.*

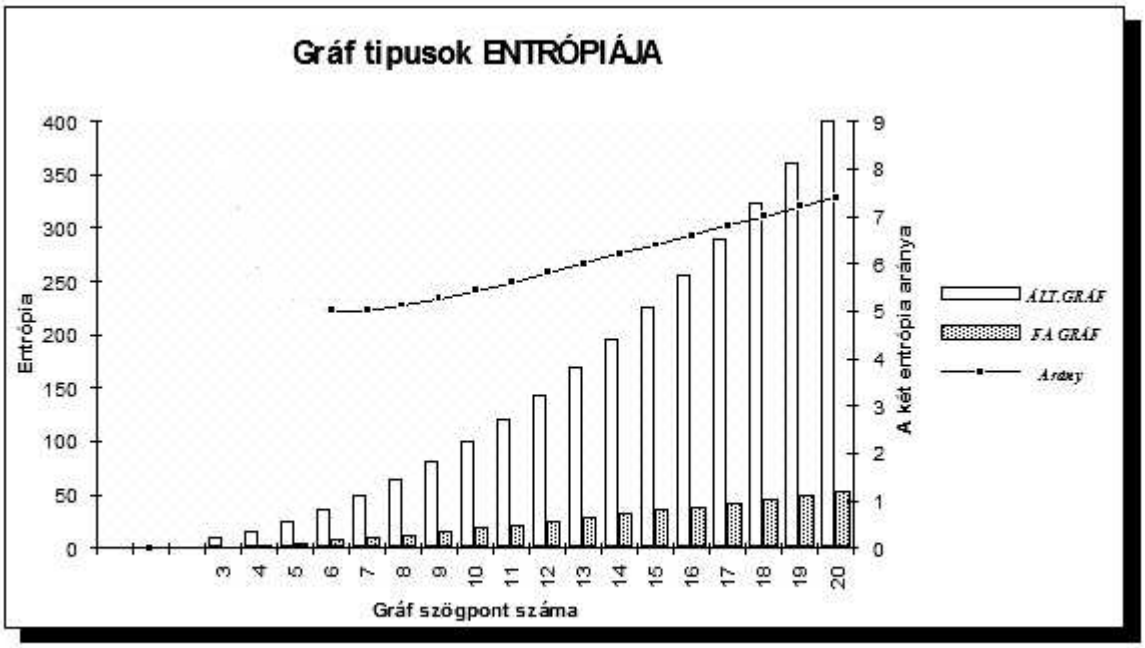
A társadalmi struktúrák elemzésére, ezek törvényszerűségeinek egzakt leírására a matematika gráfelmélet nevű ága bizonyult a legalkalmasabbnak.[60] Ezt mutatja az a könyvtárnyi irodalom, amely a 20. század közepétől e témakörrel foglalkozik.

Fontos felhívni a figyelmet arra, hogy ugyanezek a gráfelméleti eszközök igen alkalmasak a kommunikációs (információs) rendszerek leírására, elemzésére. A kommunikáció, mint az információ áramlás relációja, az információalapú társadalom meghatározó struktúra generátora. A biztonság szempontjából igen fontosak azok a strukturális jellemzők, amik a társadalmi és kommunikációs hálózatok egyensúlyáról, centralitásáról, átjárhatóságáról, összefüggőségéről, izomorfiáról, stb. egzakt leírást adnak.

[60] A 2003-ban megjelent Barabási Albert-László: Behálózva című kötete (magyar kiadása: [BARABÁSI 2008]), amelyben a klasszikus gráfelmélet újszerű alkalmazásait vezeti be. Könyvének népszerűségét mutatja, hogy azóta könyvének alcímét, a hálózatok tudománya elnevezést használják a tudományos közbeszédben.

Ezek a struktúrák határozzák meg azt a mozgásteret, amelyben a társadalmi folyamatok zajlanak. Ezekre a „hálókra" utal Farkas János [FARKAS J. 1999] tanulányában, amikor felteszi a kérdést: *„Kiszámíthatók-e a társadalmi folyamatok?"*
Erre a kérdésre sejti (csupán mennyiségi megfontolások alapján), hogy *„… alig kiszámítható bármely döntés várható következménye"*. Ez tehát maga a bizonytalanság!

Nos, az eddigiekben arra igyekeztem rámutatni, hogy a biztonság lényegileg nem mennyiségi kategória, így alapvetően strukturális jellemzők határozzák meg. A 6.2., 6.4. struktúrákat fa gráfoknak, míg a 6.3., 6.5. struktúrákat általános gráfoknak nevezzük. Megmutatjuk, hogy a „feszesebb" fa struktúrával jellemezhető hierarchikusabb társadalmak entrópiája sokkal lassabban növekszik, mint a globalizálódó „nyitottabb" általános gráf struktúrájú társadalmaké. Sőt a 6.6. ábra kis fekete négyzetekből álló görbéje mutatja, hogy a kétféle entrópia aránya is egyre növekszik (egyre távolabb kerülnek egymástól!).



6.6. ábra

Makroelméleti szinten tehát az információalapú társadalom, mint globális társadalmi modell, amely az információra és kommunikációra épül, a biztonság szemszögéből nézve nem sok jóval kecsegtet. Ugyanakkor az egzaktabb matematikai modellek és ezek segítségével leírható törvényszerűségek pontosabban arra mutatnak, hogy *az információalapú társadalom biztonság szempontjából jóval sebezhetőbb az eddigieknél.*

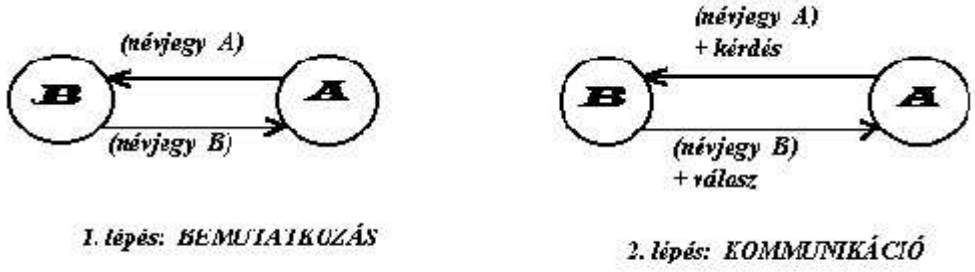
Jövőnk szempontjából ez már jóval biztatóbb, hiszen itt is érvényes Pólya György professzor[61] híres gondolata, amely szerint: *„A probléma megfogalmazása fél út a megoldáshoz."*

[61] A matematikai heurisztika atyja, A problémamegoldás iskolája című világhírű könyv szerzője.

6.5. A klasszikus és a globális kommunikáció modellje

A klasszikus kommunikáció magában rejtette a személyesség, az azonosíthatóság jegyeit. Sajnos ma már csak az etikett világára szűkültek az emberi megbecsülés, tisztelet olyan megnyilvánulásai, mint a bemutatkozás, kézfogás, meghajlás. A levelezés az aláíráson kívül is teljes terjedelmében tartalmazta a kézírás személyes jegyeit. Később az írógépes, majd a számítógépes papír alapú levelezés megőrizte a kézi aláírást, valamint a hitelesítő pecsétet, mint a küldő személyazonosításának eszközét. A klasszikus kommunikációban tehát a személyesség (vagy a személyiség 'lenyomata') mindkét irányban alapvető szerepet játszott. A kommunikáció első lépése a *kölcsönös bemutatkozás* volt, ezt követte a most már egymás számára azonosítható felek kommunikációja.
Ezt a modellt mutatja a 6.7. ábra, amelyen a személyazonosítás jegyeit *„névjegy”*-ként foglaltuk össze. Természetesen itt a névjegy általános értelemben értendő, ami esetenként lehet a névjegykártya is.
A modell lényege a bemutatkozás önálló lépése és a kölcsönösség, ami a kommunikáció során is megmarad! Az így kialakított *kétoldalú függőség* (Te tudod, hogy én ki vagyok, én tudom, hogy Te ki vagy), kölcsönös ellenőrizhetőséget és ezáltal KÖLCSÖNÖS BIZTONSÁGÉRZETET teremtett.

Klasszikus kommunikáció
(Kétoldalú függőség = kölcsönösség = biztonság)



6.7. ábra

Ahogy azt a rejtjelzéssel és rejtjelfejtéssel kapcsolatban megjegyeztük, a biztonság definiálása hasonlóan nehéz, mint a TITOK-é. Ezt általában úgy egyszerűsítik le, hogy a „biztonság” szó elé jelzőt tesznek, ezzel speciális esetekre korlátozva azt. A Shannoni kvantitatív gondolat rendszerben ez úgy oldható fel, ha a *biztonságot* a komplementerével, vagyis a *bizonytalanság mértékével* (entrópia) jellemezzük. Így a redundanciához hasonlóan azt mondhatjuk, hogy a

Biztonság = legkisebb mértékű bizonytalanság

Ebből az összefüggésből az is kiderül, hogy a *biztonság önmagában nem értelmezhető*, mivel egy adott rendszer tulajdonsága.

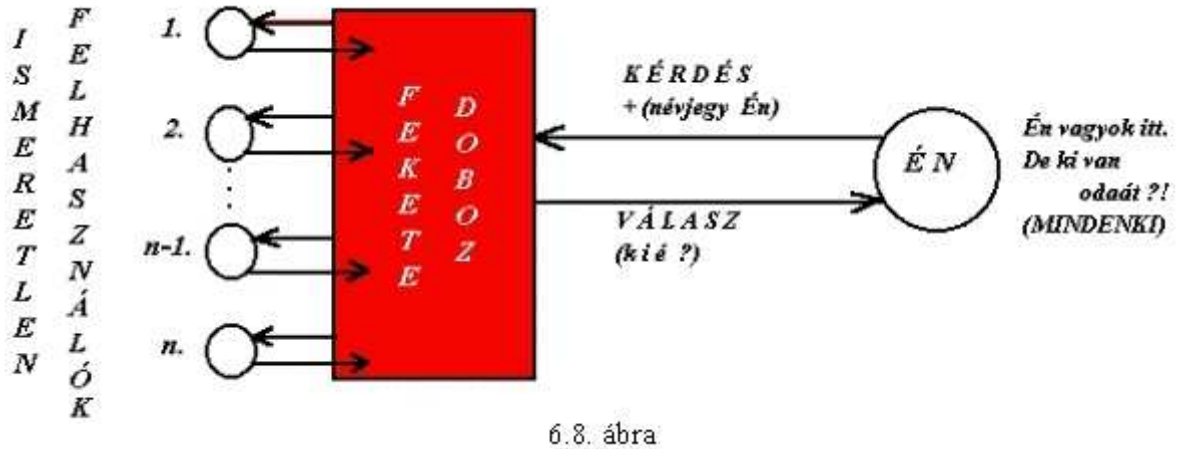
Az információalapú társadalom azonban a tömegesen és gyorsan elérhető információdömping oltárán feláldozza a személyességet és egy FEKETE DOBOZ modellt valósít meg. Ebben a modellben (lásd 6.8. ábra) egy óriási információ tárolóval (ez a 'fekete doboz') kommunikál

minden felhasználó. A felhasználók *egymás számára ismeretlenek* és csak a 'fekete doboz'-nak kell bemutatkozniuk, azaz névjegyet (azonosítást) adniuk, fordítva ez ellenőrizhetetlen.[62]

A modell tehát úgy működik, hogy mindenki egy közös dobozba ('fekete doboz') helyezi be az információit (lehet az személy, cég, intézmény, stb.) és ebből mindenki annyit vehet ki, amennyire a 'fekete doboz' engedélyt ad. A *függőség* tehát *egyoldalú*, ami *kiszolgáltatottságot* és ezért *bizonytalanságot* eredményez a felhasználókban.

Globális kommunikáció

(Egyoldalú függőség = kiszolgáltatottság = bizonytalanság)



6.8. ábra

A globális modell tömören leírható Arkagyij Rajkin szavaival: *„Én vagyok itt. De ki van odaát ?!”*

A válasz, mint látni fogjuk az információalapú társadalom kulcskérdéséhez vezet. A 20. század 30-as éveiben Turing, aki a mesterséges intelligencia kutatásokat is elméleti útjára bocsátotta, megfogalmazta a következő gondolatmenetet:
„Azt állíthatjuk, hogy egy gép gondolkodik, ha kérdéseket tehetünk fel neki, éspedig tetszőleges kérdéseket és az úgy válaszol, hogy ha nem 'nézünk oda', nem tudjuk, hogy a felelet géptől, vagy embertől származik-e.”

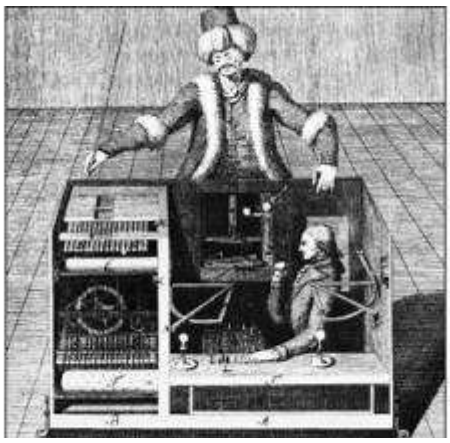
Turing gondolatmenete látnoki volt, ugyanis tökéletesen illeszkedik az információs társadalom 6.8. ábrán felvázolt *globális kommunikációs hálózataira*.
A kommunikációs hálózat minden felhasználója valóban egy monitor előtt ül és kérdéseket tesz fel. A monitoron megjelenő válaszok tartalmából azonban, ha odanézünk sem dönthető el biztosan a válaszoló 'személye', így annak valódi, vagy virtuális volta sem! (Természetesen itt a 'személy' jelölhet csoportot, céget, szervezetet, stb.)
A válaszoló 'személyének' bizonytalansága felveti az *általa képviselt információk valódiságának, a virtuális információknak* a problematikáját. Ez az elektronikus kommunikációs rendszerek és így az információalapú e-társadalom kulcskérdése.

[62] Napjainkban az internet egyik fő vonzereje a "globális névtelenség", ami egyúttal számos visszaélés és bűncselekmény forrása is.

7. Turing-teszt az e-társadalom napi gyakorlata
(Valódi vagy virtuális információ?)

„A mesterséges intelligencia
mindig egy program,
azaz egy Turing-gép."
(Church-tézis)

Az ENIAC és EDVAC elnevezések közötti (látszólag jelentéktelen) eltérés, már tükrözte azt a jelentős különbséget, amely a mind nagyobb teljesítményű, a szó szoros értelmében vett *számoló gépek*[63] és a változtatható és tárolt programokkal programozható *számítógépek* között létrejött.
Ez az a pont, ahol kezdett versenytárssá válni a gép és az ember, ahol már a nagy mennyiségi teljesítményekre képes automatikusan működő, de alapjában véve egyszerű gépek helyére léptek a programvezérelt automaták. Az automaták már az 18. században, a magyar polihisztor *Kempelen Farkas* (1734-1804) zseniálisan megtervezett és kivitelezett „*sakkozó automatája"* idején is nagy csodálattal töltötték el az embereket.



Kempelen Farkas sakkozó „autómatája"

Később a logikai gépek, majd az emberi funkciókat modellező automaták, már elkerülhetetlenné tették a programnak, mint matematikai fogalomnak a definiálását.
Éppen A.M. Turing volt az, aki az 1930-as években elsőként adta meg a program és a programozható számítógép matematikai modelljét, a róla elnevezett *Turing-gép* definícióját. Ez a gép tulajdonképpen egy absztrakt automata, amelyre teljesül az a meghökkentő tétel, amelyet *Alonzo Church* amerikai matematikus 1936-ban állított fel és amely szerint ***minden programhoz található egy azzal ekvivalens Turing-gép*** és fordítva, minden Turing-gép egy programot (algoritmust) valósít meg, azaz a Turing-gép tökéletes modellje a program fogalomnak. A Turing-gép, mint minden igazán zseniális elképzelés, egyszerűen leírható (az 5.3. fejezetben leírt definícó leegyszerűsítve):
Képzeljünk el egy olyan automatát, amely véges sok szimbólumot (jelet) képes feldolgozni úgy, hogy egy adott időpillanatban egyetlen szimbólumot képes leolvasni, vagy felírni egy elvileg végtelen szalagra. A feldolgozást egy speciális jel, a STOP jel feldolgozásakor fejezi be.

[63] A számológépek célja, minél nagyobb számokkal, minél gyorsabban végzett műveletek, azaz egyszerű aritmetikai műveletek nagyszámú gyors végrehajtása.

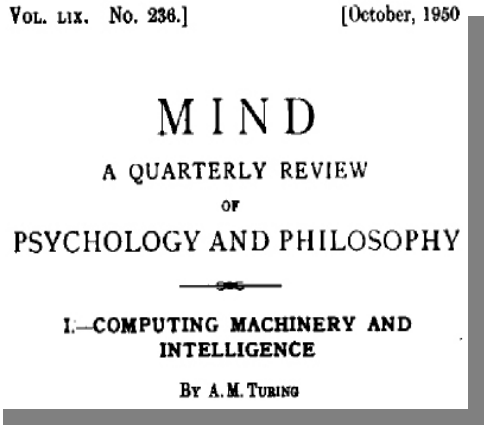
Ebben az absztrakt definícióban valóban benne van a jelek hosszabb jelsorozatokká való összeláncolásának és így tetszőleges bonyolultságú utasítások létrehozásának és tárolásának, a végrehajtás közben keletkezett jelek (adatok) tárolásának lehetősége, vagyis mindazon funkciók elméleti lehetősége, amelyeket egy évtizeddel később, Norbert Wiener a korszerű „számítógépek 5-parancsolata”-ban foglalt össze.

A programok, az automaták, a számítógépek számtalan elméleti kérdést vetettek fel, amelyek megválaszolására részben a matematikai logika, az absztrakt algebra és más matematikai területek segítségével kerestek válaszokat, részben egészen új tudományterületek születtek, mint például az *automataelmélet*, a *kibernetika*, a *számítógép tudomány*, vagy az *információelmélet*.

7.1. A Turing-teszt

A programozható gépekkel kapcsolatban, szintén a 20. század 30-as éveiben vetődött fel a kérdés, hogy létezik-e (létezhet-e) olyan programozási feladat, amely nem oldható meg? Azaz a Church-tézis szerint, létezik-e olyan programozási feladat, amelyhez nem található Turing-gép ?
1937-ben Turing bebizonyította, hogy a válasz *„igen”*, mivel azok és csak azok az algoritmusok programozhatók, melyekhez úgynevezett rekurzív függvények tartoznak. A matematikának azt a területét, amely eme kérdések egzakt tárgyalását tűzte ki céljául, *kiszámíthatóság elméletnek*, *algoritmus elméletnek*, illetve Turing előbbi tétele szerint a rekurzív függvények elméletének nevezzük. Ezek az elméleti területek leegyszerűsítve a következő kérdéssel foglalkoznak:
Melyek azok a számítások, amiket a számítógép el tud végezni, ha minden gyakorlati jellegű korláttól eltekintünk (mint például a rendelkezésre álló idő és tárkapacitás)?

Turing tehát kereste saját konstrukciójának a korlátait és egyben a mesterséges intelligencia kutatások előfutárának is tekinthető, mivel Ő vetette fel elsőként azt a kérdést, hogy *mit is jelent a „gépi intelligencia”?* Az első megválaszolásra váró kérdés persze az, hogy létezik-e ilyen?
Hiszen a máig létező többségi felfogás szerint intelligenciával csupán az ember rendelkezik, ezért a „gépi intelligencia” szóösszetétel értelmetlen. Turing azt is jól látta, hogy az intelligencia és gondolkodás fogalmak egymástól elválaszthatatlanok, ezért fogalmazta meg 1950-ben megjelent, klasszikussá vált [TURING 50] cikkében kérdését: *„Tudnak-e a gépek gondolkodni?”*


VOL. LIX. No. 236.] [October, 1950

MIND

A QUARTERLY REVIEW

OF

PSYCHOLOGY AND PHILOSOPHY

I.—COMPUTING MACHINERY AND INTELLIGENCE

BY A. M. TURING

Ezzel a kérdéssel és az ezt követő gondolataival indította útjára, a napjainkban egyre aktuálisabb mesterséges intelligencia kutatást. Turing szerint a "gondolkodni" szó inkább érzelmi kérdéssé teszi ezt az egész kérdéskört, ezért el is vetette, mint túlságosan bizonytalan (szubjektív) fogalmat. Ugyanakkor az 1950-es években sokan úgy gondolták, hogy Kurt Gödel (1906-1978) nemteljességi tétele a mesterséges intelligencia lehetetlenségét is bizonyítja:

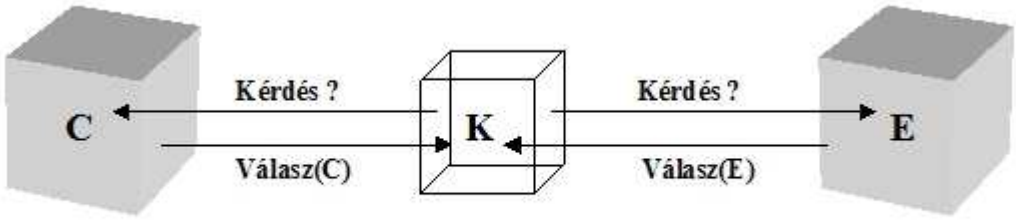
A mesterséges intelligencia mindig „egy program”, azaz egy Turing-gép (Church-tézis). Az ebben a gépben tárolt axiómarendszer meghatároz egy "nyelvet", amely nyelven megfogalmazható olyan kérdés, amelyre ebben az axiómarendszerben nem vezethető le igen-nem jellegű válasz (Gödel-tétel). Tehát e mesterséges intelligencia számára érthető nyelven, megfogalmazható olyan kérdés, amelyre nem tud sem igennel, sem nemmel válaszolni!

Bár ez az érvelés több sebből vérzik, témánk szempontjából csupán egyet emelek ki ezek közül: *Ha a mesterséges intelligenciát, mint az emberi intelligenciát utánzó konstrukciót fogjuk fel, akkor ennek megvalósíthatatlanságát nem bizonyítja az az érv, hogy bizonyos kérdésekre nem tud felelni, hiszen ez az emberi gondolkodásnak is jellemzője.*

Kalmár László (1905 – 1976)

A rekurzív függvények elméletének, a matematikai nyelvészetnek jelentős alakja, a magyarországi kibernetikai iskola megalapítója, *Kalmár László* (1905 – 1976) az 1948-as amszterdami Filozófiai kongresszuson tartott előadásában bebizonyította, hogy a Church-tétel a Gödel-tételből levezethető, így Church tétele nem bizonyíthatja abszolút eldönthetetlen probléma létezését.
Kalmár László hangsúlyozta, hogy ezeket a tételeket (Gödel, Church) szabatosan úgy kellene megfogalmazni, hogy a kérdéses problémasereg általános rekurzív eljárással nem oldható meg, nem pedig abszolút megoldhatatlanságról beszélni [KALMÁR 1986].

Turingot az ellenvetések és főleg a „gépi intelligencia” fogalmának bizonytalansága inspirálta egy új megközelítés felvetésére. Ennek lényege, hogy e szubjektív és ezáltal tudományosan megfoghatatlan fogalmak helyett, egy olyan módszert kell konstruálni, amelyet jól definiált technikai fogalmakkal lehet leírni. Javaslata szerint ez az általa *„utánzási játéknak”* nevezett módszer, amelyet manapság *Turing-teszt, vagy Turing-próba* néven ismerünk. A Turing-teszt lényege (lásd 7.1. ábra):
Képzeljük el, hogy egy C számítógép és egy E ember két külön helyiségben van elkülönítve és mindketten elektronikus kapcsolatban állnak egy harmadik helyiségben levő K személlyel, aki elektronikus úton kérdéseket tehet fel mindkettejüknek. K-nak az a célja, hogy a kérdéseire érkező válaszokból meg tudja különböztetni, hogy mely válasz származik C-től és melyik E-től.



7.1. ábra *Turing-teszt vázlata*

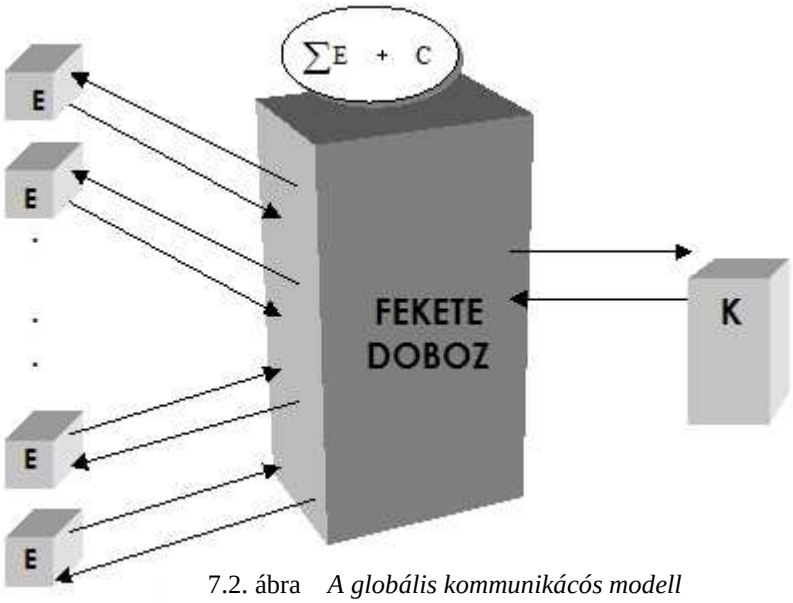
A teszt egyik óriási előnye, hogy az intelligenciáról, gondolkodásról való elmeélesítő gondolatkísérletek síkjáról, gyakorlatban kivitelezhető és a probléma lényegét megragadó eszközt kaptunk a kezünkbe. Hiszen most már az eredeti kérdés helyett azzal a jól kezelhető kérdéssel állunk szemben, hogy *"van-e olyan gép, amely ezt a játékot jól tudja játszani?"*
Az eredeti Turing probléma valóban a gépi és emberi intelligencia megkülönböztetése volt. A mesterséges intelligencia kutatások célkitűzése tehát, a gépek alkalmassá tétele arra, hogy az embert minél pontosabban tudják utánozni.

Turing eme korszakos cikkében kifejezte meggyőződését, hogy a 20. század végére a gépek már elég jól fogják játszani ezt a játékot ahhoz, hogy egy átlagos kérdezőnek nem lesz 70%-nál több esélye az azonosításra 5 percnyi kérdezés után. Ma már tudjuk, hogy a technikai fejlődés túlteljesítette Turing elképzelését.

7.2. A Turing-teszt és az e-kommunikáció

Vajon ha Turing megérte volna éppen 2012-ben esedékes 100. életévét, hogyan értékelné saját hatvan évvel ezelőtti elképzeléseit?
Valószínűleg elismerné, hogy fantáziája nem volt elegendő ahhoz, hogy előre lássa azt a technikai robbanást, amely a számítástechnikában, elektronikában, kommunikáció-technológiában bekövetkezett, s amelynek eredményeként a jelenünk, mindennapjaink részévé, napi gyakorlattá vált a Turing-teszt.

A mai információsnak nevezett, információalapú, vagy inkább e-kommunikációs társadalom ugyanis a 6.8. ábrán bemutatott FEKETE DOBOZ modellt valósít meg. Ez a globális kommunikációs modell tulajdonképpen egy megsokszorozott Turing-teszt modell (lásd 7.2. ábra), ahol mindenki a géppel kommunikál elektronikusan, így mindenki lehet kérdező (K) és kérdezett (E), a gép pedig összegyűjti és tárolja a $\sum E$ információt.



7.2. ábra *A globális kommunikációs modell tulajdonképpen egy megsokszorozott Turing-teszt modell*

Azt már Turing is látta, sőt elméletileg bebizonyította, hogy ha egy gép tökéletesen játsza az „utánzási játékot", akkor a Turing-teszt kérdésfeltevése *(Mesterséges vagy természetes intelligenciával állunk szemben?)* eldönthetetlen. A globális kommunikációs modellben ugyanakkor a *C* gép igazából nem a saját, hanem a sok-sok E_1 ,E_2 ,E_3 ,… felhasználó intelligenciájával „játszik", így *K*-val szemben emberi intelligenciák sokasága áll. E modell kísértetiesen hasonlít Kempelen báró 200 évvel előbbi „sakkozó automatájához", amelynek saját korában csodájára jártak, az utókor pedig egy szélhámos szemfényvesztéseként tartja számon. Pedig Kempelen „automatájában" valószínűleg csupán egyetlen pici, ámde zseniális emberke kuporgott!

A globális e-kommunikációs rendszerekben elhelyezett gépek, mint információgyűjtő fekete dobozok, túl jól játszák az "utánzó játékot", így sajnos a mesterséges és természetes intelligencia megkülönböztetésének problematikája hosszú időre a titkos kutatólaboratóriumokba szorult, míg eme e-kommunikációs rendszerekben a *Valódi vagy virtuális információ?* alapkérdés váltja fel. Ez egy egészen új kihívás.

Míg Turing elképzelése szerint a *K* kérdezőhöz a két másik féltől jövő válaszok *(E és C)* összehasonlítása fogódzót adhat a *„gép vagy ember?”* kérdés eldöntésére, addig az e-kommunikációban ilyen fogódzó nincs.

*Hiszen **minden válaszoló, gép által leképezett ember**.*
Az e-modellben tehát (Kempelen sakk-automatájával ellentétben) világos, hogy az "automatában ember ül", de a kilétét és állításainak valódiságát éppen a "tökéletes utánzás" fedi el.

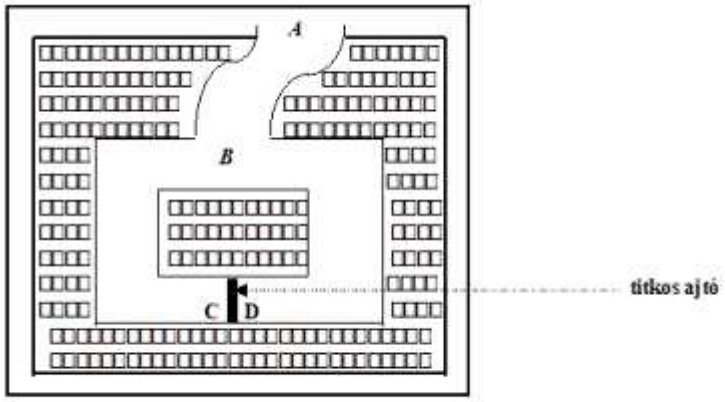
Egy olyan társadalomban, amely az információk szabadon áramló, tömeges áradatára épül (információalapú társadalom), reménytelen vállalkozás minden információ valódiságát egzakt módon ellenőrizni, így egyre nagyobb jelentőséggel bír az információforrások "beolvadása" a "fekete dobozba", amellyel az információ így szinte teljesen személytelenné válik.
A *K* kérdező számára tehát már nem az a kérdés, hogy emberi, vagy gépi intelligenciával áll szemben, hanem azt kell eldöntenie, hogy a kérdéseire érkező válaszok valódi, vagy virtuális "személytől" származnak, azaz döntéseket építhet-e rájuk, vagy sem. A *K* kérdező így teljesen kiszolgáltatott helyzetbe került, ami döntései szempontjából is jelentős bizonytalanságot jelent.

Az információalapú társadalom kulcsfogalma tehát az információbiztonság, azaz a titkos és nyilvános információk jó elkülönítése, tárolása, továbbítása, hiszen az e-kommunikáció dominanciája egyre jobban kizárja a hagyományos értelemben vett személyes azonosítást (lásd a klasszikus kommunikáció modelljét a 6.7. ábrán), a tapasztalatokon nyugvó ellenőrzést, így a legkülönbözőbb mesterséges azonosító eszközöket kell alkalmaznunk. A mesterséges azonosításhoz egyre több titkos kód, jelszó, kulcs megőrzésére, tárolására kényszerülünk. Hiszen ezek mindegyike számunkra, vagy más közös érdekeltségű csoportok számára, értékes információkat takar (hitelkártyák, telefonkártyák, igazolvány kártyák, PIN kódok és jelszavas azonosítók, stb.), akárcsak a fekete doboz "labirintusának titkos ajtója". A titkolódzás az e-kommunikációban általánossá válik, kilép a titkosszolgálatok szűk világából és mindennapjaink része lesz. Egyre nyilvánvalóbb a "nyíltan titkolódzás" szükségessége, amely "paradox játék" nagyon hasonlít a Turing-tesztre, sőt mára önálló területté vált a kriptográfiában, ez a *zero-knowledge proof*, azaz az *előismeretek nélküli bizonyítás*.

7.3. A *zero-knowledge proof* (*„előismeretek nélküli bizonyítás”*)

A probléma megfogalmazása igen egyszerű, ha észrevesszük, hogy a globális kommunikáció 7.2. ábra szerinti modelljében a szerepek felcserélhetők, azaz mindenki lehet kérdező és kérdezett, valamint fenti gondolatmenetünk szerint a gép és a számtalan felhasználó sem különböztethető meg információelméleti alapon.
Tételezzük fel, hogy a "fekete dobozban" egy labirintus van, mely egy titkos ajtót rejt, amelyen mindenképpen át kell jutni ahhoz, hogy a labirintus egyik feléből a másikba jussunk (lásd 7.3. ábra). A B *játékos ismeri az ajtó titkát (ki tudja nyitni azt!), de úgy kell ezt bebizonyítania*

az A *játékosnak, hogy közben magát a titkot ne árulja el. Ezt nevezi a nemzetközi szakirodalom „zero-knowledge proof"-nak, azokat az eljárásokat, amelyek alkalmasak az ilyenfajta bizonyításra, „zero-knowledge protocol"-nak.*



7.3. ábra *Labirintus titkos ajtóval*

Íme egy általános eljárás (protocol) az előismeret nélküli bizonyításra:

1. *Az A játékos a labirintus bejáratánál áll, míg a B játékos eltűnik a labirintusban.*
2. *Az A játékos két dolgot kérhet B-től:*
   - *Gyere ki a jobboldali folyosón!*
   - *Gyere ki a baloldali folyosón !*
3. *Mivel a B játékos a titkos ajtó egyik oldalán állhat csak (C vagy D), így ahhoz, hogy a kérést mindenképpen teljesítse, feltétlenül ki kell tudnia nyitni a titkos ajtót.*
4. *Az A játékos n-szer ismételheti meg a kérést és a B játékos mind az n-szer teljesíti.*

Így a *B* játékos bebizonyítja, hogy ismeri a titkot, de *A*-nak mégsem kell elárulnia azt. Ha csak egyszer játszák el a 2.-3. lépéseket (*n=1*), akkor az *A* játékos bizalmatlanul mondhatná, hogy *1/2* valószínűséggel, véletlenül is átjuthatott a titkos ajtón a *B* játékos.
Ha azonban 10-szer, vagy akár 20-szor ismétlik meg a 2.-3. lépéseket, akkor már mindössze $\frac{1}{2^{10}} = 0.0009$ vagy $\frac{1}{2^{20}} = 0.0000009$ a tévedés valószínűsége.

A zero-knowledge protocolok jelentősége egyre nyilvánvalóbb, így a szakirodalomban és a gyakorlati információ védelemben is egyre nagyobb szerepet töltenek be. A modell analógia alapján könnyen belátható, hogy ilyen „labirintus" szituációban vagyunk minden bankautomatánál, kártyával történő fizetésnél, vagy akár telefonálásnál, vagy például az email fiókunkba való belépésnél.

Szeretném az Olvasó figyelmét ráirányítani arra az alapvető paradigma váltásra, amely a globális e-kommunikációval a gép-ember, a mesterséges és természetes intelligencia viszonylatában bekövetkezett, és amely az információ tartalmáról, annak virtuális, vagy valóságos voltára, így az információbiztonságra tereli a figyelmet.

Szellemi relaxációként bemutatok néhány érdekes példát a zero-knowledge proof alkalmazására, amelyek modell analógia alapján igen komoly alkalmazásokra adnak módot.

7.4. A sakknagymester probléma

*Hogyan képes **Valaki**, aki éppen csak a sakkjáték szabályait ismeri, méltó ellenfélként játszani, vagy akár legyőzni egy sakknagymestert?*

Valaki kihívja egyszerre Gary Kasparovot és Anatolij Karpovot egy játszmára, ugyanabban az időpontban és ugyanazon helyen, de két külön helyiségben *(figyelemre méltó, hogy a kísérleti elrendezés mennyire hasonlít a Turing-teszthez)*. ***Valaki*** világossal játszik Kasparov és sötéttel Karpov ellen.

1. Karpov, mint a világos figurákkal játszó játékos megteszi a kezdőlépést. ***Valaki*** megjegyzi a lépést és átmegy Kasparov helyiségébe, ahol Ő vezeti a világos figurákat, így megteszi ugyanazt a lépést, amit Karpov tett.
2. Ekkor megvárja Kasparov válaszlépését, amelyet szintén megjegyez és átmegy Karpov helyiségébe, ahol Ő játszik a sötét figurákkal, így meglépi ugyanazt a lépést, amit Kasparov lépett.
3. Ezt az eljárást folytatja mindaddig, míg megnyeri valamelyik játszmát, vagy döntetlent játszik mindkettővel.

Így ***Valaki*** valóban szinte nulla ismerettel bizonyítja be a gyanútlan résztvevőknek (és nézőknek!), hogy nagymesteri szinten tud sakkozni.

7.5. Az átlagéletkor probléma

Hogyan lehet egy csoport tagjainak átlagéletkorát kiszámítani úgy, hogy senkinek az életkora ne derüljön ki?

Bár e kérdés felvetése úgy tűnik főleg női társaságban aktuális, mégis a módszert számos igen komoly területen is alkalmazhatjuk, ha például az életkor helyett jövedelem, vagyon, vagy akár szavazatok, vagy más titkos adatok szerepelnek. Íme a problémához rendelhető zero-knowledge protocol:

1. Legyen az *A* csoport tag adata *a*, a *B* csoport tagé *b*, a *C* csoport tagé *c*.

2. *A* választ egy tetszőleges (általában véletlen) számot, legyen ez *v* és képezi az $a'=a+v$ számot, amit egy borítékban átad *B*-nek.

3. *B* a borítékban kapott számhoz hozzáadja a saját adatát, azaz képezi az $b'=a'+b$ számot, amit egy borítékban átad *C*-nek.

4. *C* a borítékban kapott számhoz hozzáadja a saját adatát, azaz képezi az $c'=b'+c$ számot, amit egy borítékban továbbad.

5. Az utolsó csoport tag a saját borítékját átadja *A*-nak, aki a borítékban kapott számból kivonja a csak általa ismert *v* értéket, majd elosztja a csoport létszámával, így megkapják a csoport átlagértékét (pl. átlagéletkor), anélkül, hogy bárkinek az adata mások számára kiderült volna.

Bírálható ez a protocol azzal, hogy túl nehézkes az a megoldás, hogy minden csoport tag csak egymás után adhatja le adatát, azaz az eljárás szekvenciális. Az eljárás könnyen "párhuzamosítható":

1. Legyen az *A* csoport tag adata *a*, a *B* csoport tagé *b*, a *C* csoport tagé *c*.

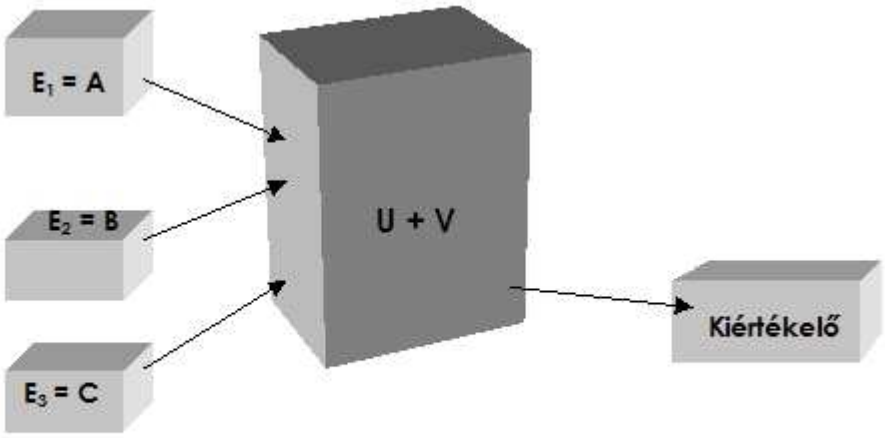
2. *A* választ egy tetszőleges véletlen számot, legyen ez *x* és képezi az *a+x* számot. *a+x*-et az U urnába, míg *x*-et a V urnába dobja be.

3. *B* választ egy tetszőleges véletlen számot, legyen ez *y* és képezi az *b+y* számot. *b+y*-t az U urnába, míg *y*-t a V urnába dobja be.

4. *C* választ egy tetszőleges véletlen számot, legyen ez *z* és képezi a *c+z* számot. *c+z*-t az U urnába, míg *z*-t a V urnába dobja be.

5. A kiértékelés egyszerű, hiszen csak az U urnában levő számok összegéből *(a+x+b+y+c+z)* levonjuk a V urnában levő számok összegét *(x+y+z)*, ekkor pontosan a csoport tagok adatainak összegét kapjuk *(a+b+c)*, amelyet elosztunk a csoport létszámmal, így pontosan az adatok átlagához jutunk. Világos, hogy mivel az U és V urnába dobott számok utólag már nem összepárosíthatók, a számítások közben az egyedi adatok nem azonosíthatók, azaz úgy számítottuk ki a csoport átlag adatát, hogy közben senkinek az egyéni adatára nem derült fény.

Vegyük észre, hogy ez a protocol is könnyen megfeleltethető a 7.2. ábra modelljének, hiszen az $E_1=A$, $E_2=B$, $E_3=C$, *U+V="fekete doboz"*, *K=kiértékelő* megfeleltetéssel éppen a 7.4. ábra modelljét kapjuk.



7.4. ábra *Az „átlagéletkor"probléma zero knowledge proof modellje*

Érdekes annak a modell analógiának végiggondolása, hogy ez a problémahelyzet nagyon hasonló bármely szavazáséhoz, így például az országgyűlési választásokéhoz is. Tehát a jövő e-társadalmának egyik pozitív perspektívája lehet az *e-szavazás* (elektronikus szavazás) lehetősége, amelynél a zero knowledge protocol igen fontos szerephez jut. Ugyanakkor vegyük észre, hogy mindhárom bemutatott példában a *valódi üzenet elrejtése* játszott alapvető szerepet. Ha például a „sakknagymester problémánál" nem biztosítjuk a két megfelelően elkülönített helyiséget, akkor máris „meztelen a király", vagyis meghiúsul az utánzó játék lehetősége.

A globális e-kommunikációs rendszerek azonban kitűnő lehetőséget biztosítanak a „virtuális szeparálódásra” a minden információt „bekebelező fekete dobozban”. Ez a csapda helyzet már csak látszólag hasonlít Turing modelljéhez, hiszen itt már nem a természetes és mesterséges intelligencia szétválasztása az igazi probléma, itt már egészen új, talán minden eddiginél nehezebben megválaszolható kérdés merül fel.

7.6. A 21. század új kérdése: *Valódi vagy virtuális információ?*

Szeretném, ha Ön is elgondolkodna azon, vajon eldönthető-e, hogy valós vagy virtuális információ van a globális kommunikációs rendszerek fekete dobozában?

> *Ez a kérdés nem azonos a „természetes vagy mesterséges?”-sel, nem azonos az „igaz vagy hamis?”-sal, ez a kérdés nem csupán a kommunikálókra és nem csak a kommunikáció tartalmára, hanem magára a kommunikációra vonatkozik.*

Az emberi kommunikációnak csak a verbális elemeit veszi át az e-kommunikáció, a fekete dobozba csupán a „tartalom”, vagy inkább annak is csak a „jel” része kerül. Az emberi kommunikáció legalább 50%-át alkotó metakommunikáció elvész. Pedig ez az, amitől az információ teljes, ez az a redundancia, az a tartalék, ami a kommunikációs „hibák” felismerését, esetleges javítását lehetővé teszi. Ez az 50% az, amely azt a vonatkoztatási alapot képezi, amelytől a puszta „jel” valódi „jelentéssé” válik.

Gábor Dénes
(1900-1979)

Ez az a csoda, amelyre *Gábor Dénes* (1900-1979) gyermeki naivitással rácsodálkozott, mikor a holográfiát, a teljes kép rekonstruálhatóságát felfedezte. 1971. december 11-én a Nobel-díj átvételekor tartott előadásán ezt így adta elő (lásd [GÁBOR 1976] 15.old.): *„A közönséges fényképen azonban a fázisok teljesen elvesznek, a fénykép csupán az intenzitásokat örökíti meg. Nem csoda, hogy elveszítjük a fázist, ha nincs mivel összehasonlítani!”*

Jelen szerző [TDT 1978]-ban általános rendszerekre is kiterjesztette a holográfia elméletet és bevezette az *egységes vonatkoztatási rendszer* kategóriáját, mint olyan strukturális fogalmat, amely alkalmas általános (így társadalmi), vagy éppen kommunikációs rendszerek modellezésére és igen pontos leírására.

Megállapítható tehát, hogy míg a közvetett (elektronikus) kommunikációnál minimális redundanciára törekszünk (különböző gazdasági, racionális technikai megfontolások miatt), addig a közvetlen emberi kommunikáció, a természetes rendszerek evolúciós törvényeinek megfelelően „felfelé optimalizálja” a redundanciát, azaz az entrópiát maximalizálja.

Ez ad magyarázatot arra, hogy az ember által racionális meggondolások szerint alkotott kódrendszereknél, titkosításoknál is igyekszik ezt az elvet érvényesíteni, azaz *a rejtjelzés minimális redundanciával törekszik a maximális entrópiára*. Lényegét tekintve ebben az esetben a titkosítás ténye nyilvánvaló, bár a megfejtés lehet nagyon nehéz. A rejtjelzés csupán a bemeneti információkhoz kötődő, statikus eljárás, így „érzéketlen” a környezeti változásokra. Ez tehát a *Találd ki!* titkosítási filozófia.

Talán nem véletlen, hogy a természet a titkosításra inkább a rejtést használja (pl. mimikri), amely éppen a jelentős redundanciára épít. A rejtés optimumát ekkor nem a rejtőzködő, hanem a környezete határozza meg! Ha megváltozik a környezet, akkor ezzel együtt kell változni a rejtőzködőnek is. Ez tehát a *Találd meg!* titkosítási filozófia (lásd például az előzőkben bemutatott „zero knowledge protocol”-t).

Turing tesztje és így a *„természetes vagy mesterséges intelligencia?”* kérdésfelvetése a fentiek alapján a globális e-rendszerekben már-már naivnak tűnő *Találd ki!* titkosítási filozófia feltételezésére épült. A teszt ugyanis magában hordozza azt a rejtett feltételezést, hogy az emberi nyelv tisztán információelméleti, illetve formális logikai megfontolások alapján képes a „teljes információ” közvetítésére. Azonnal hiányérzetünk támad azonban, ha az *információ* fogalma helyett az *ismeret* fogalmát használjuk a közölt üzenettel kapcsolatban. Ekkor ugyanis az üzenet jelsorozat tulajdonságához, annak jelentés tartalmát is hozzárendeljük, amely csupán valamely vonatkoztatási rendszer (értelmező, vagy fogalom-rendszer) birtokában értelmezhető, azaz a holográfia elv alapján, a teljes információ rögzítésére szolgál.

Az információ mennyiségi leírása statikus, melynek következtében a redundancia „felesleg”, így a mesterséges rendszereknél a „racionális szervezés” igyekszik azt minimalizálni. Ugyanakkor a természetes kommunikációnak a redundancia elengedhetetlen része (pl. metakommunikáció!), hiszen éppen ez biztosítja azt a vonatkoztatási rendszert, amely az üzenetet jelentéssel tölti meg.
Kalmár László több területen korát jóval megelőzte (matematikai nyelvészet, algoritmus elmélet, kibernetikai kutatások), így már az 1960-as években a kvalitatív információelmélet problémájával foglalkozott. Igyekezett felhívni a figyelmet az információelmélet továbbfejlesztésének szükségességére, s rámutatott, hogy a jelek, jelsorozatok alakjában továbbított információ (üzenet) mennyiségi vizsgálatán túllépve, az információ tartalmi-minőségi vonatkozásaival is törődni kell. Sajnos, amint erre már az előzőkben utaltunk, a kor nem kedvezett eme gondolatok széleskörű elterjedésének, de a 21. századi információalapú társadalom újra kikényszeríti e problémakör megoldását.

Ennek jegyében tesszük fel a következő kérdést: *Lehet, hogy éppen a redundancia rejti a természetes és mesterséges intelligencia között megbújó titok kulcsát ?* Eme kérdésre adott pozitív válaszunkkal mutatunk rá arra, hogy a titok kulcsa csupán egy olyan ajtót nyit ki, amely mögött újabb titok lappang. Az újabb titok a *„valós vagy virtuális információ?”* titka, amelynek megfejtéséhez már ez a kulcs kevés!

7.7. Turing szemléltető példája

Turing idézett, úttörő jelentőségű cikkében [TURING 50], demonstrációként bemutat egy elképzelt párbeszédet a *K* kérdező és a *V* válaszadó között:

K: Kérem, írjon egy szonettet a Forth-i Híd témájára (ez egy híd a Firth of Forth folyón Skóciában)
V: Ne számítson rám, sohasem tudtam verseket írni.
K: Adja össze a 34.957-et és a 70.764-et.
V: 105.621 (kb. 30 másodperc várakozás után jön a válasz)
K: Tud sakkozni?

V: Igen.
K: A királyom e1-en áll és nincs más bábom. Az Ön királya e3-on áll, a bástyája az a8-on. Ön következik. Mit lép?
V: Bástya a1 matt. (15 másodperc múlva jön a válasz)

E párbeszéd jól mutatja, hogy a *K* kérdező erőteljes törekvése ellenére, amely az emberi intelligencia legjellemzőbb „műfajait" (művészi hajlam, rutin műveletek, logikai képesség) igyekszik tesztelni, a válaszokból nem könnyen vonhatunk le a *„természetes vagy mesterséges?"* kérdés megválaszolásához messzemenő következtetéseket. Az azonban meghökkentő, hogy az utánzási stratégia legtöbb problémája éppen a legegyszerűbb rutinkérdéssel, az összeadással kapcsolatban vethető fel.
Azonnal feltűnik a hosszú válaszolási idő (30 másodperc), ami gépi válasz esetén teljesen elfogadhatatlan, emberi válasz esetén közepesnek tekinthető. Azt azonban kevesen veszik észre, hogy a *V* válaszoló által megadott eredmény helytelen (a pontos eredmény: *105.721*) és a tévedés is „inkább emberi" tulajdonság. Hiba lenne ugyanakkor elhamarkodottan a *V* válaszolót egyértelműen embernek minősíteni, hiszen számtalan érv szólhat a „gépi tévedés" mellett is. Példaként néhány ilyen hiba lehetőség:

- véletlen hardver hiba
- programozási hiba
- rendszer hiba

El kell ismernünk, hogy ha a *V* válaszoló meg akarja téveszteni a *K* kérdezőt (ha a Turing-tesztet játéknak tekintjük, éppen ez a cél), akkor legalább olyan nehéz feladata van, mint a *K* kérdezőnek, akinek e válaszok alapján döntenie kell arról, hogy *V* gép, vagy ember. A fenti rövid párbeszéd elemzéséből (amelyet idézett cikkében Turing igen részletesen megtesz) kiderül, hogy Turing tesztje valóban „utánzó játék", azaz *V* számára kétféle stratégia követhető:

- az ember utánozza a gépet
- a gép utánozza az embert

Turing cikkében így foglalta össze módszerének előnyeit:

„Az új problémafelvetés előnye az, hogy elég éles határvonalat húz
az ember fizikai és értelmi képességei között ….
Nem akarjuk ugyanis büntetni a gépet azért,
mert nem képes szépségversenyen tündökölni,
de az embert sem, mert veszít egy repülőgép elleni versenyben."

Márpedig *az információalapú társadalomban a Turing-teszt napi gyakorlattá válik* és a globális kommunikációs rendszerek fekete dobozában (mint arra az előző részben rávilágítottunk), a két stratégia bábeli keveréke áll elő. Felmerül tehát ílymódon az információk azonosíthatóságának, valódiságának, azaz az információbiztonság garantálhatóságának problémája, vagyis a *„valós vagy virtuális információ?"* alapvető jelentőségű kérdése, amelyre mindenképpen egy információalapú társadalomnak válaszolnia kell!

7.8. A Turing-teszt e-gyakorlata

A mesterséges intelligencia éppen az emberi racionalitás miatt, csak a jó, pozitív, „hasznos" emberi, illetve élő tulajdonságokat igyekszik modellezni (lemásolni). Hiszen az emberiségnek eme tulajdonságokkal lehet általában a teljesítményét maximalizálni. Attól jó egy gép, ha „fáradhatatlan", kiszámíthatóan, biztonságosan működik. Például az emberi fáradást, betegségeket, vagy más tökéletlenséget senkinek nem áll érdekében lemásolni, modellezni, gépi formában reprodukálni. Éppen ezért a mesterséges (gépi) rendszerek tesztelésére olyan pozitív tulajdonságok, paraméterek meglétét tételezzük fel, amelyekkel általában az ember (vagy az élő organizmus) rendelkezik. Ilyen tulajdonságok például az organizmusban keletkező hibák kijavítása, az organizmus reprodukáló, vagy alkalmazkodó képessége, stb.

Turing is arról beszél, hogy az ezredfordulón *„a gépek elég jól fogják játszani az utánzó játékot"* és ezalatt azt érti, hogy *„elég intelligensen lehet egy géppel kommunikálni"*. Így tehát, ha Kempelen Farkas módjára egy gépben elég ügyesen emberi intelligenciát helyezünk el (éppen ez történik az e-kommunikációs rendszerek fekete dobozában!), azaz *„virtuális gépembert"* készítünk, akkor a saját teljesítményközpontúságunk akadályoz meg abban, hogy az utánzó játékkal, mint tesztelési lehetőséggel célhoz érjünk, ha a gépet és az embert akarjuk megkülönböztetni egymástól.

Turing fent idézett példája tükrözi azt a humánus személyiséget, aki nem tud a valódi, a szó szoros értelmében vett gép – ember viszonyon túllépni, akinek látnoki képzelőereje sem volt képes a tiszta játékszabályokon túlra látni. Ezért csupa tényszerű, vagy konkrét emberi cselekvésre irányuló kérdés (kérés) képezi a képzeletbeli párbeszédeit. Kritikája, probléma listája is mélyen emberi! A valóságos jelenségvilágból nem tud (valószínűleg nem is akar!) kiszakadni. Ezért talán joggal hitte azt, hogy a tesztje valóban el tudja dönteni a *„tudnak-e a gépek gondolkodni?"*, avagy a *„természetes vagy mesterséges intelligencia?"* kérdését.

Turing gondolatkísérlete, mára a globális e-kommunikációs rendszerek mindennapi gyakorlata, amely az alábbihoz hasonló párbeszédek millióit hozza létre a nap 24 órájában (az alábbi párbeszéd-töredék csak modellezi a valódi gyakorlatot). A jelölések az 7.1. ábra Turing modelljének felelnek meg.

V: 8-kor a CSA-ban mindenki ott lesz. Gyere Te is!
K: Mi a téma?
V: QKAC, IDTLEN és még sok más téma, ami mindenkit érdekel.
K: Szó lesz a PARA-MÉTER-ről?
V: Biztos, mert sok mindenről szó lesz.
K: ….

Mint azt példánk is szemlélteti, az általános alany stílusában (megszólítás, személyes azonosítás és azonosíthatóság nélkül) megfogalmazott célirányos, „hatékonyságra" törekvő kommunikációnál, amely az e-kommunikációban tulajdonképpen információtovábbítássá zsugorodik és szinte „felesleggé válik" a metakommunikáció. Azaz a fentiek alapján éppen az üzenet „jelentéstartalmának vonatkoztatási rendszere" válik az „idő pénz" szemlélet martalékává. Igen szemléletesen mutatják ezt a tömörítési törekvést, az e-kommunikációban gyakorta használt (csupán szűk kommunikációs csoportok számára érthető) rövidítések, vagy például a tájékoztatásban, „reklám-kommunikációban" használt piktogramok, stb. Az üzenetek jelentése, a tulajdonképpeni ismeret, az e-kommunikációban olyan titokká válik, melynek „nyílt elrejtésére" a *zero-knowledge protocolok* bemutatásával mutattunk példát.

A jelen információs társadalmában az egyedek „észrevétlenül”, mint digitálisan tárolt adatsorok képződnek le a „fekete doboz(ok)ba”, a *„digitális Bábel tornyokba”*. Ezek az adatsorok egyre több és részletesebb adatot tartalmaznak, a tárolók részéről azzal a racionális igyekezettel, hogy minimális legyen a tárolt információk redundanciája. Ugyanakkor alapvető kérdés, hogy *„ki a tároló (tárolt információk) tulajdonosa?”*, aki(k)nek módjában lehet a „fekete dobozba” rejtett temérdek titok (információ) ismeretté konvertálása, majd jó vagy rossz célokra való felhasználása.

A Turing-teszt formális utánzó játékát valóban egyre „tökéletesebben” játszák és fogják játszani a gépek, azonban teljesen megváltozik a viszonyítási alap (a „mihez képest?”), hiszen a *K* kérdezőt és az E_1 , E_2 ,… egyéneket egyaránt a *C* fekete doboz „kebelezi be” (lásd a 7.2. ábrát). Azaz mint a kifordított kesztyű, kerül a külvilág (a valóság) a fekete dobozba, amelyen belül már valóban megkülönböztethetetlen a kint és bent, a *K* és *E*, így a *C*, *K* és *E* is! Vagyis mindenki kérdező és válaszoló, mindenki természetes és mesterséges intelligencia, mert nincs fogódzónk a valós és virtuális információ megkülönböztetéséhez.

A racionalitás, azaz az általános redundancia-minimalizálásra törekvés során ***megszületik az e-társadalom****, amelyben e-rétegződés, e-mobilitás, e-kultúra és így egyáltalán e-gyetlen rendező elv szerepel: ez az* ***„e-gy értékű társadalom”.***

Az e-gy társadalomban az emberek e-mberekké válnak, azaz olyan digitális információ-halmazokká, amelyek (és nem akik!) már a hatalom (az információs fegyver birtokosai) számára nem különböznek bármely virtuálisan előálló információ-halmaztól, így tetszés szerint manipulálhatók.

Szomorú, hogy akárcsak Orwell 60 évvel ezelőtti „utópiája” (lásd [TDT 2010]), mely szerint *„Az embernek annak tudatában kellett élnie, hogy lehallgattak minden hangot, amit kiadott, s a sötétséget leszámítva minden mozdulatát megfigyelték.”*, az elektronikus és globális ECHELON műholdas lehallgató rendszer mára megvalósult tény. Ugyanígy sajnos az információs fegyver elképzelése sem helyezhető az utópiák távoli világába, hiszen a mai reklám (főleg az e-reklám, e-média, e-sajtó) és PR eszközök tartalmazzák már eme manipulációs csírákat. Fel kell tenni tehát a következő kérdéseket:

Lehet, hogy a globális információs rendszerekkel, az *e-gy társadalom* alapkövét helyezzük el?

Lehet, hogy a 21. század információalapú társadalmának „csodafegyvere” a valós és virtuális világot megkülönböztethetetlenné tevő információs fegyver lesz ?

Lehet, hogy ez a fegyver az abszolút gazdasági racionalitás doktrínáját megvalósítandó, már semmiféle látványos pusztítást nem végez, csupán a valódi emberek tömeges, virtuális manipulációját valósítja meg, a globális és helyi hatalom kénye-kedve szerint?!

Lehet, hogy ezekre és még sok hasonló kérdésre kellene egy valódi EMBERKÖZPONTÚ, valóban TUDÁSALAPÚ társadalomnak, igazi válaszokat keresni, mielőtt felállítja az *„információalapú társadalom = e-társadalom”* egyenletet?

A lehetőség ma még, az utolsó pillanatban adott. Ehhez azonban fel kell ismernünk a már létező és a *globális e-gy társadalmakban* rohamosan terjedő *„virtuális agárverseny effektust”*, amely így fogalmazható meg röviden: *„Érjük utol a nemlétező nyulat egy virtuális agárversenyen!”*

7.9. PÉLDÁK a már alakuló virtuális „valóságra”

Az 1999-es év egyik szenzációja volt, hogy a digitálisan létrehozott „filmszínésznő”, Lara Croft világsikere után, egy kaliforniai filmcég (Virtual Celebrity) bejelentette az első digitális klón megszületését. Ez a digitális klónozás Marlene Dietrich arcát keltette életre és így a már régen elhunyt sztár, egy újonnan készült 30 másodperces filmben szerepelhetett a maga *„virtuális valóságában”!*

Az angol sajtószövetség által készített, a hús-vér műsorvezetők személyiségével rendelkező Ananova híreket, sport és időjárás jelentést olvas fel. Legfőbb előnye a testreszabhatóság, a felhasználó igényei, preferált hírei, kedvenc focicsapata szerint állíthatja be. A Posh Spice és Lara Croft keresztezésének kinéző Ananova arckifejezése, hangjának tónusa hírről hírre változik. Programozói reményei szerint idővel kialakul személyisége. A gyártó PA New Media nyilatkozata szerint céljuk "arcot adni az információnak". (CNN 2000. április)

Az amerikai Northwest Egyetemen olyan animált karakterek által megjelenített hírműsort hoztak létre, mely az egyes nézők személyes preferenciái alapján az online újságok hírei és az azokra reagáló bloggerek megjegyzéseiből állít elő híradásokat. A beszélő ágens mögött a hírek témájához passzoló képeket látunk és néha számítógépes játékokból kölcsönzött jelenetek színesítik az adást. (ORIGO, 2006. október)

Már nem csak virtuális bemondó,
de virtuális hírműsor is létezik az USA-ban! (ORIGO, 2006. október)

Tökéletesen beszél, sőt érzelmeket is képes kifejezni az a háromdimenziós modell, amelyet a Miskolci Egyetemen fejlesztettek ki. 10 éve dolgoznak a programon. A virtuális bemondó a siketek és nagyothallók beszédtanításában is sokat segíthet. (miNap online 2011. január)

E *„valós vagy virtuális információ?”* problematikáját elemző fejezet végére, mint felkiáltójel alá a pontot, kínálta maga az élet: ***„Az USA Legfelsőbb Bírósága engedélyezte a gyermek pornó filmeket, amennyiben nem élő, hanem csak virtuális szereplők szerepelnek benne.”*** (MTI, 2002. április)

8. Tömeges titkosítás és egyéni biztonság
(A dokumentumvédelem problémái és új módszerei)

„Néha nehéz megmondani, mi az igaz,
de egy hazugságot sokszor
nagyon könnyű felismerni."
(Albert Einstein)

8.1. Személyhez kötött és tömeges dokumentumok

Az USA vízumok biometrikus azonosítóval való biztonságosabbá tételéről szóló hír bejárta a világsajtót és jelentős nézetkülönbségek mellett, mégis igen nagy feltűnést keltett. Íme néhány idézet a 2004. júniusi tudósításokból:

„Az amerikai kogresszus nemrég úgy döntött, hogy a terrorfenyegetettség miatt még megbízhatóbb szűrőre van szükség a vízumok elbírálásakor. Az Egyesült Államok főkonzulja szerint a szigorú ellenőrzés nem csak az amerikaiak biztonságát szolgálja. Péntektől az ujjlenyomatát is rögzítik annak, aki az Egyesült Államokba szeretne utazni. A vízumkérelem elbírálásakor a kérelmező fotója mellé csatolják az ujjlenyomatát is. Az adatokat egyelőre még csak érkezéskor ellenőrzik, később majd kiutazáskor is, így ugyanis könnyen kiderül, ha valaki tovább maradt az Egyesült Államokban, mint amennyi időre vízumot kapott. Az Egyesült Államok nagykövete maga mutatta meg, hogyan is működik az új rendszer. Egy kattintás, és már nem csak a vízumigénylő fényképe, hanem ujjlenyomata is az adatbázisban van."

„Digitális ujjlenyomat az amerikai vízumokban. *Az amerikai kongresszus döntése alapján a vízumoknak a jövőben biometrikus azonosítót is tartalmazniuk kell. A magyar nagykövetségen bemutatták az eljárást. Az amerikai kongresszus a szeptember 11-i terrortámadás hatására döntött úgy, hogy további biztonsági elemeket épít be a vízumokba, hogy azonosítani tudják az Egyesült Államokba utazókat. Az elfogadott törvény alapján csak géppel leolvasható, biometrikus azonosítóval ellátott vízumokat adhatnak ki."*

*„**A magyar turistáktól is ujjlenyomatot vesznek az amerikai vízumhoz.** Mától a budapesti amerikai nagykövetségen is digitális ujjlenyomat készül azokról, akik az Egyesült Államokba kívánnak utazni. A világ csaknem 140 országában bevezetett, úgynevezett biometrikus adatfelvételtől az USA azt reméli, hogy sikerül csökkenteni az országot fenyegető terroristaveszélyt. A jövőben csak azok léphetnek az Államok területére, akik nem szerepelnek valamelyik feketelistán. Az eljárás nagyon egyszerű: a jobb és a bal mutatóujjat kell az átvilágítóra helyezni, s egy kamera digitális fotót készít a vízumkérőkről. A beutazók adataihoz az amerikai belbiztonsági minisztérium és a külügyminisztérium férhet hozzá, a büntetés-végrehajtási szervezetek csak a törvényes engedélyek után kaphatják meg az azonosítókat."*

Ezen sajtó idézetek jól mutatják, hogy igen aktuálissá és meggyőződésem szerint szükségessé vált több olyan, a dokumentum biztonsággal kapcsolatos fogalomról, nézetről és megoldásról beszélni, amelyek egyre gyakrabban bukkannak fel mindennapi életünkben. Ilyen fontos és pontosításra szoruló témák és fogalmak, az egyedi és a tömeges dokumentumok biztonsági védelmének kérdése, a biometrikus azonosító, vagy a digitális, illetve a digitálisan rögzített ujjlenyomat fogalmai.

A fogalmak pontosítása kapcsán képet kaphatunk a dokumentumok védelmének új, a digitális technika által kínált irányairól és lehetőségeiről, valamint arról a lényeges különbségről, amelyet a személyhez kötött (egyedi) és a nem személyes, azaz tömeges dokumentumok védelme jelent.

A dokumentumok biztonságán az egyértelmű azonosíthatóságot értjük, azaz bármely hamis dokumentum megkülönböztethetőségét a valóditól.

A 8.1. ábra összefoglalja azokat a szempontokat, amelyek mentén felvázolhatjuk a dokumentumok védelmének főbb irányait. A táblázat oszlopai egyfajta történelmi trendet mutatnak, hiszen az írásbeliség megjelenése évszázadokon keresztül csak egyedi dokumentumok (levelek, oklevelek, igazoló okiratok, stb.) előállítását tette lehetővé. Nem véletlen, hogy e hosszú történelmi periódus alatt igen hatékony, de személyhez kötött módszerei alakultak ki a dokumentumok védelmének (kézírás, aláírás, pecsét, stb.). *Ebben a történelmi periódusban a dokumentumok egyedi volta miatt nem vált el a dokumentum tartalmának és hordozójának védelme*, mivel bármelyik sérülése egyértelműen igazolta a dokumentum hamis voltát. Ekkor még a kézbesítés személyhez kötött volta is a dokumentumok biztonságát (bizalmas jellegét) szolgálta.

	Egyedi dokumentumok (személyhez kötött) *- magán és hivatalos levelek* *- igazoló okiratok* *- oklevelek* *- igazolványok* *- titkos iratok*	**Tömeges (védett) dokumentumok (nem személyhez kötött)** *- bakjegyek* *- értékpapírok (pl. részvények)* *- csekkek*
Dokumentum adathordozójának védelme	*- speciális minőségű papír* *- vízjel* *- előnyomott (fejléces) papír*	*- speciális minőségű papír* *- vízjel* *- fémszál* *- dombornyomat* *- mikronyomat*
Dokumentum tartalmának védelme	*- kézi aláírás (kézírás)* *- pecsét* *- iktatószám* *- dátum* *- speciális tinta* *- igazolványoknál fénykép*	*- precíziós nyomdatechnika* *- speciális festék* *- azonosító (kód) szám*

8.1. ábra *Dokumentumok hagyományos védelme*

A nyomtatás megjelenésével kezdett növekedni a védett (bizalmas) dokumentumok kibocsátása, és napjainkra, főleg a bankjegyek, értékpapírok elterjedésével tömeges méreteket öltött. Ez a tömegesedés új (tömegesen alkalmazható) dokumentum-védelmi technikákat követelt meg. *Ekkor vált szét az adathordozó és a rajta levő tartalom védelme.*

Az 8.1. ábra szemléletesen mutatja, hogy míg az adathordozó (hagyományosan általában papír) védelme óriási technikai fejlődést produkált, addig a dokumentumok tartalmát szinte ugyanazokkal az eszközökkel védik a mai napig. Az így kialakult biztonsági filozófia tehát alapvetően a dokumentum hordozójának nyomdatechnikai védelmére épült:

Legyenek az azonos típusú dokumentumok (pl. azonos címletű bankjegyek) teljesen egyformák, mert így, ha egy bankjegy (dokumentum) eltérő, az a feltűnő, az a hamisítvány.

Az adathordozók nyomdatechnikai védelme napjaink dokumentumvédelmének is a fő iránya (mikronyomat, hologram, lézergravírozás, stb.), csak ma már bizonyos dokumentum típusoknál a papír egyeduralmát átveszik a korszerűbb műanyag (plasztik) kártyák. Az új adathordozó a dokumentumok repertoárját is bővíti (hitelkártyák, telefonkártyák, igazolvány kártyák, stb.) A kibővült dokumentumskála biztonsági problémái azonban nem változtak. Csupán a súlypont áthelyeződéséről van szó, mivel *minél magasabb szintű technikát alkalmazunk az adathordozók védelmére, annál nehezebbé tesszük (nem lehetetlenné!) a hamisításukat, de egyúttal a hitelességük ellenőrzését is!*
Manapság egy bankjegy, egy értékpapír, vagy akár egy igazolvány hitelességének biztos eldöntéséhez komoly műszerezettségre és szakértelemre van szükség. És akkor még nem is vizsgáltuk a dokumentum tartalmi hitelességét.

A számítástechnika rohamos térhódításával, a dokumentumok elektronikus előállításának elterjedésével az egyedi dokumentumok előállítása egyre személytelenebbé vált, így már nem megkerülhető a dokumentumok tartalmi hitelesítésének kérdése. Ennek a problémakörnek a megoldására született *a digitális aláírás.*

A digitális aláírás tulajdonképpen a hagyományos kézi aláírásnál többre képes: egyszerre azonosítja az aláírót és a dokumentum tartalmát. Sőt ugyanez a technika képes az egyedi dokumentum azonosítók egy szintén klasszikus elemét (lásd 8.1. ábra), a dátumot is beépíteni a digitális aláírásba, ez az úgynevezett időpecsét.

A napjainkban jórészt elektronikusan előállított, de nem elektronikusan továbbított és tárolt dokumentumok, azaz a papír, illetve műanyag adathordozókon tárolt dokumentumok biztonsági (védelmi) helyzetét foglalja össze, a 8.1. ábrának megfelelő 8.2. ábra.

	Egyedi dokumentumok (személyhez kötött) *- magán és hivatalos levelek* *- igazoló okiratok* *- oklevelek* *- igazolványok (plasztik kártyák)* *- titkos iratok*	**Tömeges (védett) dokumentumok (nem személyhez kötött)** *- bakjegyek* *- értékpapírok (pl. részvények)* *- csekkek* *- bank és hitelkártyák*
Dokumentum adathordozójának védelme	*- speciális minőségű papír* *- vízjel* *- előnyomott (fejléces) papír* *- hologram* *- lézer gravírozás* *- biometrikus azonosítók*	*- speciális minőségű papír* *- vízjel* *- fémszál* *- dombornyomat* *- mikronyomat* *- hologram*
Dokumentum tartalmának védelme	*- kézi aláírás (kézírás)* *- pecsét – tintával – dombornyomással (száraz pecsét)* *- iktatószám* *- dátum* *- speciális tinta* *- igazolványoknál digitális fénykép* *- digitális aláírás* *- digitális ujjlenyomat*	*- precíziós nyomdatechnika* *- speciális festék* *- azonosító (kód) szám* *- digitális aláírás* *- digitális ujjlenyomat*

8.2. ábra Nem elektronikus dokumentumok védelme napjainkban

Mint az a 8.2. ábrából is jól kivehető, a dokumentumok modern biztonságtechnikája szinte mindent megvalósított a klasszikus biztonsági eszköztárból, csak a biztonsági filozófia maradt még napjainkban is érintetlen.

Ez pontosan azt jelenti, hogy a dokumentum tartalmának azonosítása még mindig független a dokumentum adathordozójától. Az egyedi dokumentumokhoz hasonlóan a tömegesen előállított dokumentumok esetében is csak bonyolult számítástechnikával és műszerezettséggel ellenőrizhető a teljes hitelesség. Ez pedig a hétköznapi helyzetekben (pl. bankjegyek, igazolványok, stb. ellenőrzése) nehezen, vagy egyáltalán nem megvalósítható. Ennek a problémának naponta vagyunk tanúi, amikor professzionális módszerekkel hamisított igazolványokkal (pl. rendőr igazolvánnyal), okmányokkal, bankjegyekkel, vagy éppen más értékpapírokkal való visszaélésekről kapunk hírt a sajtóból. A bűnüldöző szervek tagadhatatlan sikereként könyveljük el egy-egy hamisító banda felszámolását, de érdemes elgondolkodni azon, hogy a valódi kár jelentős részét sokszor nem maga a hamisítás okozza, hanem az, hogy a hamis dokumentum hosszú ideig van forgalomban, felfedezéséhez igen nagy és drága apparátusra van szükség. Vagyis szembe kell nézni a bűnüldözés kontra bűnmegelőzés dilemmával, annak elméleti, gyakorlati és anyagi vonzatait is figyelembevéve. Különösen igaz ez akkor, amikor csupán az audio-video műsoros adathordozók hamisításából származó károkat csak Magyarországon, évente több milliárd forintra becsülik. Ha a becsült károknak csupán töredékét az elméletileg kidolgozott, csupán technológiai kidolgozásra és

bevezetésre váró módszerekre költenék, akkor szinte nullára csökkenthetők lennének az adathordozó dokumentum hamisítások.

Mindehhez szükséges tehát egy újabb, koherens dokumentum-biztonsági filozófia megfogalmazása, amely ötvözi a bevált régi tapasztalatokat az új technikai lehetőségekkel. Ez így hangzik:

Legyen mindenegyes dokumentum hordozóját és tartalmát tekintve is egyedi (különböző), így minden darabról önmagában eldönthető, hogy valódi-e vagy hamis.

Azaz most nem a különbözőség, hanem éppen az azonosság az, ami feltűnő. A hamisítványt tehát egy másik példánnyal való azonossága árulja el.

Ennek az új biztonsági filozófiának a megvalósításához az szükséges, hogy az adathordozót és annak tartalmát egyértelműen egymáshoz tudjuk rendelni, mint ahogy egy konkrét személyhez egyértelműen tartozik az ujjlenyomata. Ugyanakkor világossá válik, hogy élesen el kell különíteni az egyedi, azaz személyhez kötött és a tömeges dokumentumokat a védelem szempontjából (ezt demonstrálja a 8.2. ábra).

Az elkülönítés alapvető okát a dokumentumok tömeges, gépesített előállításában érhetjük tetten. Hiszen míg a nem személyhez kötött dokumentumok biztonságát az adathordozó és a tartalom védelme egyértelműen biztosítja, addig a személyhez kötött dokumentumoknál (pl. igazolványok) a tulajdonos és a dokumentum egyértelmű egymáshoz rendelését is biztosítanunk kell. Csupán ez utóbbi célt szolgálja a bevezetőben idézett újsághírekben is „dokumentumvédelmi csodaszerként” üdvözölt biometrikus azonosítók sora. Nem csökkentve e módszercsalád 21. századi digitális technikával megvalósított magasszintű biztonsági paramétereit, világosan kell látni, hogy ez csupán a 8.2. ábra egyetlen cellájának védelmi problémáját szolgálja, nem általában a dokumentumok teljes védelmét. Például nem védhetők a tömeges, nem személyhez kötött dokumentumok (pl. bankjegyek) személyes azonosító jegyeinkkel (pl. ujjlenyomat), sőt az is belátható, hogy pusztán az igazolványunkon elhelyezett ujjlenyomatunk, semmit nem mond arról, hogy az igazolvány adatai megfelelnek-e az ujjlenyomathoz tartozó személynek.

A helyén és értékén kezelt biometrikus azonosítás, napjaink digitális technikájának lehetőségeit kihasználva, igen magas biztonsági paraméterekkel rendelkezik. Ugyanakkor az alkalmazása számtalan alkalmazástechnikai és állampolgári jogokat érintő problémával küzd.

8.2. Biometrikus azonosítás, avagy a személy egyedisége és a dokumentum személyessége

Manapság a legkorszerűbbnek számító védelmi (ezen belül dokumentumvédelmi) rendszerek biometrikus elven működnek, azaz az ember egyéni jellegzetességeinek felismerésére épülnek. Ezek már nem csak azonosítást végeznek, hanem komplex védelmi feladatok megvalósítására is képesek.

Az ilyen típusú eszközök első családja a felhasználók ujjlenyomatának azonosítására épült. Például miközben az egérrel klikkelgetünk, a rendszer automatikusan összehasonlítja ujjlenyomatunkat a tárolt adatbázisban lévővel, és vagy engedélyezi a belépésünket vagy nem. Ezek a rendszerek a legegyszerűbbek közé tartoznak, mégis olyan mennyiségű adat tárolását

és feldolgozását igénylik, ami csak megfelelő számítógép és érzékelő eszköz birtokában valósítható meg. A legkorszerűbbnek az úgynevezett többdimenziós rendszerek számítanak, vagyis azok, amelyek az arc azonosítására, a hanganalízisre és a szájmozgás felismerésére egyaránt képesek. A rendszer az egyik biometrikus jegy kismértékű megváltozása esetén is biztonságosan azonosítja a felhasználót a másik két jegy alapján.

Az íriszazonosításon alapuló eljárások azok, amelyek kétségkívül a legmegbízhatóbbak közé tartoznak. Az eddigi tapasztalatok szerint az írisz mintázata az egyének meglehetősen stabil azonosítását teszi lehetővé, azonkívül a sérülések ellen sokkal jobban védett, mint például a kéz. Az elv az emberi szem retinája fényvisszaverési és elnyelési tulajdonságainak mérésén alapul, miközben a felhasználó bizonyos távolságból egy fényforrásba néz. A rendszer a mért értékeket hasonlítja össze egy tárolt mintával.

A biztonság fokozható az azonosítási módszerek kombinálásával. A megfelelő biztonság érdekében természetesen gondosan védeni kell a berendezéseket, és mivel személyhez kötött dokumentumokról van szó, így alapvető jelentőségű az azonosítandó személyekről tárolt legszemélyesebb biometrikus adatok védelme. Minderről, valamint ezen technikák és a személyes adatok védelmével kapcsolatos aggályokról is szó lesz a továbbiakban.

8.2.1. Néhány szó a biometriáról

A biometria olyan automatikus technika, amely méri és rögzíti egy személy egyedi fizikai, testi jellemzőit és ezeket az adatokat azonosításra és hitelesítésre használja fel. A biometrikus felismerés alkalmazható személyazonosítás céljára, amikor a biometrikus rendszer azonosítja a személyt, és egy egyértelmű számsorozatot rendel hozzá, majd egy adatállományból kikeresi az ezzel megegyezőt. Használható továbbá ellenőrzési célból, amikor a biometrikus rendszer hitelesít egy személyt az előzőleg tárolt mintái alapján. Számos előnyt kínál a biometria alkalmazása a személyazonosság és hozzáférés jogosultság vizsgálatánál. A biometrikus azonosítás ugyanis az emberek valódi, egyedi testfelépítésüktől függő és az embertől elválaszthatatlan azonosító jegyein alapul.

A hagyományos azonosítási eljárásokban alkalmazott tárgyak, mint például a chipkártyák, a mágneskártyák, vagy a fizikai kulcsok, jelszavak stb. elveszthetők, ellophatók, lemásolhatók. A jelszavak sokasága könnyen elfelejthető, vagy mások által elleshető. Ezektől a hátrányoktól mentes minden biometrikus eljárás: az ujjunkat mindenhova magunkkal visszük, és a hangunkat sem tudjuk kölcsönadni.[64] Ugyanakkor a gyakorlati tapasztalatok szerint nem okoz nehézséget az embereknek azonosításkor egy szenzor megérintése vagy a nevük kimondása.

8.2.2. A legelterjedtebb biometrikus technológiák

Ujjlenyomat-azonosítás: Az ujjlenyomat egyedi és konzisztens, a rendelkezésre álló technológia a személyek pontos azonosítására alkalmas ujjlenyomatuk képe alapján. Csak mintegy negyven-hatvan jellemző pontot rögzít az ujjlenyomat teljes képéből, így annak kikeresése a teljes adatbázisból az azonosság megállapítására, igen gyors. Ugyanakkor a

[64] Természetesen a képzett bűnözők számára ezek az azonosítási módok sem jelentenek áthághatatlan akadályt, de a biometrikus azonosító rendszerek kijátszásához nagyon drága technika és igen komoly felkészültség szükséges, így csak jelentős megtérülés esetén vállalják a tetemes kockázatot.

felvett mintából nem lehet visszaállítani a teljes ujjlenyomatot, így nem kell tartani a személyiségi jogok megsértésétől.

Hanganalízisen alapuló felismerés: Használata rendkívül egyszerű, hiszen csak egy mikrofonba kell néhány szót (például a nevünket) bemondani, azonban számolni kell a háttérzaj, illetve hang egyéb torzulása által okozott problémákkal.

Kézgeometria-elemzés: Használata szintén egyszerű, de problémát okozhat az ízületi gyulladás, illetve a jelentős fogyás.

Retinavizsgálat: A retina szkennelése különleges pontosságú azonosítási eljárás, de agresszív módszer, használata körülményes, mivel a fejet rögzíteni kell ahhoz, hogy a fénysugarat a retina hátfalára vetíthessük.

Íriszdiagnosztika: Az írisz szkennelése nagyon sokat fejlődött az elmúlt néhány évben, és napjainkban is intenzív fejlesztési szakaszban van. Pontos, mintegy négyszáz "adatpontot" használ az azonosításhoz, bár nem mindenkinek van konzisztensen mérhető írisze (például a kontaktlencse, a szürke hályog okozhat problémák).

Arcfelismerés látható fényben: Az arc felismerése - párosulva a mintaazonosító eljárásokkal - jó azonosítást szolgálhat. Jelenleg különleges esetekben használják. Nem alkalmas tökéletesen egyforma egypetéjű ikrek megkülönböztetésére.

Arcthermogram: Az arcthermogram egy olyan felvétel, melyet infrakamerával készítenek, és az arc hőmintázatát mutatja. A kép egyedi, és kombinálva nagy bonyolultságú mintaazonosító algoritmussal - amely ellenőrzi a relatív hőmérséklet-különbségeket az arcon - olyan technikát kínál, amely független a kortól, az egészségi állapottól, de még a test hőmérsékletétől is. A módszer tizenkilencezer „adatpont” felvételével kivételes pontosságú, képes megkülönböztetni a teljesen egyformának tűnő ikreket, akár sötétben is. További előnye a teljes diszkréció. Ennek a technológiának a fejlesztése manapság a költségek csökkentésére irányul annak érdekében, hogy minél szélesebb körben váljék alkalmazhatóvá az azonosítási és hitelesítési eljárásokban. Az arcthermogram a legígéretesebb módszer, a legpontosabb, leghatékonyabb és a legbiztonságosabb eljárást kínálva, ha a technológiai költségek elfogadható szintre csökkennek.

8.2.3. Adatvédelmi aggályok

A biometrikus azonosító technológiával kapcsolatban többször felvetődik az erkölcs és a törvényesség kérdése. Vajon mi különbözteti meg az ellenőrzést az azonosítástól? Talán az érintett beleegyezése? Az új technológiák fejlődése nagymértékben fenyegeti a magánéletet, és kétségessé teszi az emberi személyiség megőrizhetőségét. Sokak véleménye szerint a technológia már annyira tökéletes, hogy sértheti a személyiségi jogokat, mivel a biometrikus azonosítók egész életünkben változatlanok, ezért magukban hordozzák a későbbi nem célhoz kötött felhasználás veszélyét.

Minden, a személy azonosítására alkalmas adat használata adatvédelem alatt áll Magyarországon. A személy azonosítására alkalmas eszközök használatáról (ujjlenyomat-rögzítők, hangfelvétel-készítők stb.) szintén a törvény határoz. A hanganalizátorok például képesek arra, hogy megállapítsák vele, mennyire egészséges valaki. Ám ehhez a személyes

adathoz is csak az illető hozzájárulásával lehet köze bárkinek is. Az adatvédelem szabályai arról is rendelkeznek, hogy a térfigyelő rendszerek által adott képeket nem lehet tárolni, csak abban az esetben, ha épp bűncselekményt rögzítettek vele.

Jelenleg a rendőrség csak a rendőrségi törvényben meghatározott esetekben használhat titkos információgyűjtésre például azonosító készülékeket, eszközöket, nyilvántartást és adatbázist. Az arcazonosításról a hatályos jogszabályokban nincs szó, ám a fénykép őrzése például megtalálható benne, így értelmezés kérdése, hogy szabad-e vagy sem a rendőröknek arcazonosító technológiát használniuk. Ugyanakkor a DNS-sel való azonosításra szűk körben ugyan, de van törvényi felhatalmazása a bűnüldözőknek, holott ez is megváltoztathatatlan kódja az embernek, miként az arca is. Aggályosnak tartja az adatvédelmi biztos is, hogy ujjlenyomatot, vagy pláne íriszazonosítót tartalmazzon az útlevél. Ugyanis így olyan személyes adatokra is lehet következtetni (utóbbiból például öröklődő betegségekre), aminek a nyilvántartása sérti a személyiségi jogokat. Eddig csak a bűnözők ujjlenyomatát vették nyilvántartásba, emiatt az emberek idegenkednek ettől a megoldástól. Nem zárható ki, hogy később az íriszazonosítót is bevezeti az EU, mivel az íriszképet tartják a legbiztonságosabbnak a szakértők.

8.2.4. A biometrikus azonosító mint adat

Az eddigiekből világosan kiderül, hogy a biometrikus azonosító jegyekhez (pl. ujjlenyomat) a további felhasználás céljából egy-egy jól definiált számsorozatot rendelnek hozzá. Így válik egy adatbázisban tárolható és visszakereshető adattá. Tulajdonképpen a digitális számítógépesítés elterjedése előtti korszakokban, maga az ember is így „működött”, hiszen az igazolványban, vagy útlevélben elhelyezett fényképről is csak a jellemző vonások alapján azonosították az igazolványt felmutató személyt. Furcsa és időigényes eljárás lett volna, ha az igazolványt felmutató személy arcát pontról pontra összehasonlították volna a fényképpel. Ugyanígy, néhány (vagy néhány tucat) jellemző alapján történik az ujjlenyomat azonosítás, vagy az egyéni írás grafológiai azonosítása. Mindezek alapján látható, hogy a biometrikus jegyek kölcsönösen egyértelműen tartoznak egy-egy személyhez, azaz mindenkinek egyedi ujjlenyomata van és egy adott ujjlenyomat pontosan egy emberhez tartozik. Ugyanezt a kölcsönös egyértelműséget kívánjuk meg a biometrikus jegyhez rendelt digitális adattól (számsortól), de mégis egy igen nagy különbség fedezhető fel a kettő között. A biometrikus jegy digitális megfelelőjéből (képéből) ugyanis nem rekonstruálható tökéletesen az eredeti. A digitalizálás ugyanis információveszteséggel jár. Érdemes megjegyezni, hogy ez a tulajdonság minden numerikus adat sajátja, mivel az adatok mindig mérés útján keletkeznek és a mérőeszközök minden esetben csak bizonyos pontossággal közelítik meg a valóságot. Jelen esetben éppen annyira kell pontosnak lenni a biometrikus jegy digitális megfelelőjének (kódolt alakjának), hogy a kölcsönös egyértelműség, azaz az egyértelmű rekonstrukció, azonosítás biztosítható legyen.

Mindezek alapján fontos annak megállapítása, hogy a biometrikus azonosító olyan speciális digitális adat, amelynek célja, hogy kölcsönösen egyértelműen egymáshoz rendelje a dokumentumot és annak tulajdonosát. A 8.2. ábrában közölt dokumentumvédelmi rendszerezés egyetlen cellájának specialitásait testesíti meg, azaz csak személyhez kötött dokumentumoknál alkalmazható és mint az a fentiekből kiderül, egyáltalán nem foglalkozik a dokumentum harmadik tényezőjével, a dokumentum tartalmával.

Tehát a nem elektronikus dokumentum egyértelmű azonosítását biztosító triád, a *dokumentum adathordozója -tartalma –tulajdonosa* által meghatározott három relációból a biometrikus azonosító egyet véd magas biztonsági szinten (adathordozó és tulajdonos megfeleltetése). Ezt bizonyítják a biometrikus azonosítók alapvető alkalmazási területei:

· Büntetés-végrehajtó intézetek, ahol a fogva tartottakhoz érkező látogatókat azonosítják, hogy a látogatás ideje alatt ne cserélhessenek helyet
· Gépjárművezetői engedélyek kiadásánál, hogy elkerüljék azt: a gépjárművezetők (különösen kamionsofőrök) több jogosítványt állíttassanak ki maguknak, vagy egymás között cserélgethessék azokat
· Segélyezési rendszerek
· Határellenőrzés (figyelemre méltó példa az amerikai Inspass eljárás, melyben az országba érkezőket olyan kártyával látták el, amely lehetővé tette számukra, hogy az elhelyezett biometrikus terminálokat használják, és elkerüljék a hosszadalmas sorban állást a bevándorlási hivatalnokoknál)
· Személyi és egyéb igazolványok (olyan chipkártya alapú azonosító igazolvány, amely tulajdonosának ujjlenyomatadatait is tartalmazza)
· Szavazó rendszerek, ahol a politikusok igazolják személyazonosságukat a parlamenti szavazások során; ennek segítségével megakadályozható, hogy "helyettesek" adják le voksaikat
· Utazás és turizmus (a biometriai azonosítókat hordozó kártya lehetővé tenné, hogy az utazók a különböző, törzsutasok számára biztosított kedvezményeket igénybe vegyék, a határátlépést ellenőrző rendszerekben használják, valamint fizetési eszközként repülőjegyek vásárlásánál, szállodai költségek, bérautók díjainak kiegyenlítésénél valamennyit kényelmesen, egyetlen kártya használatával)
· Számítógépes rendszerek hozzáférése, Internetes tranzakciók

· Telefonos ügyfélszolgálatok (számos távközlési vállalat vezetője hangsúlyozza a biometria alkalmazását)

A teljes védelmi rendszer áttekintéséhez adósak vagyunk még a másik két reláció (adathordozó-tartalom, adathordozó-tulajdonos), valamint a tömegesen alkalmazott, így egyáltalán nem személyhez köthető dokumentumok biztonsági kérdéseinek tárgyalásával.

8.3. Digitális aláírás, avagy a dokumentum tartalmának és tulajdonosának hitelessége

A nem elektronikus, mondhatjuk általános értelemben vett „papír alapú” dokumentumok biztonsági problematikáját egy háromtényezős (három dimenziós) rendszerben lehet csak teljesen leírni. A három tényező: T1-a dokumentum hordozója (anyaga), T2–a dokumentum tartalma (a rajta tárolt információk), T3-a dokumentum tulajdonosa (a személy, vagy intézmény, akihez a dokumentumot fizikailag és tartalmilag hozzárendelték). Egy dokumentum biztonságos védelméhez, mint azt a napi gyakorlat számtalan példával bizonyítja, nem elegendő a három tényező valamelyikének megbízható védelme, sőt mindhárom tényező egymástól független, bár egyidejű védelme sem. A három tényező három relációpárt határoz meg: R1-dokumentum hordozója és tulajdonosa (azaz T1-T3), R2-dokumentum tartalma és tulajdonosa (azaz T2-T3), R3-dokumentum hordozója és tartalma (azaz T1-T2). Teljes biztonságról tehát akkor beszélhetünk, ha az R1, R2, R3 relációk magasfokú biztonságáról egyszerre tudunk gondoskodni. Az R1 reláció biztonsági kérdéseivel

az előző fejezetben foglalkoztam. Most az R2 relációval, vagyis a dokumentum tartalmának és tulajdonosának biztonságos egymáshoz rendelésével, azaz a digitális aláírással foglalkozom. Egyúttal szeretném felhívni a figyelmet bizonyos e tárgyban használatos fogalmi pontatlanságokra, azaz az elektronikus és digitális aláírás közötti jelentős különbségre.

8.3.1. Elektronikus aláírás

Az előzőkben tisztáztuk, hogy a tömegesen előállított papír alapú dokumentumoknál tulajdonképpen megmaradtak a klasszikus dokumentumvédelmi technikák, míg az újabban terjedő elektronikus dokumentumoknál az aláíró személye és a dokumentum tartalma szétválik.
Amint ezt a biometrikus eljárásokkal kapcsolatban bemutattam, bizonyos területeken érdemes kifejezetten személyazonosítás céljából a különböző egyedi személyazonosító jegyeket felhasználni (kézi aláírás, ujjlenyomat, hang azonosítás, stb.). A hagyományos aláírás tehát nem kötődik az aláírt dokumentum tartalmához, hanem csupán az aláíró személyéhez, ez tehát nem tesz eleget az R1 relációnak, hiszen ez csupán a T1 biztonsági tényező. Mindjárt világossá válik a különbség, ha megvizsgáljuk, hogy hogyan kerül a kézzel írott aláírásunk az elektronikus rendszerbe?

A hagyományos módon készített aláírást analóg formában érzékeli egy erre a célra készített berendezés (pl. scanner). Az érzékelésnek, elektronikus letapogatásnak különböző formái vannak, de a közös tulajdonságuk, hogy elektronika segítségével kerül rögzítésre az ember aláírása. Innen származik az elnevezés: *elektronikus aláírás.*

Rá kell mutatni azonban, hogy az elektronikus aláírás itt félreérthető elnevezés. A helyes, habár kicsit hosszú elnevezés az lenne, hogy elektronikus úton rögzített és ellenőrzött kézi aláírás.

A kézi aláírás számítógépes tárolásának legegyszerűbb módjával sokan találkozhattak már a bankokban, ahol aláírásunkat egy scanner (elektronikus letapogató) berendezés segítségével beviszik a számítógépbe. Az így tárolt kézi aláírásunk a későbbiekben gyorsan a számítógép monitorán megjeleníthető és emberi vizsgálattal összevethető egy aktuálisan az átutalásunkon, vagy csekkünkön megjelenő aláírással. Lényeges, hogy ebben az esetben a gépi tároláson kívül minden pontosan ugyanúgy történik, mint hagyományosan papíron. Így már világosan felismerhető a fentiekben leírtak szerint, hogy az elektronikus aláírás tulajdonképpen egy biometrikus azonosító!

Valószínűleg az elektronikus és digitális aláírás fogalmi keveredése pontosan ebben a fázisban érhető tetten. Ugyanis a kézi aláírás elektronikus érzékelését egy digitalizáló eljárás követi, amelynek eredményeképpen kerül tárolásra a számítógépben az aláírás. *Tehát az elektronikus aláírás fentinél is pontosabb meghatározása az, hogy elektronikus úton rögzített, digitálisan tárolt és ellenőrzött kézi aláírás.*

Ahhoz, hogy *a tárolt és az aktuális aláírást gépi úton tudjuk összehasonlítani*, két lépés hiányzik: - az aláírás analóg módon (papír közbeiktatása nélkül) jusson a számítógépbe
- a tárolt és az aktuális aláírás összehasonlítását és kiértékelését egy automatikus program végezze, amely nagy megbízhatósággal eldönti a két aláírás azonosságát, vagy különbözőségét.

A kézi aláírás elektronikus rögzítésére aránylag régóta használnak különböző biometrikus elektronikus készülékeket. Ezek a berendezések speciális érzékelő felület, illetve elektronikus toll segítségével, elektromos jelekké képezik le aláírásunk különböző jellemzőit és magát az írásképet. Ezek a jelek digitalizálás (azaz digitális jelekké való átalakítás) után kerülnek a számítógépben tárolásra. A feladat nem olyan egyszerű, mint amilyennek kinéz, mivel ugyanaz az ember sem tudja a saját aláírását kétszer teljesen egyformán megismételni. A megoldás és így az alkalmazott rendszer lényege is abban rejlik, hogy az aláírás műveletének mely jellemzői azok, amelyek az aláíró állandó személyiségjegyeiből következnek, és ezeket milyen pontossággal képes a rendszer rögzíteni.
Éreznünk kell annak a döntésnek az óriási tétjét, amikor egy automatikus rendszer egy kézi aláírásról eldönti, hogy az valódi-e és utat enged az ezzel hitelesített tranzakciónak!
Úgy tűnik, hogy a legújabb kézi aláírás-ellenőrző rendszerek, a többi biometrikus azonosító rendszerekhez hasonlóan, jó hatásfokkal megbirkóznak ezzel az igen nehéz feladattal.

Hogyan történik az elektronikus aláírás és ellenőrzés?

A későbbi ellenőrzéshez aláírás mintákat vesznek a felhasználótól, mégpedig a rendszerparaméterezéstől függően többet (esetleg több tucatot).
Az aláírást egy grafikus érzékelőlapon elektronikus tollal végezzük, amely érzékeli és rögzíti írásunk számtalan jellemzőjét (tollvonások sebessége, ritmusa, toll nyomás erőssége, szóközök hossza, és egyéb grafológiai jellemzők sokasága).
A legújabb aláírás-elemző rendszerek úgynevezett tanuló algoritmusokat tartalmaznak, amelyek az aláírásminták változásainak szabályszerűségeit is rögzítik („megtanulják”). Ezzel szinte lehetetlenné teszik a nagyon ügyes utánzók (hamisítók) dolgát.

Az elektronikus aláírás mintáit tehát az ellenőrző számítógépben digitalizált formában rögzítve tárolják. Ez a digitális tárolási forma teszi lehetővé, hogy a későbbiekben akár floppy lemezre, akár mágnes, vagy chipkártyára rámásolható az aláírásunk, így elektronikusan megismételhetővé, azaz hordozhatóvá válik. Lényeges megjegyezni, hogy ettől, mint azt a következő részben látni fogjuk, egyáltalán nem digitális aláírásról van szó.

Az ellenőrzési folyamat abból áll, hogy például egy pénzügyi, vagy más szerződéses tranzakció lebonyolításakor (amely ma már akár az interneten keresztül is történhet), a személyazonosság megállapítása végett egy ellenőrző aláírást kérnek az ügyféltől. A számítógépben működő felismerő program eldönti az aláírásról, hogy ugyanazon személytől származik-e, mint a minta. Ha a betáplált adatok (minták) alapján a gép nem képes eldönteni az azonosságot, illetve a különbözőséget, úgy az aláírás megismétlésére szólítja fel az ügyfelet. Amennyiben ez sem egyezik a tárolt mintákkal, úgy a kívánt tranzakciót a gép nem engedélyezi.

Érdemes mindezek alapján megjegyezni az elektronikus aláírásról azt, hogy ez a személyazonosítás egyik korszerű elektronikus eszköze, amely bármennyire pontos, mégis a biometrikus módszerekhez hasonlóan, statisztikus algoritmusok alapján működik, így nem árt, ha alkalmazásakor mód van a gépi intelligenciát felülbírálni képes emberi felügyeletre. Ugyanez a bizonytalansági tényező, mint látni fogjuk nem áll fenn a digitális aláírás esetében.

8.3.2. Digitális aláírás

Ma már a nyilvántartásoknak, az adatforgalomnak egyre kisebb része történik papíron, nagyobb részük számítógépeken keresztül valósul meg. Így a hagyományos, évszázadok alatt kialakult hitelesítési eljárások, mint a kézi aláírás, kézi pecsét, speciális papír, stb. egyre kevésbé járhatók. Ezek korszerű elektronikus helyettesítésére, sőt meghaladására alkalmas az elektronikus adatátvitel és tárolás bármely területén a digitális aláírás.

Az elektronikus aláírással szemben a digitális aláírás magából a dokumentumból indul ki, annak tartalmához és tulajdonosához is szigorúan (nem statisztikus!), algoritmusokkal hozzá van rendelve. Egy másik igen lényeges különbség az, hogy a digitális aláírás kriptológiai eljárás.
Amíg tehát az elektronikus aláírás csupán a fentiekben jelzett három biztonsági tényező közül a T3 azonosítását valósítja meg, addig a digitális aláírás eszközt kínál az R2 reláció megvalósítására.

A digitális aláírás két részből áll. Egyrészt egy a tartalmat hitelesítő karaktersorozatból, ez az úgynevezett *hash függvény*, melyet egy speciális eljárással készít a számítógép a szöveg, adatállomány alapján. Másrészt az aláíró(k) személyét azonosító szintén speciális gépi átalakításból (*rejtjelzés*).

Így a digitális aláírás az "elektronikus irat" tartalmát és az aláíró(k) személyazonosságát is igazolja.

A hash függvény a dokumentumot egy úgynevezett hitelesítő sorozatra (sűrítményre) képezi le, amely biztosítja, hogy a szövegben (dokumentumban) történő akár egy bitnyi változtatás is kiderüljön.

- A *hash függvénnyel* szemben támasztott elsőrendű követelmény az, hogy az azonos hosszúságú hitelesítő sorozatra leképezhető üzenetek száma minden egyes hitelesítő sorozatra nagyjából (nagyságrendileg) azonos legyen.
- Egy másik feltétele a hatékony *hash függvénynek* az, hogy egy megadott hitelesítő sorozathoz ne lehessen hamis üzenetet hozzárendelni, ami azt jelenti, hogy egy A üzenethez tartozó B hitelesítő sorozathoz ne lehessen olyan A’ (A-tól különböző) üzenetet konstruálni, amelynek hitelesítő sorozata B.

A hitelesítő sorozat hosszában optimumot kell találni. Ha nagyon rövid, akkor a teljes kipróbálás segítségével a hamisítást el lehet érni. Ha nagyon hosszú a hitelesítő sorozat, akkor ez az eljárás gazdaságosságát rontja.

A digitális aláírás következő lépése a hitelesítő sorozat rejtjelzése. Ennek a rejtjelzésnek az aláíró személyét kell igazolni, hogy ő az aláírásra jogosult, s ugyanakkor nem más volt a hitelesítő sorozat rejtjelzésének végrehajtója.
A digitális aláírás tehát egy kódolási (titkosító) eljárás, amelynek megoldására különböző kriptológiai módszereket használunk fel. A tömeges felhasználást az úgynevezett nyilvános kulcsú (két kulcsos) módszerek tették lehetővé. Ebben az esetben az elektronikus üzenetet küldő egy saját (titkos) kódkulcsot használ az üzenet titkosítására (rejtjelzésére), míg az üzenetet fogadónak egy másik kulcs (a nyilvános kulcs) áll rendelkezésére, hogy ezt megfejtse (dekódolja). Így az elektronikus kommunikációt úgy is le tudják bonyolítani, ha egyáltalán nem ismerik egymást.

Az elektronikus iroda és az interneten tárolt dokumentumok hitelesség problémájának egyik legkényesebb része a hiteles másolatkészítés. Míg a hagyományos papír alapú irodában a másolatkészítés hitelességének számos megoldása ismeretes, addig az elektronikus irodában a másolatkészítés általában minden hitelességi ellenőrzés nélkül történik.
Míg a hagyományos irodában a másolatok általában indigóval készülnek, így az eredetit a másolattól könnyen meg lehet különböztetni, addig az elektronikus irodában a számítógépes előállítás esetén, az irat eredetiét a másolattól a nyomtatás alapján, vagy más egyszerű módon nem lehet megkülönböztetni. A másolatok hitelességének problémája tehát sok bűncselekmény kiindulópontjául szolgál. Fogalmazhatunk úgy is, hogy ez a hamisítás melegágya.

A digitális aláírás esetén a hagyományos papír alapú irodában használt kettős aláírás (cégszerű aláírás) megvalósítása akadály nélkül teljesíthető, ez esetben a két aláíró fontossági sorrendben képezi a megfelelő digitális aláírást. Vagyis a második aláíró az első aláíró aláírását is hitelesíti.

A digitális aláírás tehát a dokumentum hitelesítésben nagy lépést jelent, mivel a hagyományos kézi aláírásnál, és így az elektronikus aláírásnál is többre képes: egyszerre azonosítja az aláírót és a dokumentum tartalmát.

Sőt ugyanez a technika képes az egyedi dokumentum azonosítók egy szintén klasszikus elemét, a dátumot is beépíteni a digitális aláírásba, ez az úgynevezett időpecsét.

Ugyanis a hagyományos papír alapú irodában egy dokumentum hitelességét az aláíró mellett, a dátum, és iktatószám is biztosítja. Az iktatószámot és a dátumot az elektronikus irodánál az időpecsét váltja fel.
Szerzői jogi kérdéseknél, szabadalmi bejelentéseknél a dátumnak a szokásos év, hónap, napon kívül az órát, percet is tartalmaznia kell. Az elektronikus irodában a dátumnak a másodpercet, esetleg tizedmásodpercet is tartalmaznia kell, mivel a számítógépek műveleti sebessége ezt indokolttá teszi. Tehát, ha a megfelelő pontosságú dátumra és időpontra vonatkozó karaktersorozattal kiegészítjük az aláírandó szöveget és ezután képezzük a digitális aláírást, akkor a dátum és a keletkezés időpontja is beépül a digitális aláírásba, ez az időpecsét.
Így amikor az elektronikus dokumentum célba ér, a fogadónak módjában áll a keletkezés időpontját is biztonságosan leellenőrizni. Hiszen egy illetéktelen beavatkozás (pl. pénz átutalásnál az összeg megváltoztatása) időt vesz igénybe, amely a kommunikációs csatornát ismerve, a fogadónál gyanús késésként jelentkezik. Ugyanígy esélytelen az időpecséttel ellátott dokumentum utólagos visszadátumozása.

Szükségesnek tartom az Olvasó figyelmét felhívni arra, hogy az elektronikus aláírásnál kihangsúlyozott döntési felelősség, amely az alkalmazott módszer biztonságára épül, a digitális aláírásnál legalább oly mértékben fennáll, hiszen érvényesek a 4. fejezetben a rejtjelzések megfejthetőségéről mondottak. Ezért nem tanulság nélküliek az alábbi gondolatok.

A nyilvános kulcsú titkosítás jól demonstrálja az absztrakt matematikai eredmények gyakorlati felhasználhatóságát, de egyúttal rámutat arra is, hogy ez a felhasználás sokszor évszázados fáziskéséssel történik meg.
Jelen esetben az RSA algoritmus megalkotói (Ron Rivest, Adi Shamir és Leonard Adleman) bizonyos asszimetrikus matematikai összefüggéseket használtak fel módszerük elméleti alapjául. Ennek lényege leegyszerűsítve: az mindenki számára azonnal

világos, hogy 5•6=30, de ha az a feladat, hogy írjuk fel a 30-at két szám szorzataként, akkor már jóval több eset lehetséges: 1•30=30 , 2•15=30 , 3•10=30 , 5•6=30

Képzeljük el, hogy 30 helyett, akár többszázjegyű szám lenne a feladat !
Nos, ezt az asszimetrikus tulajdonságot használták ki az 1970-es évek végén algoritmusuk kidolgozásánál az RSA alkotói. Az érdeklődő olvasó számára érdekes lehet, hogy a probléma matematikai felvetése szinte pontosan 100 évvel korábbra, a 19. századig nyúlik vissza.
1873-ban egy W.S. Jevons nevű matematikus vetette fel könyvében, hogy sok esetben a „direkt" matematikai művelet aránylag könnyen elvégezhető, de az „inverz" művelet elvégzése nagyon nehéz. Példa erre (mint az előző illusztráció mutatja) a természetes számok szorzása, melynek „inverz" művelete a faktorizáció, vagyis a szám felbontása prímszámok szorzatára. Így ír erről W.S. Jevons:
„Meg tudja mondani az olvasó, hogy melyik két szám összeszorzásából adódik a 8.616.460.799 szám ? Úgy gondolom reménytelen, hogy akárki (magamat is beleértve), valaha megtudja."
Természetesen akkor még nem voltak másodpercenként több millió műveletet végző számítógépek, így a megoldás csak kézi számolással volt elképzelhető (illetve elképzelhetetlen). A technika nagyot fejlődött azóta. Ma már számítógéppel egy ekkora szám faktorizációja nem okoz problémát. Ezért az RSA algoritmus használatakor többszáz jegyű számokat használnak, amelyek faktorizációja a mai számítástechnika mellett olyan reménytelennek tűnik, mint 1870-ben a Jevons számé.
Ezt a reményt (vagy reménytelenséget) azonban beárnyékolja, hogy 1996-ban S.W. Golomb amerikai matematikus olyan egyszerű eljárást adott, amely kézi számolással 56 lépésben megadja a Jevons szám szorzattábontását, azaz kimutatta, hogy 8.616.460.799= 96.079•89.681.
Ez az eljárás (és az azóta felfedezett több másik) alapvetően megingatja az RSA módszer elméleti és gyakorlati biztonságát. A ma működő információs és kommunikációs rendszerek (internet, hálózati szoftverek, távközlési hálózatok, stb.) több mint 80%-ában RSA alapú információ-védelem van.
Szükségszerűen új korszak előtt állunk tehát. Olyan új kriptológiai módszerek (algoritmusok) bevezetése szükséges, amelyek biztonságát nem a jelen számolási kapacitásának korlátai jelentik, hanem a végtelen átkulcsoláshoz hasonlóan, elméletileg bizonyítható a megfejthetetlenségük.

Az eddigiekben megmutattuk, hogy az R1 és R2 biztonsági relációkra rendelkezünk megbízható, modern hardver és szoftver eszközökkel egyaránt jól kivitelezhető eljárásokkal. Ezek alkalmazásai napjainkban egyre szélesebb körben terjednek. Alapvető problémát okoz ugyanakkor, hogy az elektronikus és elektronikusan előállított „papír alapú" dokumentumok terjedése jóval gyorsabb ütemű, ami kecsegtető lehetőségeket kínál a hamisítóknak és hackereknek. Ennél talán még súlyosabb biztonsági rés keletkezik abból, hogy a dokumentumok biztonságát nem a teljes R1, R2, R3 rendszerrel biztosítják. Hogy ez mennyire így van, azt az mutatja legjobban, hogy bár az R3 reláció elméleti alapjai kidolgozottak, alkalmazása ma még a többitől függetlenül is gyerekcipőben jár.

8.4. Digitális ujjlenyomat, avagy a dokumentumvédelem periódusos rendszere

Az eddigi fejezetekben a „papír alapú” dokumentumok biztonságának tárgyalásához három szempontot vezettem be (a dokumentum adathordozója, a dokumentum adattartalma, a dokumentum tulajdonosa). A három tényező közötti relációk a dokumentumvédelem különböző aspektusait mutatják be, illetve azokra a biztonsági szempontokra hívják fel a figyelmet, amelyekről gondoskodnunk kell, ha dokumentumainkat a funkciójuknak megfelelő maximális biztonságban akarjuk tudni. Az eddigiekben a három alapreláció közül kettővel foglalkoztam, az R3 reláció, azaz a dokumentum adathordozójának és adattartalmának egymáshoz rendelésével még adós vagyok.
Jelen fejezetben ezzel a témával foglalkozom, melynek nem csupán önmagában van kitüntetett jelentősége, de az eddig tárgyalt ismeretek szintéziseként lehetővé válik a dokumentumvédelem teljes rendszerének, mint egyfajta periódusos rendszernek a felvázolása. Ezzel biztosítható a dokumentumvédelemmel kapcsolatos fogalmak és módszerek egyértelmű tisztázása. Ugyanakkor bízom benne, hogy ezáltal sikerül a különböző biztonsági szintek és a hozzájuk tartozó maximális védelmi módszerek rendszerezett bemutatása.

8.4.1. A hiányzó láncszem a digitális ujjlenyomat

Amint az az 8.1. fejezet 8.1., 8.2. összefoglaló táblázataiból jól kivehető , a dokumentumok modern biztonságtechnikája szinte mindent megvalósított a klasszikus biztonsági eszköztárból, csak az új biztonsági filozófia maradt még napjainkban is érintetlen. Ez pontosan azt jelenti, hogy a dokumentum tartalmának azonosítása még mindig független a dokumentum adathordozójától (ezt jelöli az R3 reláció).

A 8.1. fejezetben megfogalmazott új biztonsági filozófia (Legyen mindenegyes dokumentum hordozóját és tartalmát tekintve is egyedi (különböző)…) alapján, ismét fontosnak tartom felhívni az Olvasó figyelmét arra, hogy itt (akárcsak a digitális aláírásnál) csak a későbbiekben ismertetendő távoli rokonság van a digitális ujjlenyomat és az elektronikusan rögzített és bizonyos dokumentumokra (biometrikus azonosítóként felvitt) emberi ujjlenyomat között.

A dokumentumok biztonsági problémái közül (lásd R1, R2, R3 relációk), talán a legnehezebben kezelhető és ezért napjainkban is a leginkább támadható az, hogy el lehessen dönteni egy dokumentumról, hogy az eredeti, vagy hamisított (R3 reláció). Mint azt a fentiekben is jeleztem, a hagyományos módszerek (vízjel, fémszál, különleges papír, hologram, stb.) mindegyike az eredeti dokumentumot igyekszik megkülönböztetni a hamistól, ezért egyre magasabb szintű (ezáltal egyre drágább) technikát alkalmazva igyekszik, például az azonos címletű bankjegyeket tökéletesen egyformára elkészíteni. Ez a biztonsági filozófia a rohamosan fejlődő technika mellett, nem csupán nagyon drága, de igen nehézkessé teszi a hitelesség ellenőrzését is.

Ezzel szemben, a digitális ujjlenyomat az egyedi azonosítást teszi lehetővé kriptológiai módszerekkel, vagyis képes egy dokumentumot nemcsak a hamistól, hanem egy másik eredetitől is megkülönböztetni.

8.4.2. Dokumentumok azonosítása kriptológiai úton

A probléma eredetileg az USA és a Szovjetunió közötti fegyverzet-ellenőrzési szerződések megkötése idején merült fel oly módon, hogy a számbavett rakétákat a legnagyobb biztonsági kritériumok mellett, egy eltávolíthatatlan matricával kellett megjelölni, hogy azok bármikor egyedileg azonosíthatók legyenek.

A nyomdatechnikában általában alkalmazott biztonsági jegyek az ilyenfajta egyedi azonosítást nem teszik lehetővé. J. Simmons több mint két évtizedig vezette az Egyesült Államok nukleáris fegyvereinek elektronikáját gyártó legnagyobb cég, a Sandia National Laboratoriesban folyó kutatásokat a digitális ujjlenyomatok előállítására vonatkozóan (lásd [SIMM 91/1], [SIMM 91/2]). A Sandia laboratórium a több évtizedes kutatás és fejlesztés eredményeit, amit a digitális ujjlenyomatok terén nyert, s amelynek alapvető alkalmazási területe a fegyverzet-ellenőrzés és a felügyelet nélküli szeizmográfok kifejlesztése volt, amelyek a szovjet, illetve amerikai területeken a föld alatti atomrobbantások mérési eredményeinek meghamisíthatatlan észlelésére szolgáltak, más területeken is igyekeztek felhasználni.

- Ilyen terület a pénzhamisítás megakadályozása, amely például az 1999-ben kiadott, új százdolláros bankjegyekben valósult meg. A Sandia által javasolt megoldás a következő:

- a bankjegyek papír anyagának gyártása közben, tehát még pépes formában, árnyékolt üvegszálakat különböző hosszúságban a pépbe kevernek, ezek természetesen megszáradásuk után rögzülnek, és egy véletlenszerű irányultságot vesznek fel. Ezután egy sor letapogatóval el lehet érni, hogy a sorban lévő, és adott sorral egyező végponttal rendelkező üvegszálak, mivel azok megfelelő burokkal vannak ellátva, a fényt csak saját végpontjukig vezetik. Mivel az üvegszálak hossza véletlenszerű, ezért egy vonali megvilágításból egy véletlenszerű ponthalmaz adódik. Ezt természetesen több vonalon meg lehet ismételni. Az eredményként létrejövő ponthalmaz megfelelő technikával történő kódolási eljárásával el lehet érni, hogy az adott bankjegyre jellemző kód, vagy kódsorozat jöjjön létre. Ezeket a kódokat digitális aláírással, a bankjegyre vonatkozó más tartalmi adatokkal, például sorszámmal, kiadási időponttal, címlettel kiegészítve a kibocsátó bank hitelesíti. Ilyen módon a digitálisan aláírt kódsorozat és a bankjegyben lévő, véletlenszerűen elszórt üvegszálak kölcsönösen megfeleltethetők egymásnak.

Ha az üvegszálak száma és hosszúságuk megfelelően van meghatározva (ami nem egyszerű és mély matematikai meggondolásokat igényel), akkor a bankjegyeken lévő kódok egyértelműen meghatározzák a bankjegyet. Egy ilyen eljárás, szemben a különböző nyomdai megoldásokkal, amelyek nem egyediek, az egyediségből adódóan számos előnnyel bírnak. A papír anyagában lévő jellemzők pedig másolhatatlanná teszik a bankjegyeket.

A digitális ujjlenyomat tehát a digitális aláírás egy olyan különleges esete, amikor az aláírásra kerülő üzenet egy része, vagy egésze, a hordozó anyag fizikai jellemzőiből adódik. Ez azt jelenti, hogy például mindenegyes bankjegy egyedileg megkülönböztethető minden más bankjegytől, hiszen nincsen olyan ív papír, amelynek bármely darabja, anyagát tekintve teljesen egyforma lenne, ha azt a papír gyártásakor (a fenti értelemben vett) véletlenszerűen „szennyeződéssel” látjuk el.

A digitális ujjlenyomat tehát nem teszi lehetetlenné a másolást, azonban az eredeti és a hamis bankjegy egymástól megkülönböztethetővé válik, mert az egyedi sajátosságok (a bankjegy anyagába bevitt jelző elemek) elhelyezkedése nem másolható.

A pénzhamisítás megakadályozására egy ugyancsak digitális ujjlenyomatokra visszavezethető módszer került kidolgozásra és felhasználásra Németországban az 1990-es években kiadott német márka (DEM) bankjegyek védelmére. A német márkákon levő 11 karakterből álló karaktersorozat tehát nem egyszerű sorszám, nem egyszerű azonosító kód volt, hanem digitális ujjlenyomat.

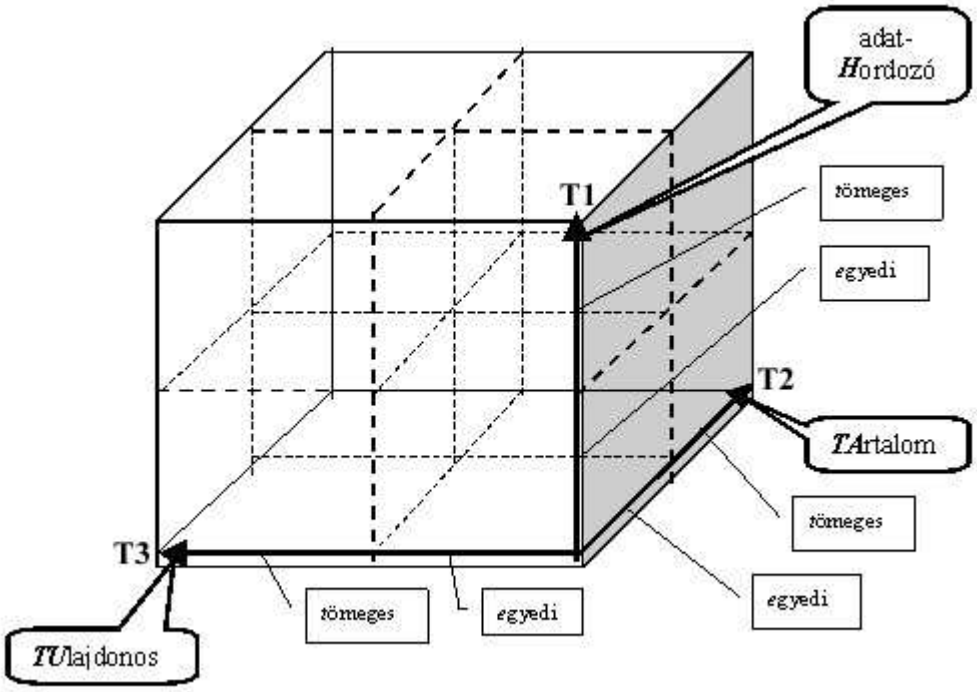
A német márka digitális ujjlenyomata úgy készült, hogy a papír gyártási folyamata során a pépbe foszforeszkáló szórat darabkák kerültek bekeverésre (hasonló módon, mint a dollár esetében), majd a létrejött papír tartalmazta ezeknek a fényvisszaverő szóratoknak egy véletlen elrendezését. Ezt a véletlen elrendezést kellett kódolni, vagyis az egyedi azonosításra rendelkezésre álló, a papír anyagából eltávolíthatatlan, és megismételhetetlen fényvisszaverő morzsalékot kellett egy megfelelően biztonságos digitális aláírás segítségével a bankjegyen lévő kóddal kifejezni. Ez a kód egyértelművé tette a bankjegy egyedi sajátosságát, és a bankjegyen lévő kibocsátó által ráírt (rányomtatott) számsorozat közötti összefüggést.

Tehát a digitális ujjlenyomat alkalmazásával a hamisítókat egyrészt el lehet rettenteni a hamisítástól, másrészt a hamisítást könnyen és gyorsan föl lehet ismerni, hiszen maga a dokumentum tartalmazza az ehhez szükséges összes információt. Így a hamisítás ténye helyben, azonnal megállapítható.

A digitális ujjlenyomat biztonsági papírok előállítására is alkalmas, sőt egy újonnan vizsgált és bevezetéshez közel álló területe a digitalizált analóg jeleknek, például digitális hangszalag, floppy lemez, CD lemez, vagy videoszalag, mint digitális adathordozó dokumentum, másolás elleni védelme.

A digitális ujjlenyomat tehát az R3 reláció minden eddiginél biztonságosabb megoldására alkalmas, akárcsak az R1, vagy R2 esetében a biometrikus azonosítók. Hiszen, míg a biometrikus azonosítók a dokumentum tulajdonosának egyedi jellemzőit rendelik a dokumentumhoz, addig a digitális ujjlenyomat, az adathordozó egyedi jellemzőivel teszi ugyanezt. Ezzel megnyílik a lehetőség arra, hogy mindhárom relációt egyetlen digitális aláírásban, egyetlen kódsorozatban egyesítsünk, amely a dokumentum minden alapvető tulajdonságát kriptológiai úton rögzíti, ezzel biztosítva a maximális biztonságot akár a lopás, akár bármilyen típusú hamisítás ellen.

Összegzésül az alábbi 8.3. ábra egy háromdimenziós rendszerben mutatja be az eddigiekben bevezetett T1, T2, T3 tulajdonságokat és az R1, R2, R3 relációkat. Ezt a rendszert tekinthetjük a dokumentumvédelem periódusos rendszerének is, mivel dokumentum biztonsági szempontból, bármely dokumentum az így keletkező nyolc részkocka valamelyikében elhelyezhető.



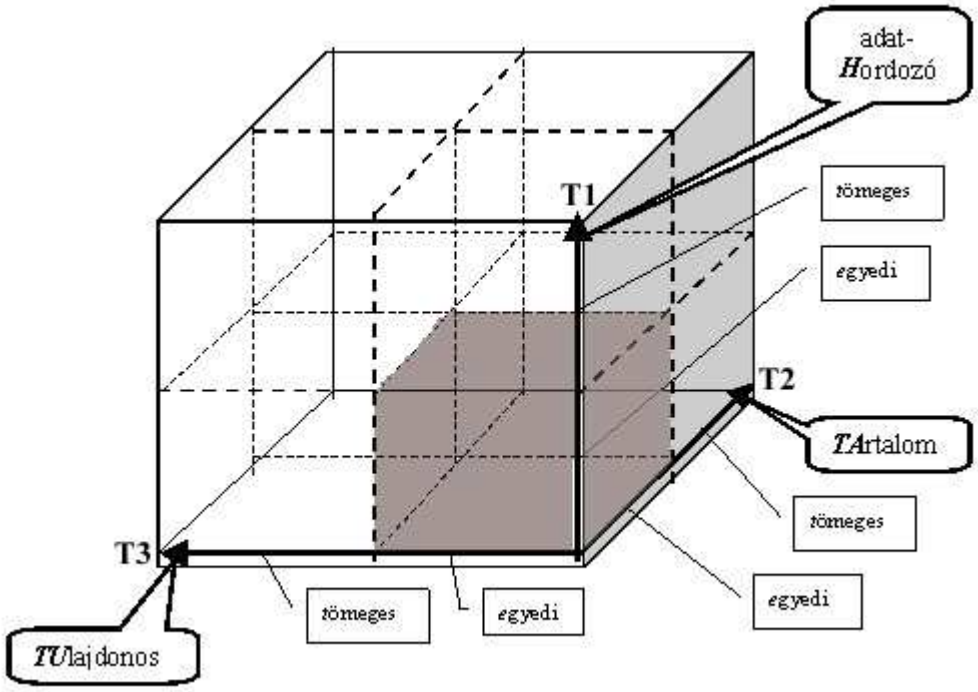
8.3. ábra A dokumentumvédelem periódusos rendszere

A rendszer létjogosultságának demonstrálására, mind a nyolc lehetséges kategóriára álljon itt néhány példa. Az egyes dimenziókat az elnevezésük kezdőbetűivel jelöljük:

- *H = adathordozó*
- *TA = tartalom*
- *TU = tulajdonos*

Minden dimenzióban megkülönböztetjük az egyedi (e) és tömeges (t) dokumentumokat, amelyet a dimenziók jelének indexeként jelölünk (pl. H_e= egyedi adathordozó). Így a következő kategóriákat kapjuk (egy-egy példával illusztrálva):

1. $H_eTA_eTU_e$ – Biztonsági „papírra" készült (digitális ujjlenyomattal ellátott), bizalmas tartalmú, személyhez kötött dokumentumok - igazolványok, bankkártyák, stb. Ezt a kategóriát mutatja a 8.4. ábra besatírozott részkockája.



8.4. ábra $H_eTA_eTU_e$ a legmagasabb biztonsági kategóriájú dokumentum típus

2. $H_eTA_eTU_t$ – Biztonsági „papírra” készült (digitális ujjlenyomattal ellátott), bizalmas tartalmú, nem személyhez kötött dokumentumok – értékpapírok, bankjegyek, stb.

3. $H_eTA_tTU_e$ – Biztonsági „papírra” készült (digitális ujjlenyomattal ellátott), nem bizalmas tartalmú, személyhez kötött dokumentumok – dedikált fotó, stb.

4. $H_eTA_tTU_t$ – Biztonsági „papírra” készült (digitális ujjlenyomattal ellátott), nem bizalmas tartalmú, nem személyhez kötött dokumentumok – postai bélyegek, stb.

5. $H_tTA_eTU_e$ – Nem biztonsági „papírra” készült (jelenleg használt alapanyagú), bizalmas tartalmú, személyhez kötött dokumentumok - igazolványok, bankkártyák, stb.

6. $H_tTA_eTU_t$ – Nem biztonsági „papírra” készült (jelenleg használt alapanyagú), bizalmas tartalmú, nem személyhez kötött dokumentumok – utazási jegyek, bérletek, stb.

7. $H_tTA_tTU_e$ – Nem biztonsági „papírra” készült (jelenleg használt alapanyagú), nem bizalmas tartalmú, személyhez kötött dokumentumok – dedikált könyv, fotó, stb.

8. $H_tTA_tTU_t$ – Nem biztonsági „papírra” készült (jelenleg használt alapanyagú), nem bizalmas tartalmú, nem személyhez kötött dokumentumok – szórólapok, könyvek, újságok, stb.

9. Az Internet, avagy a globális hálózatok biztonságáról

„Fontosnak tartottam, hogy legyen egy új kifejezés arra, amikor az adatfolyam egy-egy rövidebb darabja elkülönülten kerül átvitelre a hírközlő csatornán. Gondoltam, ez könnyebbé teszi e fogalom használatát. Rátaláltam a szórengetegben a szóra: «csomag», ami nem jelentett mást, mint egy kisebb adatköteget."
(Donald W. Davies, The Guardian, 1997/6.)

Turing már a modern számítástechnika hajnalán, 1946-ban készített tanulmányában felhívta a figyelmet arra, hogy az általa tervezett ACE (*Automatic Computing Engine*) számítógép alkalmas távoli felhasználók telefonvonali összekötésére (lásd az 5. fejezet záró gondolatát). Vagyis előre látta a számítástechnika és a telekommunikáció összekapcsolásának lehetőségét. Korai halála megakadályozta abban, hogy korszakos gondolatát megvalósítsa, de gondolatcsírája mégis kivirágzott, mivel egyik tanítványa, *Donald Watts Davies* (1924-2000) lett a *„csomag-kapcsolás"* alapelvének úttörője és így az első csomag-kapcsolt hálózat, az ARPANET kifejlesztője.

Donald Watts Davies (1924-2000)

Az internet egyszerre forradalmasította a számítástechnikai, a híradástechnikai és az egész infokommunikációs világot, példa nélküli integrációs képessége megteremtette azt a már több évtizedes látomást, hogy egy világhálózat kerekedjék ki, amely számítógépek millióit tudja összekötni, tekintet nélkül azok földrajzi elhelyezkedésére.
Két lényeges vonása van az internetnek, ami ezt a rendkívül fontos célt elérhetővé tette, nevezetesen a csomag-kapcsolás és a nyílt struktúrájú hálózat.
A 20. század végi és 21. századi információalapú társadalmak kialakulásában az internet alapvető szerepét el kell ismerni, ugyanakkor szükséges annak megvilágítása, hogy biztonság szempontjából az internetnek komoly hiányosságai vannak. A megfelelő biztonság hiánya különösen felértékelődik egy olyan rendszerben, amely egyre inkább a társadalom működésének alapját képezi. Súlyosbítja a helyzetet, hogy ezeket a hiányosságokat sajnos a felhasználók nagyon kismértékben ismerik fel, e veszélyérzet hiányát a biztonság tekintetében talán a leglényegesebb problémaként kell jelezni.

Ebben a fejezetben a globális hálózatok és az ezekre épülő rendszerek, mint például az elektronikus kereskedelem, vagy a banki alkalmazások biztonsági problémáiról lesz szó, különös tekintettel a hozzáférés-védelemre, az adatbankok hitelességére vagy a legújabb pénzkímélő törekvésre, a digitális pénzre, amelyek biztonságának modern eszközei az intelligens chip- vagy memóriakártyák.

Donald Watts Davies 1947. szeptemberében egy kis kutatócsoporttal együtt csatlakozott a II. világháborúban híressé vált, de mégis szigorúan titkos Bletchley Parkban működő, Turing által vezetett laboratóriumhoz. A laboratórium alapvetően Turing tervei alapján dolgozott a Pilot ACE számítógépen, amelyen az első program 1950. május 10-én futott. Ted Newman, Jim Wilkinson és mások mellett Donald W. Davies alapvető szerepet játszott a gép megtervezésében és megépítésében. Ilyen tapasztalatok birtokában került a laboratóriumból az iparba. Széles érdeklődési köre felölelt minden területet, ahol elképzelhető volt a számítógépek alkalmazása (például megépített egy közúti közlekedés-szimulátort).

Turing, sok egyéb korszakos gondolata mellett, először adta meg az elektronikus számítógépek programozásának pontos leírását is, így érthető, hogy Donald Davies közvetlen munkatársaként, annak kitűnő képességeit kamatoztatva, képes volt a döntő áttörésre a modern számítógépes kommunikáció megteremtése terén. Ez volt az úttörő jelentőségű „csomag-kapcsolás" gondolata, amely lehetővé tette a számítógépek közötti gyors adat- és információcserét.
1954-ben a Commonwealth Fund tagjai közé választotta, ajánlásában többek között ez olvasható: „Ajánlásra méltó nem csupán rendkívüli intellektusa, de tudományos, technikai és általános ismeretei alapján is. Ő az egyike azon keveseknek, akik képesek egy elektronikus számítógép komplett logikai tervét elkészíteni, megvalósítani azt konkrét áramkörök formájában, és önállóan összeállítani úgy, hogy az nagy valószínűséggel a tervek szerint fog működni. Majd képesek erre a gépre olyan programot írni, amellyel megoldhatók a kiszámítandó problémák."

Meglepően újszerű gondolkodásáról tanúskodik, hogy már 1958-ban létrehozott egy kutatócsoportot, amely számítógépet alkalmazott technikai szövegek oroszról angolra fordítására, majd 1963-ban kinevezték a számítógép-fejlesztési project technikai vezetőjének. Tulajdonképpen Albert Uttley örökébe lépett, mint a National Physical Laboratory (NPL) önálló osztályának igazgatója, amelyet nemsokára számítástudományi osztállyá alakított át, és új kutatási területeket jelölt ki, amelyek kulcsát az általa 1965-ben kidolgozott számítógépes hálózatok elmélete alkotta. Ennek lényege, hogy a számítógépek közötti gyors üzenet-átvitel szükségszerű velejárója a hosszú üzenetek feltorlódása, ezért szét kell választani azokat kisebb kötegekre, így minimalizálható a torlódás és az átvitel kockázata. A kisebb üzenetkötegeket nevezte el „csomagok"-nak, és az átviteli technikát „csomag-kapcsolás"-nak.
Donald W. Davies alaposságára jellemző, hogy amikor e kifejezések használata mellett döntött, amelyek az akkori számítástechnikában teljesen új gondolkodásmódot képviseltek, két nyelvész kutatótársának véleményét is kikérte, hogy a szavak értelmezhetők legyenek más nyelvekben is.

Davies számítógépes hálózatokra vonatkozó tervét lelkesen fogadta az *America's Advanced Research Project Agency* (ARPA), így lett az ARPA és az NPL közös hálózata az első számítógépes hálózattá a Földön, amelyet ARPANET-nek neveztek el. Ez az eredeti gyökere a mára internetté terebélyesedett világhálónak.

1979-ben Davies lemondott az NPL-nél betöltött vezető pozíciójáról, és tisztán a technikai munkákra koncentrált. Széles körben használható számítógépes hálózatokat hozott létre, különös figyelemmel a káros hatások megelőzésére. Ezért alapította meg az adatbiztonsággal foglalkozó csoportot, amely már egy új biztonsági filozófiára, a nyilvános kulcsú kriptográfiai rendszerekre koncentrált. A csoport szakértőivel igen erős konzultációs tevékenységet épített

ki például a brit bankvilágban. 1984-ben nyugalmazott adatbiztonsági szakértőként folytatta tevékenységét. 1987-ben a Royal Society (az Angol Tudományos Akadémia) tagja lett, és vendégprofesszor a Royal Holloway és Bedford New College-ban.

Davies szellemi nagyságát bizonyítja, hogy utolsó megvalósult terveként, a Pilot ACE megépítésének 50. évfordulójára megalkotta e gép szimulátorát egy korai modern személyi számítógép számára. 1997-ben a The Guardian-be írt cikkében a következőképpen foglalja össze alapvető gondolatait:
„1965. novemberében gondoltam a célzottan tervezett hálózatoknál a csomag-kapcsolás alkalmazására, azaz az adatfolyamot rövidebb üzenetekre, csomagokra tördelni, amelyek mindegyike önállóan találja meg a célhoz vezető utat, ahol azután ismét összeállnak az eredeti adatfolyammá."

9.1. Az Internet kialakulásából fakadó gyengeségek

Az 1966-67-es években létrejött a kaliforniai UCLA Egyetemen egy hálózati központ, ez volt az ARPANET-nek az első csomóponti berendezése. Később, 1969-ben az UCLA kísérleteit kibővítették, és kialakultak a mai Internet hálózathoz hasonló hálózat csírái.

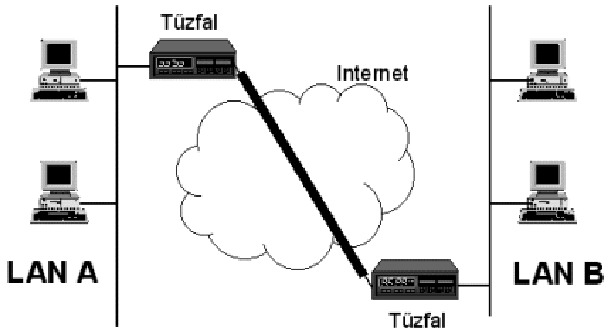
A mai Internet egyik fő alkalmazási területe először 1972-ben került bemutatásra, az ARPANET elektronikus postaként való felhasználásával. Ezzel tulajdonképpen megvalósult egy olyan számítógépes hálózati összeköttetés, amely közvetlen kapcsolatot teremtett a felhasználók között. Az 1980-as években kezdődött el a személyi számítógépeken és a munkaállomásokon alapuló lokális hálózatok elterjedése, ami később, a 80-as évek végén vezetett az Internet mai architektúrájának megalkotásához. Az 1980-as évek végétől beszélhetünk Internetről annak mai formájában. Megjelentek az internetszolgáltatók és az Internet széles körben elterjedt a kutató-fejlesztő környezeten kívül is, vagyis kereskedelmi szolgáltatássá vált.

Jelenleg, amikor az elektronikus postai szolgáltatások mellett számos más szolgáltatás is (például home banking, elektronikus kereskedelem stb.) megjelenik a hálózaton, világosan kiütközik az Internet fejlődéséből adódó probléma, nevezetesen, hogy a főleg kutatókra, fejlesztőkre, tehát alapvetően azonos érdekeltségű és motivációjú résztvevőkre épülő Internetet megelőző hálózatoknál a fejlesztők és a felhasználók *sem tekintették alapvető kérdésnek a biztonságot*. Ez a felfogás, a veszélyérzet szinte teljes hiánya a tömeges felhasználásnál visszaüt, és az Internetet nagyon sebezhető globális hálózattá teszi.

Jelenleg az Internet a biztonság utólagos megteremtésének problémájával küzd, és szemben egy olyan megoldással, amikor a biztonság a szolgáltatással együtt épül be a rendszerbe, igen gazdaságtalan is.

Az Internet környezete megváltozott, és a közös kutatást végző, kollégiális kapcsolatban álló kutatók mellett megjelentek a tömeges alkalmazások, sőt, ahogy arra a 7. fejezetben rámutattunk, a „láthatatlanság", „felismerhetetlenség" homályába burkolódzó, bűnözésre hajlamos egyének, és potenciálisan a szervezett bűnözés eszközévé (is) vált a világháló.

Tehát kétféle típusú veszélyforrás kiküszöbölése látszik a legfontosabbnak, az egyik a rendszerhez való *hozzáféréssel kapcsolatos védelem*, a másik, hogy a szolgáltatás egy biztonságos operációs rendszerbe legyen beépítve, azaz *a rendszerben tárolt temérdek adat biztonsága*.



9.1. ábra

9.2. A tűzfalak biztonsága

A hozzáférés-védelmet az Interneten a tűzfal biztosítja. Az elnevezés a régi építkezésekből ismert téglafalból ered, amely a házakat elválasztotta egymástól, és ezáltal megakadályozta a tűz továbbterjedését. A tűzfalak Internet-rendszerbe illesztését szemlélteti az 9.1. ábra.

Az egyenszilárdság elvének[65] megtartása nagy hálózatokban igen nehéz, mivel a hálózatban lesznek tűzfalat nem használó és gyenge tűzfalat használó végpontok is. Az ezek közötti színvonalkülönbség könnyen kihasználható, és egy helytelen konfigurálás, egy rosszul megválasztott jelszó nagy károkat okozhat az egész hálózatban.

Egy tűzfalrendszer általában két részből áll. Egyrészt egy útvonal-kiválasztóból, másrészt egy illetékességet vizsgáló szerverből. Az *útvonal-kiválasztó* olyan, egy vagy több ponttal rendelkező elrendezés, amely számos szabályt ellenőrizhet a bejövő üzenetcsomagokban. Ezeknek a szabályoknak az ellenőrzése során eldöntheti, hogy az adott csomagot továbbítja vagy sem. A megfelelő információkat az üzenet fejlécében lehet elhelyezni, ilyen lehet a használt protokoll (algoritmus) azonosító száma, az üzenet forrása és címzettje (címekkel megadva), a port sorszáma, esetleg számos más opció.

Az *illetékességet vizsgáló szerver* olyan algoritmusokat valósíthat meg, amelyek a felhatalmazás megadását (a hozzáféréshez) a felhasználó részéről elbírálhatják. Ugyancsak a tűzfal feladata eldönteni, hogy az érkező üzenetet befogadja-e. Természetesen ezeket a funkciókat, vagyis a forrás-azonosítást, az információ hitelességének az eldöntését különböző algoritmusok valósíthatják meg. A tűzfal hiánya az Internet globalizációjával egyre veszélyesebb.

Ahol alkalmaznak tűzfalakat, ott az esetek egy részében gyenge megoldások kerülnek felhasználásra, mint például az egyszerű jelszó. A tűzfalak tehát akkor lehetnek hatásosak, ha a bennük megvalósuló védekezés biztonságos algoritmusokra épül, ilyen például az *egyszer felhasználható* vagy *dinamikus jelszó*.

[65] Egyenszilárdság alatt az információs rendszerek azon tulajdonságát értjük, hogy a rendszer bármely pontjának biztonsága azonos erősségű biztonsági alrendszerrel védett (lásd [VASVÁRI 2009]).

Az egyszer felhasználható jelszó előképét már a rejtjelzés fejezetben láttuk, ez a *one time pad*, vagyis a végtelen átkulcsoláshoz használt egyedi kód generálás. Elöljáróban még néhány további veszélyforrásra is fel kell hívni a figyelmet, mint például:

- a nyilvános kulcsok listájának manipulálása,
- a belső árulás, vagyis az, hogy a még el sem küldött nyílt szövegeket egy beépített, úgynevezett „trójai faló programmal" egy behatoló részére nyílt szövegként elküldi, így semmiféle rejtjelfejtési vagy egyéb elemzési módra nincsen szükség a nyílt szöveg megszerzéséhez,
- veszélyt jelent a forgalomanalízis,
- valamint a hierarchikus rendszereknél a rendszergazda árulása (emberi tényező).

A védekezés biztonságának növelését teszi lehetővé a tűzfalaknak a mai egyszerű, azaz többször használatos jelszónál lényegesen biztonságosabb dinamikus jelszóval való működtetése, illetve az úgynevezett kettős tűzfalak bevezetése.

A kettős tűzfal azt jelenti, hogy a tűzfal nemcsak egy irányba, tehát az Internettől a felhasználó felé véd, hanem a felhasználótól kimenő információkat is megszűri, és ezáltal megnehezíti az olyan árulásokat, ahol egy bennfentes alkalmazott az Internet vonalán keresztül küld egy illegális partner számára üzeneteket. A kulcsfelhasználás szempontjából bizonyos fokú védelmet jelent például, ha a nyilvános kulcs használata esetén a személyre szóló titkos kulcsot nem tárolják a gépben, hanem az az illető személyes használatába kerül, és ennek megfelelően személyes felelősségével, egy külön chipkártyán nyer elhelyezést. Mindezek a megoldások, amelyek ma még sajnos nem széles körben alkalmazottak, sem jelentenek tökéletes biztonságot.

Egy egész más területről vett példán bemutatva, az autópályák elkerülik az azonos szintű kereszteződéseket, és ezáltal lényegesen csökkentik a balesetek számát. Azonban senki sem gondolja azt, hogy egy autópályán nem lehet baleset, vagyis hogy az autópálya bevezetése minden közlekedési balesetet kiküszöböl.

Az Internet közel sem teljes biztonsági réseinek felsorolását az Internettel kapcsolatos jogvédelmi problémák tovább árnyalják.

A szellemi tulajdonok védelmével foglalkozó genfi székhelyű nemzetközi szervezet, a *World Intellectual Property Organization* (WIPO) 1999-ben, Genfben tartott konferenciáján foglalkozott az úgynevezett *elektronikus kihívással*, ami azáltal fenyeget, hogy az internetről letölthető, szerzői jogvédelem alá eső műveket jogdíj megfizetése nélkül lehet rögzíteni, illetve terjeszteni. A WIPO komolyan foglalkozik az interneten közvetített szellemi alkotások (audió, videó, film, tévéprogram, szoftver stb.) védelmének és az ezek után járó szerzői díjak beszedésének kérdésével.

Az Internet egy kiegészítő szolgáltatása a *„dial in"*, ami azt jelenti, hogy a jogszerű internet-felhasználó nem a saját termináljáról, hanem egy másik, esetleg földrajzilag nagy távolságban lévő terminálról is elérheti saját adatállományát. Például lekérheti az elektronikus postán (e-mailen) érkezett üzeneteit. (Ez a szolgáltatás hasonlít az üzenetrögzítőhöz, illetve a mobiltelefonnál használt hangpostához).

Sajnos a rosszul szervezett *dial in* szolgáltatás többször használatos jelszóval védett az esetek túlnyomó többségében. Így a jelszó lehallgatása, mivel az külső, nem védett módon megy végbe, még egyszerűbb. A megoldás a dinamikus vagy egyszer használatos jelszóval működő, visszahívást lehetővé tévő tűzfal beépítése.

A vírusok Interneten keresztüli terjesztésének megakadályozása is szükségessé teszi a jól felépített tűzfalak használatát.

A fentiek alapján a valódi probléma tehát, hogy a biztonság utólagos beépítése nem ad megfelelő megoldást, és igen költséges, mivel például a biztonsági követelményeket ki nem elégítő alapszoftverek (ilyen a forgalomban lévő alapszoftverek döntő hányada) lecserélését vonná maga után.

Ugyanakkor illúzió azt hinni, hogy a számítógépes biztonság problémája az USA-ban vagy akár az Európai Unió nálunk fejlettebb országaiban megoldott, s csak megfelelő technológiatranszfer szükséges a hazai megoldáshoz.

9.3. Az elektronikus kereskedelem biztonsága

Az Internetről leírtak több-kevesebb változtatással az elektronikus adatcserére (Electronic Data Interchange = E.D.I.) is érvényesek. Az E.D.I. igen lényeges része az úgynevezett papírmentes irodának, és fontos alkalmazási területe a jelenleg kulcsfontosságú, rohamos fejlődés alatt álló és globalizálódó elektronikus kereskedelem.
Az elektronikus kereskedelem a műszaki adottságok mellett számos jogi és kereskedelemszervezési problémát vet fel, így fontos tudni, hogy az elektronikus kereskedelem előmozdítása gazdaságfejlesztési tevékenység (nem csupán számítástechnika).
AZ ENSZ Kereskedelmi Jogi Bizottsága kidolgozta az elektronikus kereskedelemre vonatkozó mintajogszabályt, amelynek alapelve, hogy – bizonyos követelmények betartása esetén – semmilyen bizonylatot nem lehet arra hivatkozva visszautasítani, (annak hitelességében kételkedni), hogy az elektronikus úton készült.
Eme alapelv érvényesítésének szükséges feltétele a digitális aláírás segítségével történő hitelesség igazolása. Így kap kiemelt hangsúlyt, hogy a kriptológián belül a hitelesség-vizsgálat jelenleg az elektronikus kereskedelem szempontjából műszaki és jogi vonatkozásban is a legfontosabb terület.
Az elektronikus kereskedelem az üzleti információk szétosztását, az üzleti kapcsolatok ápolását és az üzleti tranzakciók végrehajtását jelenti, hírközlési csatornák segítségével.

Ebből a definícióból kiviláglik, hogy az elektronikus kereskedelem nincs szorosan az Internethez kötve, de ugyanakkor az Internet az e-kereskedelemnek egy lehetséges és igen gyakran használt terepe.
Az elektronikus kereskedelem, hasonlóan a hagyományos kereskedelemhez, három részre oszlik, nevezetesen az ügyfél és a kereskedő közötti kapcsolatra, a kereskedők egymás közötti kapcsolatára és a kereskedelmi szervezetek közötti kapcsolatokra. Ez a felosztás megfelel a kiskereskedelem, nagykereskedelem és külkereskedelem szokásos felosztásának.
Az elektronikus kereskedelem tervezésénél szinte teljes mértékben az Internet-hálózatot veszik figyelembe. Ugyanakkor fel kell hívni a figyelmet W. W. Wu. [Wu 1999] cikkére, amelyben a szerző az *Egyesült Államok Szövetségi Hírközlési Bizottságára* (FCC) hivatkozva megállapítja, hogy a műholdas távközlési piac az eddiginél nagyobb növekedésre számíthat.
A műholdaknak egyre kitüntetettebb szerepe van, és kulcsszerepe lesz a globalizációban, mivel szinte semmi összefüggés nincs a költség és a távolság között. Bizonyos piacokon a műholdak kínálják az egyetlen gazdaságos megoldást. Az FCC megállapította, hogy a világ összes háztartásának az internetes, fénykábelekkel való összekötése kb. háromszázmilliárd USA-dollár költséggel járna, míg ugyanennek a feladatnak a műholdak segítségével való megvalósítása csupán ennek 3%-a lenne.

Az eddig nem tárgyalt problémák közül ki kell emelnünk azt, hogy amíg az elektronikus kereskedelem, vagyis a papír nélküli iroda számos előnnyel jár, addig egy vonatkozásban biztosan biztonsági kockázatot jelent. Nevezetesen könnyen előfordulhat, hogy a bizonylatokat (ez esetben elektronikusan tárolt információkat) fizikai, esetleg tartalmi sérülés éri, például véletlenül vagy szándékosan letörlik, vagy eltulajdonítják. Ez sokkal könnyebben véghezvihető, mint a papír alapú irodában. Ennek a kockázati tényezőnek az elhárítása csak látszólag könnyű, azonban a tényleges megoldás nem egyszerű. Ha utólagosan az elektronikusan tárolt információkat kinyomtatás útján papír alapúra változtatják, akkor az elektronikus irodának, jelen esetben az elektronikus kereskedelemnek az előnyei szinte teljesen elvesznek. Így tehát az elektronikus dokumentumok esetében különös figyelmet kell fordítani az elektronikusan tárolt adatok rendszeres, kötelező mentésére és számítógép-terminálóktól vagy számítógép-központoktól független, biztonságos tárolására. Az elektronikus kereskedelem biztonságát biztosító komponensek:

Digitális aláírás
A keletkezett elektronikus dokumentumok tartalmát, valamint az aláírót (személy vagy akár szervezet) egyszerre hitelesíti a digitális aláírás.

Kulcsletéti rendszer
A hitelesítéshez felhasznált eszközök hitelességét biztosítja a kulcsletéti rendszer. Ugyanis úgy a belföldi, mint a nemzetközi kereskedelemben biztosítani kell, hogy az aláíró hitelesítő kulcsait, azaz a személyének hitelesítését egy erre a célra működő szervezet (szerver) biztosítsa. Vagyis a kereskedelemben részt vevők kötelezve legyenek arra, hogy a kulcsokat, amiket a digitális aláírásoknál, illetve a rejtjelzésnél használnak, letétbe helyezzék. Biztonsági okoknál fogva ezt célszerű úgynevezett *titokmegosztás* segítségével több szervezetre bízni oly módon, hogy az egyes szervek csak egy kulcsrészlettel rendelkezzenek. Ez azt jelenti, hogy az üzenet kezdeményezője nem a címzettnek küldi az üzenetét, hanem egy olyan szervezetnek (szervernek), amelyik a továbbítás előtt az üzenet hitelességét meg tudja vizsgálni, és a címzett részére tudja garantálni.
A világméretű elektronikus kereskedelem egyre inkább előtérbe helyezi az űrtávközlés (VSAT terminálok) felhasználását. Úgy a hibajavító kódolás, mint a kriptológiai algoritmusok fontos és különleges szerepet játszanak az űrtávközlésben. A VSAT-terminálokhoz csatlakozó nagy kapacitású űrtávközlési csatornáknak csak kis hányadát tudja egy kereskedelmi felhasználás kihasználni. A fennmaradó szabad kapacitás lehetővé teszi a biztonság lényeges növelését, ez pedig a folyamatos rejtjelzést.
Prognosztizálható, hogy a 21. században a papír nélküli iroda elterjedése nemcsak az elektronikus kereskedelemben, hanem annál szélesebb körben, a közigazgatás egészében vagy akár a távoktatásban, sőt a teljes infokommunikációban is meg fog jelenni. Tehát *nem lehet túlbecsülni a 21. század információs e-társadalmában az információbiztonság jelentőségét.*

9.4. Banki alkalmazások biztonsága

Az elektronikus kereskedelem sok hasonlóságot mutat a jelen valóságában már létező pénzforgalmi E.D.I.-kkel, azaz az *Electronic Fund Transfer* (EFT) rendszerekkel. A hasonlóság elsősorban abban mutatkozik meg, hogy a kiskereskedelem banki megfelelője, a *home banking* segítségével az ügyfelek (ezek lehetnek magánszemélyek, gazdálkodó egységek, közhivatalok) lakásukról vagy telephelyükről adatátviteli kapcsolatot létesíthetnek bankjukkal, bankszámlájukkal bankműveleteket végezhetnek, illetve kezdeményezhetnek. A home banking gyorssá és kényelmessé teszi az ügyfelek számára a pénzműveleteket.

A bankok számára ez az új szolgáltatás a vitathatatlan előnyök mellett jelentős kockázatokat is hordoz. Az ügyféllel létesített kapcsolat támadási lehetőségeket is kínál. Ugyanakkor az ügyfélnek elvárása, hogy a bank e szolgáltatása ne jelentsen fenyegetettséget a bankkal folytatott üzleti tevékenységre nézve. Ezen veszélyforrások kiküszöbölésére alkalmazhatók a már korábban ismertetett tűzfalak.
Hasonlóan az elektronikus kereskedelemhez, itt is a hozzáférés-védelmet, a digitális aláírást és a hitelesítő szervezetek közbeiktatását lehet megoldásként alkalmazni. Az egyenszilárdság elve megköveteli, hogy az ügyfél a saját végpontján biztosítsa az egyéb védelmi intézkedéseket (például fizikai hozzáférés-védelem).

Az elektronikus kereskedelemnél leírt nagykereskedelmi rendszer itt a bankok közötti elszámolási rendszer, a *„zsiró”*. Míg a homebanking-rendszereknél a jelenleg használt védelem általában nem elégséges, ugyanis többször használatos jelszavakon alapul, addig a „zsiró”-rendszerben a létrehozással egy időben már bevezették a digitális aláírást és az időpecsétet.

Az elektronikus kereskedelem külkereskedelemnek megfelelő részét, a pénzforgalomban a SWIFT (Society for Worldwide Interbank Financial Telecommunication) testesíti meg. A SWIFT több mint 2500 tag-bankkal rendelkezik a világ minden tájáról. A hálózaton a forgalom naponta meghaladja a több millió tranzakciót. Az egyes tranzakciók pénzmozgást reprezentálnak, így különösen fontos az elérhető legmagasabb fokú biztonság. A biztonságról ebben az esetben is kettős értelemben beszélhetünk. Egyre világosabb ugyanis, hogy az adatok, információk biztonságával egyenértékű ezek tulajdonosainak (legyen az akár magánszemély, akár szervezet vagy cég) személyiségjogi védelme az illetéktelen, jogosulatlan felhasználók ellen. Azonban az e-kommunikáció, a globális adatbázisok és hálózatok rohamos terjedésével, egyre problematikusabbá válik a jogosulatlan hozzáférés és felhasználás fogalmainak pontos definiálása. Itt már nem csupán jogi, hanem bonyolult társadalmi kérdésekkel kerülünk szembe, amelyek megoldása komoly szakmai kihívás az informatikai biztonság, a titkosítás szakemberei számára. Íme e kihívás egyik legfrissebb demonstrációja:

Az amerikai kormány több millió nemzetközi pénzátutalást figyelemmel követett a 2001. szeptember 11-i terrortámadások után - jelentette a The New York Times.
A jelentés szerint a Központi Hírszerző Ügynökség (CIA) irányította a megfigyelő akciót, a művelet legfelsőbb felügyelete a pénzügyminisztériumhoz tartozott. Egy szigorúan titkos program keretében a CIA hozzáférkőzött a világ legnagyobb, pénzáramlásokat nyilvántartó SWIFT társaságának adatbankjához. A SWIFT megerősítette, hogy együttműködött ebben a titkos programban az amerikai kormánnyal.
Bár a The New York Times szerint az amerikai kormány megpróbálta eltántorítani a lapot erre vonatkozó értesülésének közlésétől, mégis a cikk megjelenése után a kormány megerősítette, hogy a terrorizmus elleni harc jegyében csaknem öt éve *„információkat gyűjt”* a pénzátutalásokról. John Snow pénzügyminiszter úgy kommentálta a lapjelentést, hogy *„különösen büszke erre a programra, amellyel a terrorizmus finanszírozóit üldözték”*.

A terrorizmus elleni küzdelem zászlaja alatt óriási költségvetési pénzekhez jutnak a hatalmi szervek, ami különösen védtelenné teszi az állampolgári jogok védelmét. (lásd a NAGY TESTVÉR fejezetet!)

9.5. Adatbankok hitelessége és biztonsága

Az adatbankok biztonsági problémáinak megértéséhez célszerű meggondolni, hogy az adatbankok a papír alapú irodák irattárainak felelnek meg. Természetesen az elektronikusan tárolt adatok számos előnnyel rendelkeznek a hagyományos irattárakhoz képest. Például helyigényük nagyságrendekkel kisebb. A papír alapú irattárakban a visszakeresési lehetőség jóval lassúbb, mint a számítógépes adatbankokban. Az osztályozási lehetőségek, statisztikák készítése az elektronikusan tárolt adatok esetén nagy előnyt mutat a szokásos papír alapú nyilvántartásokból készített kimutatások, statisztikák elkészítési idejéhez képest. Nem szabad azonban, hogy ezek a kétségtelen előnyök elhomályosítsák az adatbankok megnövekedett biztonsági problémáit.
Vannak olyan feladatok, ahol az elektronikus adatbankoknak nagyrészt csak az előnyei mutatkoznak, ilyen például a könyvtári katalógusrendszer számítógépre vitele. Ennél a feladatnál, ha a tárolt katalógust egy hálózathoz csatlakoztatjuk, akkor még egy további előny is adódik, nevezetesen, hogy a hálózathoz tartozó más bel- és külföldi könyvtárak katalógusában is lehet olcsón, nagy sebességgel keresést végezni.

Az elektronikus adatbankok legnagyobb biztonsági problémája a *hitelesség biztosítása*. Ami ugyanis egy könyvtári katalógusnál elviselhető pontatlanság, az például egy földnyilvántartásnál már nem elfogadható. A földnyilvántartás számítógépes adatbankra való átállásakor, az Internethez hasonlóan, inkább az előnyöket vették figyelembe, így például a gyors visszakereshetőséget, a kis tárolóhely-szükségletet stb.
Azonban az előnyök mellett megjelent a *közhitelesség hiányának* problémája, amely az előnyökkel összemérhető, sőt, lehet azt mondani, hogy lényegesebb követelmény, mint az előnyöket nyújtó gyorsaság, a tárolóhely-igénycsökkenése stb.
Az alábbiakban egyrészt megmutatjuk, hogy nagy anyagi áldozatok árán hogyan lehet a már meglévő eszközökkel a biztonságot (közhitelességet) növelni, másrészt azonban azt is be kell látni, hogy a jelenleg meglévő eszközök nem minden esetben elégségesek a közhitelesség vagy a biztonság problémáinak megoldására.

A papír alapú irodában működő irattárnál alapvető követelmény, hogy az irattárba helyezésnek nagyon körülhatárolt szabályai vannak. Ezek a szabályok sokkal szigorúbbak, mint egy adatbank kezelésének szabályai. Különösen ki kell emelni, hogy az úgynevezett TÜK (Titkos Ügykezelés) alá eső irattárak a papír alapú iroda amúgy is szigorú irattárazási szabályait tovább szigorítják.

Az *irattárazásnak* a papír alapú irodában meggondolandó alaki követelményei az adatbankoknál sokszor nem teljesülnek. Nevezetesen egy iratot pontos keltezéssel kell ellátni, ahol igen fontos, hogy a keletkezés keltezése nem azonos az irattárba helyezés keltezésével, valamint minden egyes betekintésnél a betekintő személye és a betekintés időpontja is rögzítésre kerül. Ezen kívül az irattározott dokumentumokat alá kell írni a készítőnek, és rögzíteni kell az irattárba helyezés tényét is azáltal, hogy az irattározó személy az irat átvételét és irattárba helyezését aláírásával igazolja. Ezek után szabályozni kell a hozzáférést, nevezetesen, hogy ki férhet hozzá az iratokhoz, kinek van joga azokba betekinteni, az iratokon változtatni, esetleg azok megsemmisítését elrendelni.
Ez utóbbi műveletet kivéve a műszaki feltételek az adatbankok közhitelességének biztosításához is rendelkezésre állnak, a jogi feltételeket pedig egy korlátozott körre magánjogi szerződésekkel biztosítani lehet. Az elektronikus iroda biztonságát azonban veszélyezteti az a tény, hogy az ügyintéző személyi számítógépe hálózathoz kötött, és így a folyamatban lévő ügyek nem különülnek el az elintézett ügyektől. Vagyis a folyamatban lévő ügyek elintézés előtt irattárazásra kerülnek.

Egy iratnak az adatbankban való elhelyezése adatrögzítés útján történik, és nem feltétlenül szükséges, hogy az irat készítője és rögzítője azonos személy legyen, de mindkettőre célszerű lehet *digitális aláírást* használni, amely egyértelműen azonosítja a dokumentum tartalmát és a rögzítő, illetve a készítő személyét. Külön kellene rögzíteni a hozzáférők körét és az irattárban történő tárolás lejártának időpontját. Mindezt egy külön digitális aláírással hitelesítve, ez az aláíró lehet az irattáros, vagy lehet a dokumentum készítője. A hozzáférés biztonságát a jelenleg általánosan elterjedt többször használatos jelszavak helyett, amelyek minimális biztonságot adnak, az úgynevezett *egyszer használatos jelszó* jelentené.

Az elektronikus irodákban és az adatbankokban egyaránt nagyon nehezen megoldható biztonsági probléma, a *másolatok készítése*. A papír alapú irodánál a másolatok készítése számozott példányokkal történik, és világosan megkülönböztethető az eredeti példány a másolati példányoktól. Ennek megoldása az elektronikus irodában nem egyszerű feladat. Ha kategorikusan megtiltanák a másolat készítését, akkor bizonyos felhasználási területeknél a rendszer szinte használhatatlanná válna. A papír alapú irodánál követett eljárás, nevezetesen a számozott másolatok készítése azonban nem túl nehezen kijátszható. Gondoljunk arra, hogy az e-világban elektronikus dokumentumoknak számítanak a digitális zenék és videók, valamint egyéb CD- és DVD-adathordozók is. Ezek másolatainak készítésére ma már egész iparágak születtek! De ezzel egy időben a hamisításuk is iparággá vált, különös tekintettel a fejezet elején már említett, Internetről való jogosulatlan letöltésekre.
E probléma igazán biztonságos megoldását a dokumentumvédelem egészen új technikája jelentené, ez a digitális aláírás egy speciális továbbfejlesztése, a 8. fejezetben bemutatott *digitális ujjlenyomat* alkalmazása.

Az elektronikus irodák, illetve adatbankok esetén a *selejtezés* szintén igen nehezen megoldható biztonsági problémákat vet fel. Valószínűleg a jelenlegi tárolókapacitásoknál a selejtezést nem is kellene végrehajtani, mivel a keletkezett információmennyiség ezt az alkalmazások legtöbbjénél nem teszi szükségessé.
A selejtezésnek a papír alapú irodánál is három lépésben kell megtörténnie. Első lépés a selejtezésre szánt anyag jegyzőkönyvbe rögzítése és érvénytelenné tétele, ezután lehet csak a tényleges megsemmisítést egy zúzógéppel elvégezni az iratokat előállító intézményen belül, ezután a lezúzott iratokat egy külső céggel elégettetni, vagy szeméttelepre szállíttatni.
A papír alapú irodáknál tehát a biztonság csak a fenti előírások teljesítésének megfelelő ellenőrzését követeli meg, az elektronikus irodáknál azonban ez a probléma hatványozott nehézséget jelent. Ugyanis, míg a papír alapú irodákban az indigós papírok megsemmisítése általában az irat megsemmisítésével egy időben megtörténik, addig a számítógépes adatbázisokból leközölt (kinyomtatott) adatok mindig eredeti példánynak tűnnek.

Az adatkezelő rendszerek hierarchikus felépítése ugyanis nagy veszélyt jelent, mivel ez a legmagasabb szintre helyezi az úgynevezett rendszergazdát, aki elől a rendszerben semmit elrejteni nem lehet, ugyanis az operációs rendszer megfelelő ismerete esetén a rendszergazda bármilyen, az operációs rendszerben a felhasználó által elrejtett vagy jelszóval védett adathoz hozzá tud jutni. A hierarchikusan felépített operációs rendszerek a nem TÜK alapú hagyományos irodákban lévő biztonságot sem nyújtják, mivel a hierarchikus hozzáférés-védelem lényege az, hogy a titkossági fokozatok szigorúan egymás fölé vannak rendelve, így például a nyílt, a bizalmas, a titkos és a különösen titkos fokozatokat különböztetik meg. Ez az egymás alá rendelés azt jelenti, hogy például minden nyílt alá van rendelve a bizalmasnak, minden bizalmas alá van rendelve a titkosnak, és minden titkos a különösen titkosnak. Ez a hagyományos és az adatbázis-kezelő programok legtöbbjében meglévő elv azonban könnyen láthatóan nem nyújt megfelelő biztonságot, ugyanis az információhoz való hozzáférhetőséget

a beosztással köti szorosan össze. Ez azt jelenti, hogy sok felhasználó hozzáféréssel rendelkezik olyan adatokhoz, amelyek a munkájával nincsenek kapcsolatban.

Számos olyan adatkezelő rendszer került kiépítésre, amelyek a hierarchikus felépítés helyett az adatbankok megfelelő biztonságát igyekeztek úgy biztosítani, hogy a szerverek egy hitelesítő-kulcselosztó szerepet is játszottak. Ilyen például a Bell-LaPadula-modell, a Biba-modell, a Clark-Wilson-modell, továbbá a Kínaifal-modell. Ez utóbbi - innen kapta az elnevezését - biztosítja azt, hogy például egy banknál az egymással konkurens vállalatok számláját nem kezelheti azonos ügyintéző.
Általában a Kínaifal-modell arra vonatkozik, hogy egymással érdekellentétben lévő felhasználók adatait egymástól el kell választani, tehát az adathozzáférést olyan modell szerint kell irányítani, amely nem teszi lehetővé, hogy ellenérdekű felek adataihoz bárki is hozzájusson. Az ilyenfajta elkülönítés a TÜK-irodákban tárolt adatok számítógépes nyilvántartásában hasznos modell. Annak érdekében, hogy a papír alapú TÜK-irodában az irattáros ne lássa át az összes nála elhelyezett iratot, a legmagasabb titokfokozatban lévő iratokat egy-egy külön-külön zárható dossziéban helyezik el, amelyek kinyitására a titokgazda vagy a titokgazda által felhatalmazott személy jogosult, munkája végeztével pedig ezeket a dobozokat le kell zárni, és úgy kerülnek be az irattárba. Ezáltal lehetőség van arra, hogy az irattáros, aki tárolja az iratokat, azok tartalmát ne ismerje. Ennek megvalósítása az elektronikus irodában nem egyszerű. Egy lehetséges megoldási mód az, hogy a közös tárolóban tárolt információk rejtjelzett formában kerülnek tárolásra, és a rejtjelzéshez használt kulcsok nincsenek a gépben tárolva, hanem például személyhez kötött memóriakártyával történik a kulcsok felhasználása.

9.6. A mágnes-, illetve memóriakártyák biztonsága

A *mágneskártya* vagy ügyfélkártya a papír alapú személyazonosító igazolványok korszerűbb változata volt. A mágneskártya csak a személyi adatok rögzítésére alkalmas, a tárolás egy mágnescsíkon történik. A jelenleg is forgalomban lévő mágneskártyák a biztonság igen alacsony fokát nyújtják, mert lehetővé teszik a kártya tartalmának egy leolvasó segítségével való megismerését és lemásolását, miközben a kártya semmiféle intelligenciával nem rendelkezik.
Ezeket a gyengeségeket látva *Roland C. Moreno* mérnök, újságíró 1970-ben javasolta a szokásos mágneskártyák helyett a memóriakártyák használatát. A *memóriakártya*, angol nevén *smart card*, magyarul okos vagy intelligens kártyának is fordítható, ötletét Moreno szabadalmaztatta. Kidolgozta a felhasználás biztonságát és szabályait. A projekt végrehajtására egy céget hozott létre, ezt elnevezte *Innovatronnak*. Az utódszervezetként alakult *Honeywell Bull* cég licencjogot nyert a memóriakártyák és az ezt leolvasó kártyaolvasó szerkezetek gyártására.
A memóriakártyák gyakorlati megvalósítása az integrált áramkörök létrejöttével vált lehetségessé, ugyanis a memóriakártyákban VLSI (Very Large Scale Integration), azaz „igen nagy mértékben integrált áramköröket (chip) alkalmaztak. Ezeknek az áramköröknek a fizikailag rendkívül sűrített logikai szolgáltatásai tették a memóriakártyákat szó szerint kulcs-jelentőségűvé (egy chip több tízezer tranzisztor funkcióit integrálja néhány négyzetmilliméteren).
A memóriakártyák feldolgozási kapacitását biztosító központi egységen kívül a kártyákon elhelyezett RAM-ok és az operációs rendszert magukban foglaló ROM-ok teszik az egész rendszert megfelelő komplexitásúvá. A mágneskártyával ellentétben egy ilyen chip-kártya

valódi biztonságát teszi lehetővé, hogy a kártyán tulajdonképpen egy általános rendeltetésű mikroszámítógép működik, illetve egy általános rendeltetésű mikroszámítógép úgynevezett biztonsági változata, ami azt jelenti, hogy a gyártási folyamat lezárta után a belső adatforgalom a mikroszámítógép be- és kimeneti pontjainak lezárása folytán a továbbiakban ezeken keresztül nem befolyásolható.

A memóriakártyák a következő alapvető műveleteket képesek elvégezni:

1. adatbevitel,
2. adatkibocsátás, adatok kiolvasása a tárolóból,
3. adatok beírása vagy törlése a tárolóban,
4. rejtjelzési műveletek elvégzése.

A felsorolt funkciók mindegyike nagyon fontos, de a második és negyedik különösen érzékeny, mivel a második funkció segítségével adatok és eredmények kerülnek a külvilágba, a négyes funkció pedig a tároló tartalmának módosítását eredményezi. Fontos megjegyezni, hogy a rejtjelzési titkos kulcsok a mikroszámítógép által kerülnek használatra, de nem képezhetnek kimenetet. Néhány, memóriában lévő adat felhatalmazást adhat bizonyos területek eléréséhez, ezért különös elővigyázatot igényel, mielőtt ezeket beírjuk vagy töröljük. A rejtjelzési számítások eredménye lehet olyan ellenőrző szó, amely a külvilágnak szól, ezért igényel különös figyelmet, mielőtt a kimeneten megjelenítik.
A kártya biztonsága csak akkor garantálható, hogyha a kártyát csak a valódi tulajdonos használhatja, illetve ennek megfelelően a kártya kívülről kap utasítást arra, hogy a kártya valódi tulajdonosa használja a kártyát. A kártyahasználatnak ez a lényeges része a többször használatos jelszavak (PIN kódok=*Personal Identification Number*) felhasználásától a hitelességvizsgáló kódokig (MAC=*Message Authentification Code*) terjedhet, és magában foglalhatja a magas szintű digitális aláírást és hitelesítő megoldásokat. Ezek a mechanizmusok *rejtjelzési módszereken alapulnak*. A kártya reagálhat arra, hogy bizonyos típusú csalási törekvéseket észlel, például ha a PIN-kóddal három alkalommal sikertelenül próbálkoznak, akkor a beprogramozott eljárás a kártya a további működést leállíthatja.
Már megjelent például a bankoknál a kártyatulajdonos bizonyos egyedi fiziológiai tulajdonságaival való azonosítás. Ilyen például az ATN-ek fölött lévő, retina-letapogató berendezés, amely összehasonlítja a kártyában eltárolt, kizárólag a kártya jogos tulajdonosának retinájára jellemző fiziológiai jegyeket az automata előtt álló személy retinájával, így biztosítva azt, hogy a kártyát csak a jogos tulajdonos tudja fölhasználni.

A memóriakártyákat két csoportba lehet osztani. Az egyik csoportba tartoznak az autonóm (offline) leolvasóval működő kártyák, a másik csoportba pedig azok, amelyek működéséhez egy központból megerősítő üzenet (dinamikus jelszó) szükséges.
Gazdasági szempontból az online rendszerek jóval drágábbak, mint az offline rendszerek, így a két megoldás közötti választást elsősorban biztonsági paraméterek befolyásolják. Könnyen belátható, hogy a biztonsági szempontok az online megoldást indokolják, mivel például kártyalopás esetén a kártya érvénytelenítése így azonnal megoldható, míg az offline esetben a letiltás sokkal bonyolultabb és időigényesebb.
Próbálkozások történnek arra, hogy az offline rendszerek eme gyengéjét a felhasználóra hárítsák azzal, hogy a bejelentett ellopások időpontjától kezdve bizonyos ideig a kártyakibocsátó a visszaélésekért nem vállal felelősséget. Az ilyen jogi megoldás azonban nem tartható, és feltétlenül a felhasználó kárát, biztonságának kockáztatását eredményezi. Az online megoldás esetén, sajnos, a többször használatos jelszóval (PIN kóddal) védett rendszerek nagyon sebezhetők, ahogy azt az Internettel kapcsolatban már említettük, mivel az

adatátviteli vonalon áthaladó információk lehallgatás elleni védelme nagyon nehezen vagy egyáltalán nem kiküszöbölhető.
A többször használható jelszónál bonyolultabb és biztonságosabb algoritmusok, mint például a dinamikus jelszó (egyszeri felhasználású jelszó), illetve a digitális aláírás alkalmazása azért is célszerű, mivel a jelenleg működő pénzkiadó automaták úgy működnek, mint egy olyan pénztár, amelyben az ügyfél a pénz átvételét nem kell, hogy elismerje, vagyis a pénzátvétel letagadható. A pénzügyi alkalmazások területén háromfajta kártyát alkalmaznak:

Debit kártya: pénz befizetését teszi lehetővé a bankba a bank nyitvatartási idején kívül is, és nem csak, vagy nem elsősorban készpénzben, hanem a kártyáról, annak egyenlegének megváltoztatása által.
Hitel- vagy kreditkártya: a pénz kivételét és esetleg más tranzakciókat, például más számláról átutalást tesz lehetővé, ugyancsak függetlenül a bank nyitvatartási idejétől.
Terhelési kártya (charge card): Ennek lényege, hogy segítségével bizonyos szolgáltatások, például telefonszolgáltatás, parkolás stb. fizetését lehet eszközölni, egy előre megállapított összeghatárig. Ilyen rendszer működik például az Egyesült Államokban a telefonoknál, ahol a kártya tulajdonosa a kártya felhasználásával biztosítja azt, hogy a bankjában vezetett folyószámláról a telefontársaság a beszélgetés végeztével vagy aközben folyamatosan a beszélgetés díját le tudja emelni. Az ilyen rendszer a biztonság szempontjából igen hatásosan működik.

Az eddigiek is rávilágítanak arra, hogy a memóriakártyák használatánál a nagyobb biztonság érdekében több problémát kell a jelenlegihez képest alapvetően másképpen megoldani. Ezek a problémák: *a felhasználó személyének azonosítása, a kártya könnyű letilthatósága, valamint az interaktív kapcsolat*.
Ez utóbbi megoldatlansága annál is érdekesebb, mivel a régebbi idők manuális távirat feladásának is olyan rendszere volt, hogy a kezelőnél bejelentett távirat-feladást csak akkor teljesítették, ha előzőleg a kezelő az állomást visszahívta, és így biztosítva volt, hogy milyen hívószámra kell számlázni. Ez a biztonságos rendszer a jól szervezett *dial in* szolgáltatásnál is működik.
A memóriakártyák a jelenlegi technológia mellett már olyan tárolókapacitással rendelkeznek (és ez a jövőben növekedni fog), amelyek egy egész adatbázis tárolását teszik lehetővé. Például a kártyabirtokos személyére vonatkozó egészségügyi, illetve más személyi természetű adatok tárolását. Ugyanez a tárolókapacitás-növekedés teszi alkalmassá a memóriakártyát a többcélú alkalmazásra is. Mindezek a tulajdonságok magyarázzák a memóriakártyák számítógépes hálózatokhoz való kapcsolását.

9.7. A memóriakártya a biztonságos hozzáférés-védelem eszköze

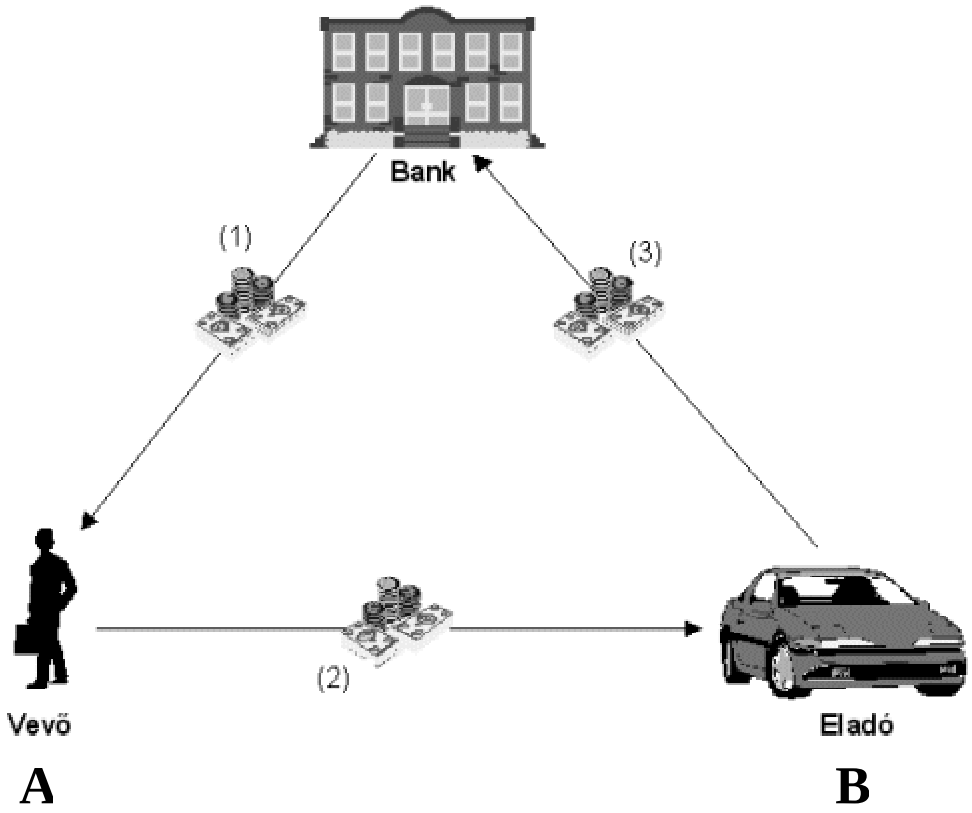
Napjaink számítógépes rendszerei általában hálózatba kapcsolt gépekből és az ezeken tárolt adatbázisokból állnak. Az adatbázisokhoz való hozzáférés ugyancsak hatásosan és biztonságosan működhet a memóriakártyák segítségével, annak ellenére, hogy jelenleg főleg gazdasági okok miatt, a biztonságot elhanyagolva, az adatbázisokhoz való hozzáférés általában többször használatos jelszavakkal történik.

A memóriakártyák rohamosan növekvő alkalmazásaiból, az előzőkben bemutatottakon túl, néhány további felsorolásával szeretném érzékeltetni a lehetőségek sokszínűségét.

Az autóparkolásnál felhasználható kártyák ma már sok esetben az érintkezés nélkül működő leolvasókkal működnek, ahol a kártya a vezető zsebében van, és az érintkezés nélküli érzékelő (leolvasó) egyrészt az automata sorompót fölnyitva beengedi a parkolóba a gépkocsit, másrészt a kijáratnál ugyanilyen módon érzékeli a vezető zsebében lévő kártyát és az ezen tárolt egyenlegből a parkolás díját levonja. Hasonló fölhasználási lehetőségek az autópálya-matricákat helyettesítő, illetve a tömegközlekedési jegyek helyett használt chip-kártyák.
Utazási irodák a díjak befizetése ellenében a szolgáltatásokra vonatkozó fizetéseket egy memóriakártyában rögzítik, így az utasnak a szállodában, az autókölcsönzésnél, a pénzváltásnál, a vámkifizetéseknél, valamint egyéb, előre kifizetett személyi szolgáltatásoknál nemhogy készpénzzel nem kell foglalkoznia, hanem az egy kártyán belül rögzített összegekből a különböző célokra történő kifizetéseket hitelkártya nélkül is tudja teljesíteni. Ennek a kényelem mellett a biztonság szempontjából is jelentősége van, ugyanis a hitelkártyák felhasználása során elkövetett csalások (másolás, nem megfelelő összegek levonása az egyenlegből, készpénz-fizetés jogtalan igénybevétele stb.) nem történhet meg.
A kereskedelmi alkalmazások vonatkozásában meg kell említeni az árukra rögzített chip-kártyákat, amelyek olyan jeladóval vannak ellátva, amely az üzlet elhagyásakor az ajtónál lévő érzékelő segítségével jelzi, amennyiben a vevő fizetés nélkül távozna, és így a kártya az árun marad.
A felügyelet nélküli kereskedelmi társas viszony esetén az, hogy például ki mennyi pénzt vitt be vagy adott ki egy közös kasszából, jól és biztonságosan követhető chip-kártya segítségével. A memóriakártya egy közös árukészletből áruló több tulajdonostárs vagy alkalmazott egymás közötti elszámolásának eszköze is lehet. Például újságárusoknál, ahol több eladó, vagy autó karbantartásnál, ahol több szerelő dolgozik stb.
A napjainkban többé-kevésbé elterjedt alkalmazások közel sem teljes bemutatása mellett fel kell hívni a figyelmet a memóriakártyák pénzügyi alkalmazásai területén egy jelenleg még egyáltalán nem elterjedt, de nagy perspektívával rendelkező alkalmazási területre, amely alapvetően kötődik a hálózatokhoz. Ez az úgynevezett *digitális pénz*, vagy más néven *digitális pénztárca* lehetősége. A digitális pénz egyúttal tökéletesen modellezi a memóriakártyák lehetőségeit a biztonságos hálózatok kialakításánál.

9.8. A digitális pénz

Praktikus okokból érthető, hogy a gazdaság szereplői számos okból igyekeznek elkerülni a készpénzforgalmat. Ugyanakkor biztosítani szeretnék a készpénznek azt a személyiségjogi szempontból előnyös tulajdonságát, hogy a készpénz útja követhetetlen. Sajnos éppen ez a tulajdonság ad módot a bűnös felhasználásra is. Például amikor a pénzt *megvesztegetés* céljára használják fel, a bankjegyekből egyáltalán nem lehet visszakövetkeztetni az átadó személyazonosságára, valamint azt sem lehet bizonyítani, hogy az átadott készpénz milyen céllal került átadásra (jól előkészített akció esetén a bankjegyek rendőrség által vegytintával való megjelölése vagy a bankjegyek sorszámának feljegyzése jelent némi megoldást). Ennek megfelelően nemcsak kényelmi okokból, hanem a bűnös tevékenység meghiúsítása érdekében is célszerű olyan digitális megoldást keresni, amely a készpénzt helyettesíti. Ezt a célt szolgálja a *digitális pénztárca*, amely egy olyan elektronikus tároló, amelyben a *digitális pénzt* elhelyezik. Célszerű módon ez a digitális pénztárca lehet egy memóriakártya.



9.2. ábra

Tegyük fel, hogy egy banknál az „A” felhasználónak van egy bankszámlája, és ennek terhére kívánja digitális pénztárcáját feltölteni. Ekkor a következőképpen jár el:

Meghatározza, hogy milyen pénzegységekre van szüksége, például ezerforintos, tízezres stb. Minden pénzegységhez, amelyet majd digitálisan akar tárolni, egy véletlen számot generál a memóriakártyájába beépített véletlenszám-generátor segítségével. A generált véletlen szám hosszának, vagyis a számjegyeinek vagy bitjei számának olyannak kell lennie, hogy két azonos véletlen szám előfordulásának valószínűsége a nullához közelítsen. A banki tranzakció személyesen vagy a homebanking-rendszeren keresztül történik úgy (a folyamatot a 9.2. ábra szemlélteti), hogy a pénzegységek értékeit és a hozzájuk tartozó véletlen számokat az „A” felhasználó beküldi, majd a bank részére a bank digitális aláírása segítségével ezeket külön-külön, tehát a címletet és a hozzá tartozó véletlen számot digitálisan aláírja. Ezután visszatáplálja személyesen a bankfiókban, vagy adatátviteli vonalon a home banking rendszeren keresztül az „A” felhasználó digitális pénztárcájába. Az „A” felhasználó, miután valamilyen szolgáltatást, vagy árucikket meg akar vásárolni, az elektronikus pénztárcájából a „B” felhasználó elektronikus pénztárcájába a megfelelő összeget átutalja, vagyis a bank által aláírt címleteket átadja személyesen, tehát offline módon, vagy pedig átviteli csatornán keresztül. Az „A” bankszámláját kezelő bank természetesen „A” adatait ismeri, és a kiadott digitális pénz megfelelő értékét számlájáról levonja. Ugyanakkor az adatokat, tehát az egyes címletekhez tartozó véletlenszámot, a címlet értékét és az elektronikus aláírást egy megfelelő adatbankban tárolja. Miután „A” és „B” között a kifizetés megtörtént, amihez „B-nek „A”-ról semmiféle információjának nem kell lennie, a „B” a megfelelő bankba bejuttatja a digitális pénzt. A bank a nyilvántartásában ellenőrzi, hogy a megfelelő véletlenszám értékű (sorszámmal rendelkező) bankjegyet nem váltotta-e már egyszer be valaki. Amennyiben nem, akkor a kifizetésnek a „B” részére a készpénzt bankon keresztül átadja, vagy pedig a „B” rendelkezése szerint valamiféle más bankba való átutalást végrehajtja. Amennyiben a

nyilvántartásból kiderül, hogy „A” ezt a digitális pénzt már valakinek odaadta, és az már a banknál beváltotta, mivel a bank ismeri „A” összes adatait, tehát egyrészt visszautasítja a beváltást, másrészt fölfedi ezeket az adatokat, hogy a bűnüldöző szervek „A” ellen fel tudjanak lépni.

Azaz mindaddig, amíg „A” törvényt tisztelően viselkedik, addig a személyi adatai titokban maradnak, ugyanakkor, ha valamiféle visszaélést követ el, akkor ennek a visszaélésnek a következményeit nem tudja elkerülni, mivel a bankban nyilvántartott adatok alapján ellene eljárást lehet lefolytatni.

A memóriakártyák technológiája állandó fejlődésben van, így napról napra új felhasználási területek nyílnak meg. Az újítások nemcsak a kártyatechnológiában és felhasználási területein mutatkoznak meg, hanem a kártyát a központtal összekötő híradástechnika is változik, így például az űrtávközlés segítségével a földrajzilag nagyon távoli terminálok a költséges földkábelek, illetve tenger alatti kábelek lefektetése nélkül köthetők össze. Az űrtávközlés, ahol a távközlési műholdak előállítása és fölbocsátása óriási összegeket emészt fel, mára már abba az állapotba jutottak, hogy eme gigantikus beruházások ellenére a felhasználás költségei versenyképessé válnak a hagyományos híradástechnikai összeköttetések költségeivel szemben.

9.9. A hozzáférés-védelem új módszerei

Dinamikus jelszó

A *dinamikus jelszó* nemcsak formálisan, hanem alapvető konstrukciójában tér el a közismert egyszerű (statikus) jelszótól. Ebben az esetben ugyanis nem maga a jelszó a kulcs, hanem az egyes felhasználókhoz rendelt matematikai képletek. A hozzáférés-védelem abból áll, hogy a felhasználó megad egy egyszerű jelszót, amelynek hatására a központi szerver egy véletlen számot küld a felhasználónak, és egyben ezt a véletlen számot a központban tárolt (felhasználóhoz tartozó) képletbe helyettesíti. Ugyanakkor a felhasználó a birtokában lévő képletbe behelyettesíti a véletlen értéket, majd az így kiszámított eredményt visszaküldi a központnak. A központ összehasonlítja a visszakapott értéket az általa kiszámítottal, és annak megfelelően, hogy a két érték azonos-e vagy sem, dönt a hozzáférés engedélyezéséről. Ez pontosan a 7.3. fejezetben bemutatott zero-knowledge protocol megvalósítása.
Könnyen látható, hogy ebben a konstrukcióban a kommunikációs vonalat figyelő lehallgató csak olyan információhoz (a véletlen számhoz vagy a képletből kiszámított értékhez) tud hozzájutni, amely semmiféle információt nem ad egy következő illegális hozzáféréshez, hiszen ezekből az értékekből a képlet nem megfejthető. Különösen, ha figyelembe vesszük, hogy minden tranzakcióhoz új véletlen szám tartozik, amely egyetlen előzővel sem egyezik meg.
Amíg tehát az egyszerű jelszó illetéktelen megszerzésével hozzáférhetővé válik a védett információ, addig a dinamikus jelszó esetén ezzel csak az interaktív azonosítás első lépéséig képes eljutni, majd a titkos képlet hiányában a rendszer letiltja a hozzáférést.

Titokmegosztás

A hozzáférés-védelemben nagy szerepet kap az úgynevezett *titokmegosztás*. E módszer ősi változatai a bankok klasszikus gyakorlatából már jól ismertek. Például a széf egy-egy kulcsa különböző személyeknél van, az egyik a széf bérlőjénél, a másik a bank alkalmazottjánál, így a széf kinyitásához a két kulcs együttes alkalmazása szükséges. Nyilván ez egy mechanikus megoldás, ennek elektronikus változata számos továbbfejlesztést tartalmaz, például nem két,

hanem tetszőleges számú felhasználó együttes akarata szükséges a titokhoz való hozzáféréshez, másrészt a felhasználók lehetnek különböző hozzáférési súlyúak, tehát például a bankigazgató a nyitás szempontjából nagyobb súllyal rendelkezhet, mint az ügyfél vagy egy beosztott banktisztviselő.

A titokmegosztásnak eme digitális változata már nem azonos a titoknak (amelyet általánosan tekinthetünk egy bináris jelsorozatnak) egyszerű darabokra bontásával. Itt a titok darabokra osztásához, és a feldarabolt titok összerakásához speciális matematikai eljárásokra van szükség.

A titokmegosztás talán legmagasabb szintű alkalmazásaként említhető, hogy például az interkontinentális rakéták indító rendszerei úgy vannak kiképezve, hogy azok indításához több döntéshozó együttes akarata szükséges. Vagy például titkos katonai objektumok (például számítógéptermek) elektronikus beléptető rendszerei úgy működnek, hogy egyszerre csak egynél több kezelő tud belépni vagy kilépni e helyiségből.

Állampolgári jogok, titok és információbiztonság

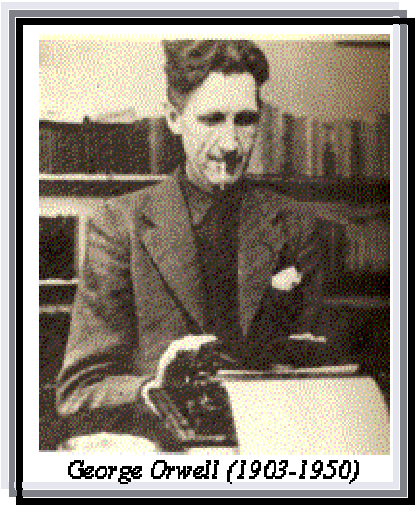
Az információ biztonsággal kapcsolatos nézetkülönbségek a távközlés kezdetei óta éleződnek. Szeretném ráirányítani a figyelmet arra az alapvető paradigmaváltásra, amely a globális e-kommunikációval, a gép-ember hálózatokkal, a mesterséges és természetes intelligencia viszonylatában bekövetkezett, és amely az információ tartalmáról annak virtuális vagy valóságos voltára, így az információ-biztonságra tereli a figyelmet. Az internet, mint a globális kommunikáció és információ-hozzáférés megtestesítője, még bonyolultabbá tette a biztonság megítélését.
D.E. Denning, a Georgetown Egyetem számítástudomány professzora így vélekedik: *„Egy olyan világban, amelyet a nemzetközi szervezett bűnözés, a terrorizmus és a vörös színezetű kormányok fenyegetnek , butaság lenne megengedni, hogy az információs szupersztrádán keringő információk mentesek legyenek a törvényes keretek között végzett lehallgatástól.”* ([HOFFMAN 1995], 268.o.)

Az elmúlt néhány évben hazánkban is számos vita zajlott a szabadság és személyiségjogok korlátozhatóságáról és annak mértékéről. Jelen szerző több dolgozatában és könyveiben is igyekezett felhívni a figyelmet a titok relativitásának egyre növekvő problematikájára, amely az információbiztonság mentén ellentétes oldalra kényszeríti a hatalmat és az egyébként „alkotmányos jogokkal” rendelkező információ-tulajdonosokat. A globalizálódó bűnözés, korrupció és terrorizmus rémképe a címer azon a zászlón, amely alá fel kéne sorakozni annak a 99%-nyi törvénytisztelő állampolgárnak, akik e rémet szeretnék megsemmisíteni, így alkotva egységfrontot a hatalommal, a közös ellenség legyőzése érdekében. A hatalom eme zászló lengetésével igyekszik elfogadhatóvá tenni mindannyiunk számára, hogy ő a mi információink legbiztosabb őre, amiből következik, hogy elégséges a titok egyirányú értelmezése. Ez már érthetőbbé teszi a fentiekben jelzett dinamikus titkosító eljárások tömeges bevezetésének nehézkességét, amelyek minimálisra csökkentve az emberi tényező szerepét (korrupció, zsarolhatóság stb.), egyenrangú biztonságot ad az információ tulajdonosának, valamint az információt tároló és továbbító szolgáltatónak.

10. A NAGY TESTVÉR valósággá válik, avagy *nyílt globalizáció ellen rejtett háború*

„Milyen siralmas látni, hogy a tudományokat alig lehet megkülönböztetni a fegyverektől."
(Coménius 1592-1670)

10.1. George Orwell irodalmi utópiája: 1984


George Orwell (1903-1950)

A NAGY TESTVÉR a 20. és ímmár a 21. század közgondolkodásának azon ritka fogalmai közé tartozik, amelynek pontos keletkezése meghatározható.
George Orwell 1949-ben megjelent *Ezerkilencszáznyolcvannégy* című regényének első oldalán csupa nagybetűvel született meg ez a fogalommá vált alak, amint azt a fenti mottó idézi. A NAGY TESTVÉR megszületésének pillanata és helye tehát pontosan meghatározható, mégis a mai napig a titok fátyola lengi körül a címválasztást. Mivel magából a regényből nem egyértelmű az *1984*-es szám eredete, több számmisztikaszerű hipotézist állítottak fel ennek magyarázatára. Egyik magyarázat szerint az író a megírás évszámának (1948) utolsó két számjegyét felcserélte. Egy másik nézet szerint ezzel akart utalni a *Fabian Society*[66] nevű brit szocialista szervezet 1884-es alapításának századik évfordulójára. Más nézetek szerint az irodalomból ered a magyarázat alapja. Lehet például Jack London *A vaspata* című regénye, amelyben egy politikai mozgalom 1984-ben éri el tevékenységének csúcspontját. Vagy akár utalhat az 1984-es szám Orwell feleségének (Eileen O'Shaughnessy) egyik versére, amelynek címe: *End of the Century, 1984* (Az évszázad vége, 1984).

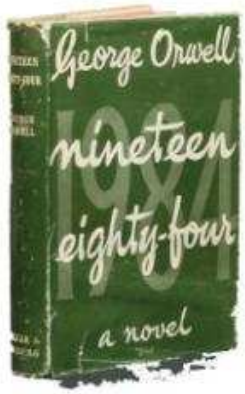
Mindezen érdekes találgatások ellenére, a legvalószínűbb és tényeken alapuló válasz az, hogy Orwell eredetileg a *The Last Man in Europe* (Az Utolsó Ember Európában) címet adta regényének. Azonban az első kiadás kiadója Frederic Warburg, a nagyobb siker reményében ezt a változtatást javasolta, amit a szerző nem ellenzett.

Valószínűleg nem csak a cím megválasztása lehetett a NAGY TESTVÉR születésének nehéz fázisa, hiszen a fennmaradt kéziratban, már az első oldal sokszoros kihúzásai és

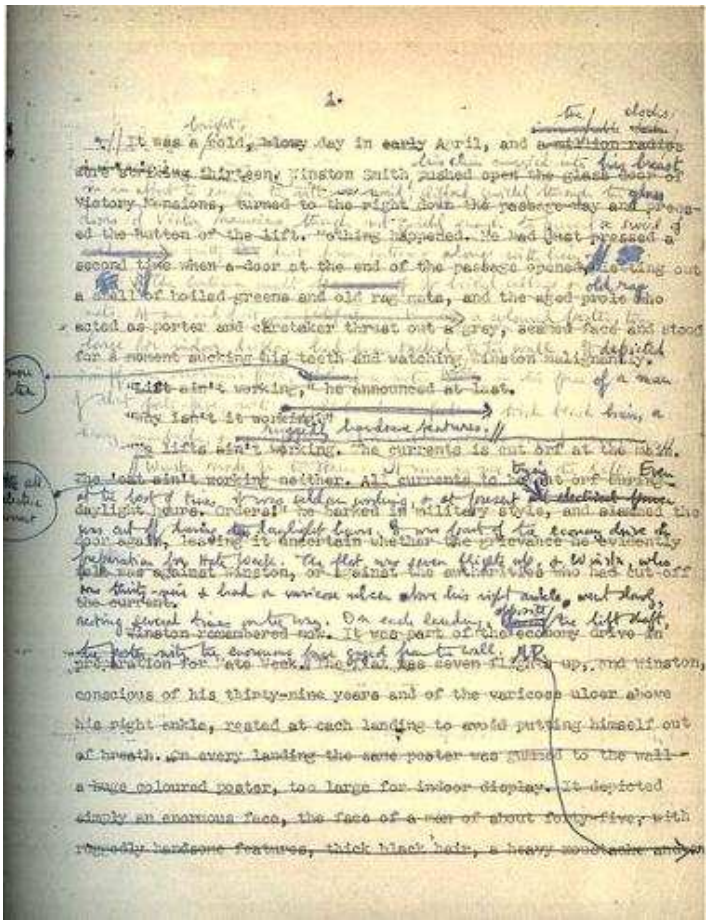
[66] A **Fabian Society** vagy Fábiánus Társaság (nevét a római politikus és katona Quintus **Fabius** Maximusról kapta) A társaságot 1884. január 4-én alapították Londonban. Céljuk a társadalom példamutatással történő átalakítása volt. A társaság megalapítását követően hamarosan olyan híres személyek csatlakoztak, mint George Bernard Shaw, H.G.Wells, vagy Bertrand Russell.

szövegmódosításai mutatják azt a vajúdást, amellyel ez az újszülött kibújt a zseniális gondolat burkából.

Nem csodálható a kézirat oldalain követhető gyötrő vajúdás, hiszen Orwell ráeszmélt arra, hogy a 20. század első felének társadalmi történései a klasszikus fogalmakkal egyáltalán nem leírhatók. Felfedezte, hogy az eltorzulóban lévő jövőt csak úgy lehet lefesteni, ha torzító tükröt tart a múlt elé és megalkotta a *newspeak*, azaz *újbeszél* nyelvet, amely a szópusztítás, azaz a degenerálódó kultúra és társadalom (ezt is alátámasztja az eredeti cím választás), illetve a degenerálódó gondolkodás fogalmi rendszere. Ezzel teremtette meg a NAGY TESTVÉR mindenlátó, mára már fogalommá vált alakjának környezetét, a 101-es szobát, a Gondolatrendőrséget, a teleképet.



G.Orwell: Nineteen eighty-four első kiadása a Secker & Warburg kiadónál



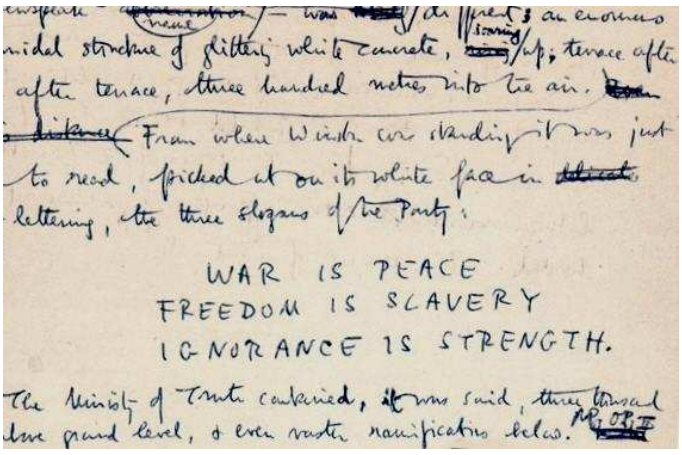
G.Orwell: Nineteen eighty-four kéziratának első oldala

10.2. *Newspeak* azaz *Újbeszél* nyelv

Az újbeszél nyelv regénybeli funkciója az, hogy ne lehessen megérteni az irányadótól eltérő véleményeket, hogy eltávolítsa azokat a szavakat (gondolatokat), amelyek a nézetkülönbségek kifejezésére használhatók lennének. Így a Gondolatrendőrségnek nem is kell kifejleszteni olyan módszert amellyel megtalálja a véleményeltéréseket az emberek gondolataiban, hiszen újbeszélül ilyenek létre sem jöhetnek. Az újbeszél tehát egyre több szót, kifejezést, azaz ezekre épülő gondolatot, fogalmat takarít meg a szótárakból, vagyis a szópusztítás és ezáltal a gondolatirtás nyelve.
„Persze az igék és a melléknevek közt végezzük a legnagyobb irtást, de a főnevek százait is teljes joggal kiirthatjuk. S nemcsak a rokon értelműeket, hanem az ellentétes értelműeket is. Mert ugyan miféle létjogosultsága van egy olyan szónak, amelyik pusztán csak egy másik szónak az ellentéte? Vegyük például a **jó** *szót. Ha egyszer van egy olyan szavunk, mint a* **jó***, ugyan mi szükség olyan szóra is, hogy* **rossz***? A* **nemjó** *éppen olyan megfelelő… Ha pedig a* **jó** *nyomatékosabb kifejezésére van szükség, mi értelme annak, hogy egész csomó olyan, teljesen haszontalan szót használjunk, mint például a* **kitűnő***, a* **ragyogó** *meg a többi hasonló? Ezeknek a jelentését tökéletesen fedi a* **pluszjó***, vagy a* **duplapluszjó***, ha még fokozottabb értelmére van szükségünk. … A végén a jóság és a rosszaság egész fogalomkörét ki fogja fejezni hat szó – azazhogy igazában egyetlenegy szó."* ([ORWELL 1989]60.old.)

Az *újbeszél* alapötlete tehát az, hogy eltávolítsa a nyelv minden jelentésárnyalatát, a kettősségek meghagyásával. Erre talán legszemléletesebb példa a regénybeli **kacsabeszél** (angolul ***duckspeak***) *újbeszél* kifejezés, melynek jelentése: *„kacsa módra hápogni"*. Ahogy a regény egyik szereplője, Syme mondja: *„Ha ellenfélre mondjuk, gyalázás; ha valaki olyanra, akivel egy nézeten vagyunk, dicséret."* ([ORWELL 1989] 63.old.)

Így érthető meg az 1984 különös komplementer gondolkodásmódja, mely szerint *„A Béke-minisztérium háborúval foglalkozik, az Igazság-minisztérium hazugságokkal, a Szeretet-minisztérium kínzással, s a Bőség-minisztérium éheztetéssel."* ([ORWELL 1989] 239.old.)
Így meglepő, ám mégis logikus az 1984-beli párt elhíresült három jelmondata ([ORWELL 1989] 10.old.):



„A HÁBORÚ: BÉKE
A SZABADSÁG: SZOLGASÁG

A TUDATLANSÁG: ERŐ"

Az 1984-beli párt három jelmondata Orwell eredeti kéziratában

Az *újbeszél* mögötti elképzelés szerint, ha valamit nem lehet kimondani, akkor azt gondolni is lehetetlen. Ez felveti azt a kérdést, hogy például el tudjuk-e mondani a szabadság utáni szükséget, tudunk-e felkelést szítani, vagy éppen az aktuális rend ellen mozgósítani, ha egyikre sincs szavunk? Vajon a gondolkodásunk nincs-e a kulturális öröklődéssel kapott beszédnyelv ketrecébe zárva, ahogy a genetikai úton örökölt adottságaink nagyrészt meghatározzák a társadalmi lehetőségeinket?

A gondolkodás beszédnyelvi determinációját persze megingatják azok a magas kreativitást mutató alkotó tevékenységek, amelyek nem a nyelvi kifejezésre épülnek, mint például a képzőművészet, vagy a zene. De még mielőtt az elit szemlélet vádja érne, gondoljunk csak a mindenki által tudatosan, vagy éppen ösztönösen alkalmazott metakommunikációra (mimika, gesztus, testtartás, stb.)! A titkosítás tudománya régóta felfedezte, hogy a titkok hordozója az a plussz (szaknyelven: redundancia), amit a mai gazdaság és technikacentrikus gondolkodás kiküszöbölendő feleslegnek tart.

Bár a nyelvészek vitatkoznak a gondolkodás és a nyelv prioritásán, az emberi kommunikáció, vagyis egymás megértésének alapja biztosan a közös fogalombázis. Csak így válik lehetővé, hogy a különböző nyelvek szavai, mondatai egymásra lefordíthatók legyenek.

Mindezek után a regényből kibontakozik Orwell utókornak szánt mély (*újbeszél*) üzenete, amely valahogy így foglalható össze: *a világ az állandó háború állapotában van, senki sem szabad, mindenki tudatlan.*

10.3. *Újbeszél* az e-kommunikációban

Orwell írt az 1984-hez egy függeléket, amelyben részletesen kifejti az újbeszél *szókincs minimalizáló alapelveit. Ennek lényege, hogy a nyelv szókészletét A, B, C szókincsekre osztja.*
„Az A szókincs a mindennapi élet dolgainak megnevezéséhez szükséges szavakból áll … Majdnem teljesen azokból a szavakból állították össze, amelyeket most is használunk – mint például: üt, fut, kutya, fa, cukor, ház, rét -, de napjaink szókészletével összehasonlítva e szavak száma rendkívül csekély, jelentésük pedig sokkal szigorúbban van meghatározva. … Az A szókincset lehetetlen volna irodalmi célokra vagy politikai és filozófiai viták céljára használni. Csakis egyszerű és célszerű gondolatok kifejezésére való …” *([ORWELL 1989] 331.old.)*

„A B szókincs olyan szavakból áll, amelyeket szándékosan politikai célokra szerkesztettek, … egyenesen azt célozzák, hogy az őket használó személyre rákényszerítsék a kívánatos szellemi magatartást. … A B szókincs anyaga tulajdonképpen szóbeli gyorsírásféle, gyakran egész gondolatsorokat néhány szótagba sűrít össze … Minden szervezetnek, embercsoportnak, tannak, országnak, intézménynek, középületnek a nevét úgy rövidítik le, hogy egyetlen könnyen kiejthető, minél kevesebb szótagszámú szó őrizze az eredeti jelentést. … például az irattári osztályt irosz-nak nevezték, a teleképes osztályt telosz-nak és így tovább. Ennek nem csak időmegtakarítás a célja. … Az újbeszél minden más nyelvtől különbözik abban, hogy szótára évről évre vékonyabb … Minden csökkentés nyereség, mert a kisebb választék kisebb kísértést jelent a gondolkodásra.” *([ORWELL 1989] 333.old.)*

„A C szókincs a másik kettő kiegészítése, és csupán tudományos és technikai kifejezésekből áll…. Minden tudományos dolgozó vagy technikus megtalálhatja a számára szükséges szavakat a szakmájának szánt listában, a többi listán előforduló szavakat azonban csak

felületesen ismerik. … Az elmondottak alapján érthető, hogy meg nem felelő nézetek kifejezésre juttatása újbeszélül – egy nagyon alacsony színvonalon felül – majdnem teljesen lehetetlen." ([ORWELL 1989] 339.old.)

Megdöbbenve tapasztaljuk a hasonlóságot napjaink politikai beszéde és az *újbeszél* között. Az *1984* című regényben az *újbeszél*t azért hozták létre, hogy növeljék az állam egyénen való hatalmát azáltal, hogy befolyásolják, korlátozzák a gondolkodását. Az *újbeszél* feltűnik a politikai szónoklásban, amelynek eredményeként mindkét oldal problémája lecsökken: *„én (és a velem egyetértők) jó, … te, ő (mindenki aki nem ért egyet) rossz."*

Orwell tehát felfedezi és az *újbeszél* nyelv mélyén rekonstruálja a *dichotóm európai gondolkodás modelljét*. Azt a kompromisszumképtelen gondolkodási sémát, amely feketére és fehérre, sötétre és világosra, jóra és rosszra osztja a világot. Ez a kétértékű logika az, amely már a hétköznapi kommunikációban is szinte kizárja, sőt feleslegessé teszi a vitát, a megbeszélést, egyáltalán a beszélgetést, a gondolatcserét. Hogyne tenné, ha minden gondolatnak csupán két kimenetele lehetséges, igaz-hamis, jó-rossz, érdekes-érdektelen, … azaz az egyik érték ismerete (ez mindig az enyém) szükségtelenné teszi a másik megismerését. Hiszen, ha a másik azonos az enyémmel, akkor azért, ha viszont ellentétes, akkor úgyis hibás, rossz, ellenséges, tehát azért!

Erről a kétértékű gondolkodási modellről rövid idő alatt kiderül, hogy tulajdonképpen csak egyetlen értéket visel el, tehát valóban szükségtelenek az ettől eltérő gondolatok és természetesen az azokat kifejező szavak is. *Az egyértékű gondolkodás pedig az egyértékű társadalomhoz vezet!*

Orwell korában, azaz a 20. századi diktatúrák idején sokan úgy vélték, hogy néhány szó vagy kifejezés „kimondhatatlan"-ná tétele (gondolatbűn) korlátozza azt, hogy milyen ötleteket képviselhetünk (*újbeszél*), és így egyenlő a cenzúrával. Mások szerint az olyan kifejezések kitörlése, melyek mára kevésbé népszerűek, vagy sértővé válnak, valószínűtlenebbé teszi, hogy az emberek régimódi vagy sértő nézettel rendelkezzenek. Az a szándék, hogy az emberek gondolkodását a nyelv módosításain, a szóhasználat tudatos manipulálásán keresztül befolyásolják, tökéletes példa az *újbeszél*re.

Korunkban a demokráciák idején, az *újbeszél* alkalmazását, sőt terjesztését a kommunikációs technikák, de legfőképpen a média vette át. Ugyanis korunk a globális digitalizáció, az így létrehozott gigantikus mennyiségű jel (információ) minimális helyen tárolásának és maximális sebességű továbbításának lázában ég. Ez a*virtuális agárverseny effektus* (Érjük utol a nem létező nyulat egy virtuális agárversenyen!) az egyértékű társadalmi modell eredménye, amelyben a pénz (és ennek modern rokonai) mint univerzális, ám valójában virtuális csereeszköz megszerzése és elköltése a cél. Mivel virtuális a cél, így virtuális a versenyfutás is eme érték után. Közben azonban „az idő pénz" mindenható elve, a jelek, szavak, gondolatok, vagyis a kommunikáció mérhetetlen sűrítését követeli meg, amely pontosan Orwell látnokian leírt *újbeszél* nyelvéhez, majd a gondolatok minimalizálásához vezet.

A NAGY TESTVÉR 21. századi utódai tehát a NAGY MÉDIA és a NAGY INFORMÁCIÓS HÁLÓZATOK, amelyek a teleképhez hasonlóan vannak jelen mindannyiunk életében és észrevétlen módon irányítják gondolkodásunkat egy modern *újbeszél* nyelven. Mindezt teszik olyan technikai eszközökkel, amelyről Orwell nem is álmodhatott. Így válik tökéletes áldozattá az emberi kommunikáció ősi, személyességhez kötődő értéke, a *metakommunikáció*, amely a puszta információcserét emberi kultúrává emeli. Így válik a 21. századi

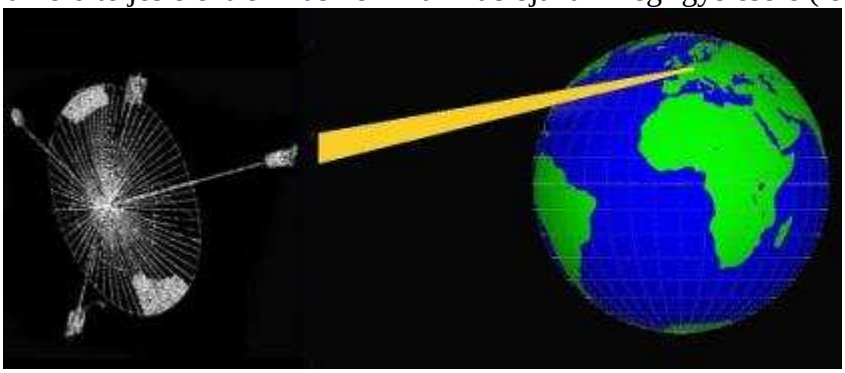
információalapú társadalom kulcskérdésévé a *lila tehén effektus*, amelynek lényege: ***vajon eldönthető-e, hogy a gigantikus digitális információtároló és kommunikációs rendszereinkben valóságos vagy virtuális információk vannak-e?!***

Pillanatnyilag úgy tűnik, hogy korunk globalizálódott NAGY TESTVÉRe nem érdekelt ennek megválaszolásában.

10.4. NAGY TESTVÉR az e-társadalomban ECHELON-ná vált

Jules Verne több mint 100 évvel később megvalósuló technikai és társadalmi utópiái után, Orwell volt képes arra, hogy víziói ne csupán a szárnyaló fantáziáját, de a jövendő kort, a globalizálódó emberi társadalmak jövőjét is megmutassák. Sőt, miközben a valóság rohamléptekkel alakult Orwell víziói szerint, az irodalomban is újabb és újabb követőkre talált az *újbeszél gondolat*. 1953-ban készült el *Ray Bradbury: Fahrenheit 451* című műve, majd a híres sci-fi író *Stanislav Lem: Éden*című regénye, amely tovább ihlette *Gheorghe Paun: 1994* című regényét.
Mindeközben egyre elemibb erővel kellene tudatosulni az emberiségben, miszerint nap mint nap arra a döbbenetes történelmi valóságra ébredünk, hogy a NAGY TESTVÉR zseniális irodalmi utópiája, már a könyv megjelenését megelőző években elindult a világméretű megvalósulás útján!

Már a II. világháború középső szakaszának idején megszületett az Egyesült Királyság és az USA titkosszolgálatai között a BRUSA COMINT (communications intelligence) egyezmény, melyet 1943. május 17-én ratifikáltak. Az Egyesült Királyság 1946-47-ben kibővítette a szövetségeseket Kanada, Ausztrália és Újzéland háború utáni hírszerző ügynökségeivel. Így jött létre az 1948-ban megkötött titkos UK-USA (Nagy-Britannia és Amerikai Egyesült Államok) megállapodás, illetve szövetség, amelynek tartalma és hatálya napjainkban is érvényes.
Az UK-USA szövetség fő koordinátora, összefogó szervezete, a National Security Agency (az Amerikai Egyesült Államok Nemzetbiztonsági Hivatala, rövidítve: NSA).
A szerződés jóval későbbi bővítése során kerültek az UK-USA szövetségesek közé Németország, Japán, Norvégia, Délkorea és Törökország titkosszolgálatai. A szigorúan titkos körülmények között megkötött UK-USA megállapodás megteremtette az alapját annak a világméretű kémműholdas lehallgató rendszernek, amely ma az ECHELON (hadrend, harcvonal) nevet viseli és a Földön ma létező legnagyobb szellemi és technikai kapacitásokat összpontosítja a Föld teljes elektronikus kommunikációjának megfigyelésére (lehallgatására).



COMINT (Communications Intelligence) műholdak geostacionárius pályán (pl. VORTEX), földi mikrohullámú kommunikáció lehallgatására

Ez a megvalósult, globális csupa szem és fül NAGY TESTVÉR!

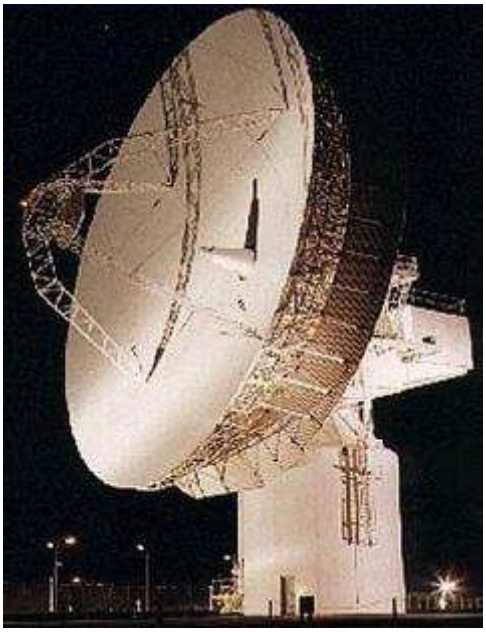
Az elektronizáció és digitalizáció narkotikuma által egyre rohanóbb világunkban a 20. század végére eljutottunk oda, hogy a valóság messze megelőzte az irodalmi fantáziát. Ma, 2001. szeptember 11-e egy évtizedes árnyékában, egyre aktuálisabb irodalmi alkotássá vált George Orwell 60 éves utópiája, a NAGY TESTVÉR és *újbeszél* társadalma.

10.5. Valóban mindent „lát" és „hall" a NAGY TESTVÉR?

A nagykövetségek és diplomáciai célpontok mellett már az 1950-es évektől az elektronikus kommunikáció teljes spektrumának szűrése volt a cél, vagyis válogatás nélkül lehallgattak minden hozzáférhető (vezetékes, rádió, mikrohullámú és műholdas) kommunikációs csatornát, üzleti és magánbeszélgetéseket egyaránt. Az ECHELON rendszer három alrendszerből áll:

1. Nemzetközi Telekommunikációs Műholdak (INternational TELecommunications SATellites = INTELSAT)
A legtöbb ország telefon társaságai az INTELSAT műholdakat használja elsősorban a civil, de részben a diplomáciai és állami telekommunikáció lebonyolítására. Az ECHELON rendszer INTELSAT fogadóállomásai:
- *Morwenstow (England)* – az Atlanti és Indiai óceán feletti műholdak forgalma Európa, Afrika és nyugat Ázsia felé
- *Sugar Grove (West Virginia)* – Atlanti óceán feletti műholdak forgalma észak és dél Amerika felé
- *Yakima (Seattle mellett)* – Csendes óceáni és távol keleti műholdak
- *Waihopai (Újzéland)* – Csendes és Indiai óceáni műholdak
- *Geraldton (Ausztrália)* – Csendes és Indiai óceáni műholdak

Műholdas lehallgató állomás Sugar Grove-nál (West Virginia), hat antennát állítottak az európai és Atlanti óceáni régió távközlési műholdjainak lehallgatására



A GCHQ által 1972-ben épített „árnyék" állomás, ami az Intelsat üzeneteket hallgatja le az UK-USA számára

Műholdas földi terminál Etam-nál (West Virginia), amelyik az Intelsat IV-en keresztül köti össze Európát az USA-val

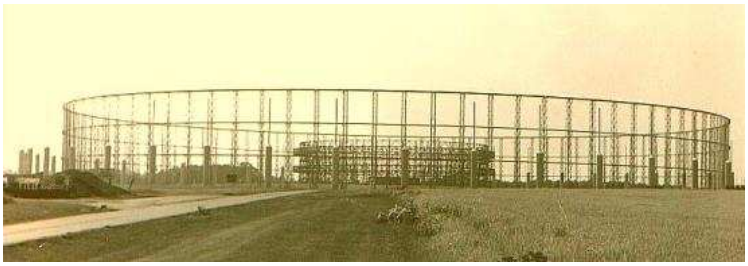
2. Nem INTELSAT műholdak

Ezek a műholdak a regionális kommunikációkat bonyolítják, amelyeket a következő fogadó állomások felügyelnek:

- *Menwith Hill (Anglia)*
- *Shoal Bay (Ausztrália)*
- *Leitrim (Kanada)*
- *Bad Aibling (Németország)*
- *Misawa (Japán)*

3. Földi és tenger alatti rendszerek

A nagy városok (többnyire fővárosok) kommunikációja általában mikrohullámú hálózatokon keresztül történik. A föld, illetve tenger alatti kommunikáció lehallgatása könnyen megvalósítható, amint a kábelek felszínre emelkednek és csatlakoznak a mikrohullámú adó-vevő tornyokhoz.



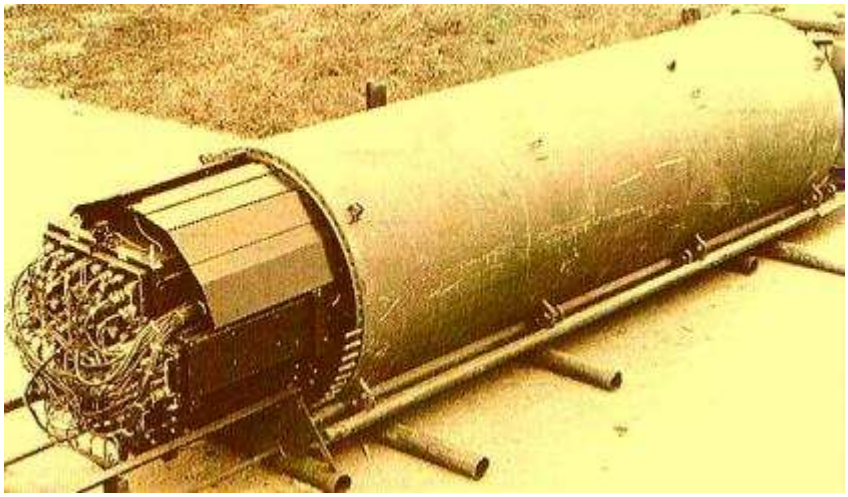
Nagyfrekvenciás rádió lehallgató antenna

10.6. NAGY TESTVÉR a tengerek mélyén

A telekommunikációs technika 21. századi forradalma eredményeként, ma már az infokommunikáció jelentős része fényhullámok formájában történik, föld és tenger alatt húzódó üvegszálas kábeleken.[67] Ez új kihívást jelent az ECHELON rendszer fenntartói és felhasználói számára, hogy új lehallgatási módszereket vezessenek be. Az NSA már 1989-ben kutatócsoportot hozott létre az üvegszáloptika lehallgathatóságának kidolgozására.

Egykori hírszerző tisztek elmondása szerint az 1990-es évek közepén az NSA pár száz méter mélyen, speciális kamrával felszerelt tengeralattjáróval lehallgató eszközt helyezett el a kontinenseket összekötő optikai kábeleken. A technika rohamos fejlődését jellemzi, hogy a napjainkban lefektetésre kerülő Csendes óceán alatti kábelek már 100 millió telefonhívást tudnak kezelni egyszerre.
Michael Hayden (1999–2005 az NSA igazgatója) egy interjúkérdésre adott válasza, amely a tenger alatti kábelek lehallgatására vonatkozott, azt sugallta, hogy az információk elérése nem probléma, azonban az adatok nagy mennyiségének feldolgozása gondot okoz. Ez különösen érdekes, annak fényében, hogy a mai napig az NSA rendelkezik a világ legnagyobb szuperszámítógépes és informatikus, matematikus, kriptográfus kapacitásával.

[67] A világ első óceán alatti üvegszáloptikai kábelét New Jersey és Nagy Britannia között az AT&T fektette le 1988-ban. A karvastagságú kábel egyszerre 40 ezer hívást tudott továbbítani, ami ötszöröse volt a legjobb tenger alatti rézvezeték kapacitásának és összemérhető volt a műholdon közvetített hang alapú forgalommal. A Csendes óceán alatt 1991-ben fektették le az első hasonló optikai kábelt, amelynek hossza 1997-ben elérte a 20 ezer kilométert és összeköttetést biztosított Európa, é-Afrika, d-Ázsia és Japán között. Ezt követően Oroszország és Kína is lefektetett mélytengeri kábeleket.

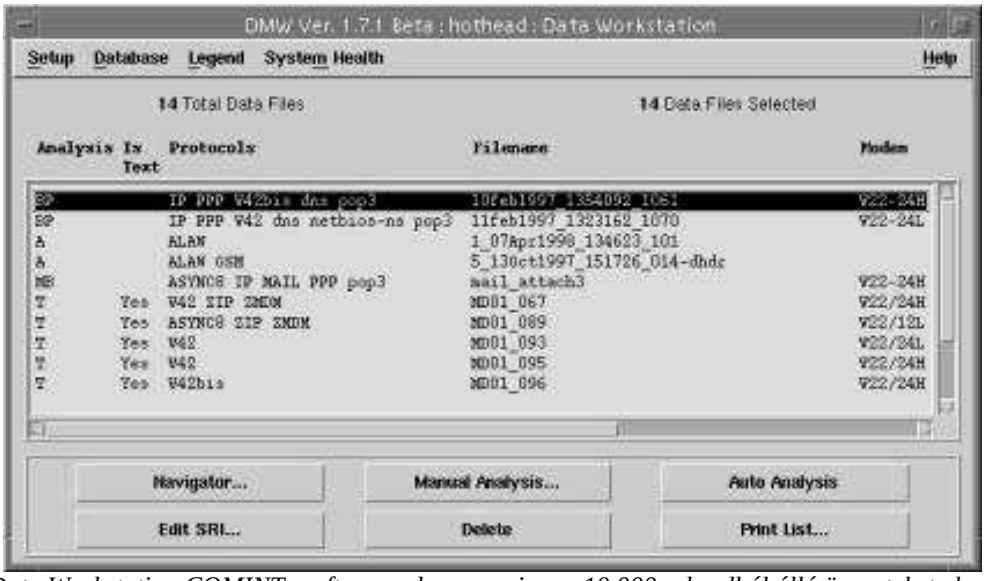


Tenger alatti kábel „megcsapoló hüvely”, amit Kamcsatkánál fektetett le egy USA tengeralattjáró

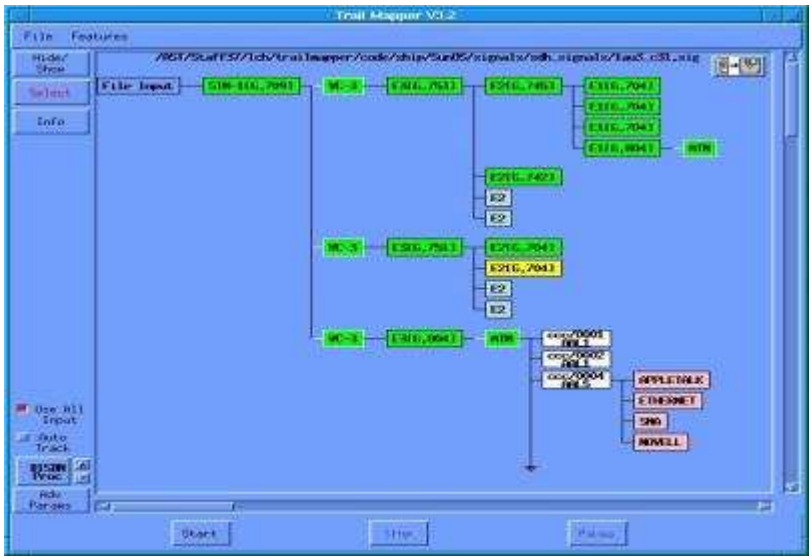
10.7. NAGY TESTVÉR az internetben

A szuperszámítógépek megjelenésével, az 1970-es évek elején az NSA automatizálta és számítógép-hálózatba szervezte az UK-USA állomásait. A nyilvános számítógép-hálózatok megjelenésével (a nemzetközi terrorizmus és a gazdasági kémkedés elleni fellépéssel indokolva) az internetes adatforgalomra is ráálltak, amelynek eredményeként szinte minden leolvasott weboldal, elküldött e-mail archiválódik valamelyik lehallgatóállomáson, csakúgy, mint a telefonbeszélgetések, amelyeket hangfelismerő technológiák segítségével analizálnak. A számítógépek minden állomáson ugyanazt a szoftvert futtatják, ez a *Dictionary (Szótár)*, amely kulcsszavas keresést tesz lehetővé a hatalmas adathalmazban.[68]
Az ECHELON tagországok titkosszolgálatai folyamatosan frissítik a Szótárt, amelyben a számukra valamiért érdekes kulcsszavak kapnak helyet. A szűrt kommunikációt átfuttatva ezen a programon, a rendszer kiválogatja a „gyanús” üzeneteket, ezek közül pedig emberi intelligenciával választják ki a valóban fontos információkat. Az egész folyamatot az NSA koordinálja. Az ECHELON európai központja az észak-angliai Menwith Hill állomás. Itt fut össze az összes adat, amelyet az Egyenlítő fölött geostacionárius pályán álló, a nemzetközi telefon és adatforgalom nagy részét bonyolító Intelsat műholdak lehallgatásáért felelős bázisok gyűjtenek (Morwenstrow (Anglia), Yakima (USA), Geraldton (Ausztrália), Waihopai (Új-Zéland). Más ECHELON-csomópontok az óceánok alatt húzódó távközlési kábeleket és a belföldi mikrohullámú vonalakat is figyelik.

[68] A Dictionary felépítésével és felhasználásával külön fejezet foglalkozik a [TDT 2004-k] kötetben.



A Data Workstation COMINT szoftverrendszer maximum 10.000 rekordból álló üzeneteket elemez, azonosítja az Internet forgalmat, e-mail üzeneteket és csatolt állományokat

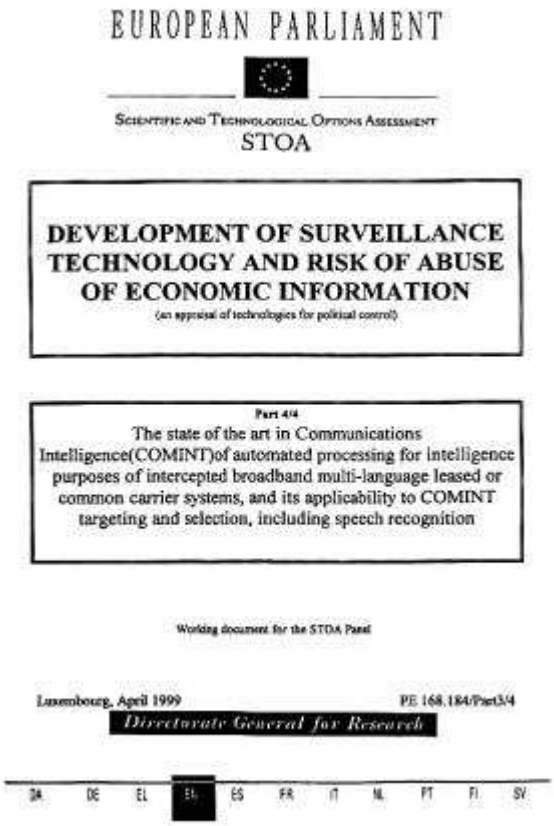


Az NSA „Nyomtérképező szoftvere”, mutatja a nagykapacitású STM-1 digitális kommunikációs rendszer automatikusan lehallgatatott belső privát hálózatát

10.8. A STOA jelentések leleplezték az 50 éves NAGY TESTVÉR-t

Majdnem 50 évig teljes titokban, a nyilvánosságtól mélyen elzárva működött az ECHELON rendszer, míg az 1990-es években megtört a lehallgató hálózatot addig övező teljes hallgatás. Egyre több részlet látott napvilágot kiugrott vagy az amerikaiakat kritizáló titkosszolgák jóvoltából. 1991-ben egy korábbi GCHQ-tiszt a BBC kamerái előtt számolt be arról, hogy a titkosszolgálat minden Londonból ki- és bemenő telexet leolvas. *„Mindent lehallgatnak: a nagykövetségeket, az összes céget, még a születésnapi üdvözleteket is. Betáplálják a Szótárba”* – állította az ügynök.
A sajtó nyomására az Európa Parlament emberi jogi bizottsága szakértőkből álló vizsgálóbizottságot hozott létre, amely 1997-es titkos, majd 1999 és 2001-es nyilvános

jelentésének (STOA[69] Report) már a címe is sokatmondó [EU-REP 2001]: *A lehallgatási technológia fejlődése és a gazdasági információkkal való visszaélés kockázata*


EUROPEAN PARLIAMENT

SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA

DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION
(an appraisal of technologies for political control)

Part 4/4
The state of the art in Communications Intelligence(COMINT)of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition

Working document for the STOA Panel

Luxembourg, April 1999 PE 168.184/Part3/4
Directorate General for Research

DA DE EL EN ES FR IT NL PT FI SV

Az Európa Parlament 1999-es STOA jelentésének [STOA-REP 1999] *címlapja*
(A lehallgatási technológia fejlődése és a gazdasági információkkal való visszaélés kockázata)

A belső címoldalon pedig ez olvasható: *„JELENTÉS a privát és kereskedelmi kommunikáció lehallgatására szolgáló globális rendszer létezéséről (ECHELON lehallgató rendszer)”*

majd a bevezető így kezdődik: *„Európán belül minden telefont, e-mailt és faxüzenetet rutinszerűen ellenőriz az NSA. A kiválasztott információkat a kontinensről London és Menwith Hill érintésével műholdon juttatják el a marylandi Fort Meade központba”*.

A STOA jelentéseknek nem csak a szakmailag részletesen és lenyűgöző alapossággal kidolgozott tartalma meggyőző, de annak jelentősége is nehezen túlbecsülhető, hogy ezek által vált nyilvánossá az 50 éve a legszigorúbb titokban kezelt globális műholdas lehallgató rendszer létezése. E helyen a teljes jelentés közzétételére nincs mód és annak alapvetően biztonságtechnikai jellege ezt a nem szakértő olvasók számára nem is indokolja, azonban mindenkinek sokatmondó lehet a jelentés tartalomjegyzéke és rövid tartalmi összefoglalása, amelynek magyar fordítása a következőkben olvasható.

Mindenképpen szeretném minél szélesebb nyilvánossággal megismertetni azokat akik a legtöbbet tették a JELENTÉS megszületéséig vezető úton. Ezért e fejezet végén külön MELLÉKLET-et készítettem e kitűnő szakújságíróknak.

[69] Scientific and Technical Options Assessment (Tudományos és Műszaki Lehetőségek Értékelése)

JELENTÉS

privát és kereskedelmi kommunikáció lehallgatását szolgáló globális rendszer létezéséről
(ECHELON lehallgató rendszer)
2001. július 11.

1. Bevezetés

1.1. A bizottság felállításának okai
1.2. A STOA tanulmányok létrehozásának igénye, egy globális lehallgató rendszer, melynek kódneve ECHELON
1.2.1. Az első STOA jelentés 1997.
1.2.2. Az 1999-es STOA jelentés

1.3. A bizottság felhatalmazása
1.4. Munkamódszer és ütemezés
1.5. Az ECHELON rendszer jellemzői

2. A külföldi hírszerző szolgálatok tevékenysége

3. A telekommunikáció lehallgatásának műszaki feltételei

4. Műholdas kommunikációs technológia

5. Nyomok amelyek legalább egy globális lehallgató rendszer létezését igazolják

5.1. Miért szükséges a nyomok alapján elindulni?
5.1.1. A külföldi hírszerző szolgálatok lehallgatási tevékenységének bizonyítékai
5.1.2. Földrajzilag különböző helyeken működő lehallgató állomások létezésének bizonyítékai
5.2. Hogyan ismerhető fel egy műholdas lehallgató állomás?
5.2.1. 1-feltétel: az üzembe helyezés felismerése
5.2.2. 2-feltétel: antenna típus
5.2.3. 3-feltétel: antenna mérete
5.2.4. 4-feltétel: hivatalos forrásokból származó bizonyítékok

5.3. Nyilvánosan hozzáférhető adatok ismert lehallgató állomásokról

5.3.1. Módszer
5.3.2. Részletes elemzés
5.3.3. Az elemzések összefoglalása

5.4. Az UK-USA megállapodás

5.4.1. Az UK-USA megállapodás történelmi kialakulása
5.4.2. A megállapodás létezésének bizonyítékai

5.5. A nyilvánosságra hozott amerikai dokumentumok értékelése

5.5.1. A dokumentumok természete
5.5.2. A dokumentumok tartalma
5.5.3. Összefoglalás

5.6. A terület szakértőitől és újságíróktól származó információk[9]

5.6.1. Nicky Hager könyve
5.6.2. Duncan Campbell
5.6.3. Jeff Richelson
5.6.4. James Bamford
5.6.5. Bo Elkjaer és Kenan Seeberg

5.7. A hírszerző szolgálatok korábbi alkalmazottainak nyilatkozatai

5.7.1. Margaret Newsham (korábbi NSA alkalmazott)
5.7.2. Wayne Madsen (korábbi NSA alkalmazott)
5.7.3. Mike Frost (a kanadai titkosszolgálat korábbi alkalmazottja)
5.7.4. Fred Stock (a kanadai titkosszolgálat korábbi alkalmazottja)

5.8. Kormányzati forrásokból származó információk
5.8.1. USA
5.8.2. Egyesült Királyság
5.8.3. Ausztrália
5.8.4. Újzéland
5.8.5. Hollandia
5.8.6. Olaszország

5.9. Kérdések a Tanácshoz és a Bizottsághoz

5.10. Parlamenti jelentések

5.10.1. A Comité Permanent R (Belgium felügyelő bizottsága) jelentései
5.10.2. A francia Nemzetgyűlés Nemzetvédelmi Bizottságának jelentése
5.10.3. Az olasz parlament Nemzet és Állambiztonsági Bizottságának jelentése

6. Létezhetnek más globális lehallgató rendszerek?
7. Egy ECHELON típusú lehallgató rendszer és az EU törvények kompatibilitása
8. A hírszerző szervezetek által felügyelt kommunikáció kompatibilitása az alapvető személyiségjogokkal
9. Az EU állampolgárokat megfelelően védik a hírszerző szolgálatok tevékenységével szemben?
10. Védekezés az ipari hírszerzés ellen
11. Kriptográfia mint az önvédelem eszköze
12. Az EU külkapcsolatai és a hírszerzés
13. Következtetések és ajánlások

A fenti STOA jelentés a tények és dokumentumok precíz feltárásán alapuló fő gondolatai az alábbiakban foglalhatók össze:

1. A kommunikációs hírszerzés (COMINT), a külföldi távközközlési eszközök titkos lehallgatása, bevált gyakorlat volt majdnem minden fejlett országban, amióta ezt a nemzetközi telekommunikáció lehetővé tette. A COMINT nagyarányú ipari tevékenység, amely hírszerzési információkkal látja el a diplomácia, a gazdaság és a tudományos kutatások résztvevőit.

2. Összesen, hozzávetőleg 15-20 milliárd Eurót költenek a COMINT-ra és a kapcsolódó tevékenységekre évente. Ennek a ráfordításnak a legnagyobb részét az UK-USA szövetség angol nyelvű nemzetei fedezik. Ez a jelentés feltárja, hogy a COMINT szervezetek több mint 80 évi előkészület után szereztek átfogó hozzáférést a világ nemzetközi kommunikációjának jelentős részéhez. Azaz a kereskedelmi műholdak, a nagytávolságú kommunikáció, a tengeralatti távközlő kábelek és az Internet jogellenes lehallgatásához. A hozzávetőlegesen 120 műholdból álló rendszer jelenleg egyidejű, összehangolt működéssel végzi a lehallgatást (információ gyűjtést).

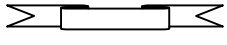
3. A nagymértékben automatizált UK-USA rendszert, amit ECHELON-ként ismernek, Európában széles körben tette ismertté az 1997-es STOA jelentés. Az a jelentés akkor még csak két elsődleges forrásból származó információt összegzett az ECHELON létezésére vonatkozólag. A jelen jelentés új, bizonyító erejű dokumentumokat mutat be az ECHELON rendszerről és annak alkalmazásáról a kommunikációs műholdak lehallgatására vonatkozóan. Műszaki melléklet is kiegészíti e jelentést, amely részletes leírását adja a COMINT módszereinek.

4. A COMINT információkat, amelyek a nemzetközi kommunikáció lehallgatásából származnak, régóta rutinszerűen használták magánszemélyek, kormányok, kereskedelemi és nemzetközi szervezetek érzékeny adatainak összegyűjtésére.

5. Ez a jelentés egy korábban ismeretlen nemzetközi szervezetet azonosít (ILETS), amely parlamenti megbízás nélkül készít terveket, az új kommunikációs rendszerekhez szükséges gyártásra és üzemeltetésre vonatkozóan. Ezek ellenőrzési kapacitása a nemzetbiztonsági és törvényvégrehajtó szervezetekre épül.

6. A COMINT szervezetek egyre jobban érzékelik, hogy a globalizálódó kommunikáció műszaki problémái növekednek, így a jövőbeli működés költségesebb és korlátozottabb lehet mint jelenleg. Eme nehézségek észlelése lehet az alapja a politika „védelmi célú” beavatkozásának.

7. A jelentés több konkrét ügyet is említ. Például 1994-ben a francia többségi tulajdonban levő Airbus konzorcium tárgyalt a szaúdi légitársasággal egy 30 millió frankos üzletről. Az üzleti tárgyalásokról szóló faxokat és telefonokat az ECHELON segítségével lehallgatták és az NSA továbbította az adatokat az amerikai McDonnel-Douglasnek, amely végül elnyerte az üzletet.



Összegzésként a STOA jelentések alapján kimondhatjuk, hogy az ECHELON gyakorlata ellentétes minden szabad ország alkotmányával és adatvédelmi törvényeivel, legtöbbször mégis a kormányok és a multinacionális telefontársaságok tudtával és beleegyezésével működik, annak ellenére, hogy többször bebizonyosodott: *főleg az USA, de más UK-USA tagország is, felhasználja politikai célokra az ECHELON rendszert.*

10.9. A „húsevő" NAGY TESTVÉR

Az USA Szövetségi Nyomozóiroda (FBI) emberei már néhány órával a 2001. szeptember 11-i terrortámadások után telepíteni kezdték a ***Carnivore (húsevő)***névre keresztelt Internet lehallgató rendszert [COLLING 2000] az amerikai internetszolgáltatók szervereire. Hivatalosan deklarált célja a bűncselekményekkel gyanúsított személyek e-mail üzeneteinek felügyelete volt.

A Carnivore rendszer (hivatalos neve: DCS 1000) milliónyi e-mailt tud másodpercenként átnézni. A rendszert az FBI quanticoi ügynökségén Edward Hill speciális ügynök tervei alapján fejlesztették ki. A Carnivore-t a használathoz közvetlenül az Internet szolgáltató hálózatára kell kapcsolni. Ha ez megtörténik, elméletileg figyelhető minden felhasználó kommunikációja, kezdve a levelezéstől az online banki műveleteken át a webezésig.

Ez a rendszer jelentős jogi problémákat vet fel a békés, jószándékú internetezők személyiségjogainak megsértésével kapcsolatban. Az Electronic Privacy Information Center (EPIC: Elektronikus Adattitkossági Központ) alig pár hónappal a Carnivore telepítése után jelezte a nyilvánosság számára, hogy ez az email megfigyelőrendszer potenciális visszaélésekre ad lehetőséget [DONALD 2000].

Az ECHELON-nal ellentétben, a Carnivore-t már nem tudták évtizedekig titokban tartani. Az EPIC hatására az FBI már 2000. januárjában Edward Hill aláírásával nyilatkozatot adott ki, amelyben elismerte a rendszer létezését [HILL 2000]. A nyilatkozat fontosabb állításainak magyar fordítása:

„Én Edward Hill a következő nyilatkozatot teszem:

1. Az FBI speciális ügynöke vagyok 10 éve. A műszaki berendezésekre specializálódtam, beleértve az elektronikus lehallgató berendezéseket. Jártas vagyok az Internet és az Internet lehallgatására szolgáló eszközök alkalmazásában.

2. Ha engedélyezik, én vagy más technikusok üzembe helyezünk egy Carnivore nevű programot. A program az EarthLink hálózat routerére lesz telepítve. …. A router és az EarthLink hálózat egyaránt a telefonvonalakhoz kapcsolódik és a csomagkapcsolt hálózat információit továbbítja a telefonvonalakon. A Carnivore program figyeli az EarthLink-re bejövő telefon forgalmat, és regisztrálja az üzenetek aláírójának log-in nevét, vagy email azonosítóját. … A program sem az üzenet tárgyát, sem annak tartalmát nem rögzíti.

3. … Mivel a számítógép kapacitás korlátozott, a program pár percenként 8-10 millió email feldolgozását képes elvégezni.

4. A program nem képez biztonsági kockázatot az EarthLink hálózatban. Bár a Carnivore program távolról elérhető, több biztonsági elemet tartalmaz, amelyek megakadályozzák az EarthLink rendszerhez való illetéktelen hozzáférést. …"

FBI Nyilatkozat a Carnivore-ról

DECLARATION

I Edward Hill hereby declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation, and have been an Agent for 10 years. I specialize in technical equipment, including electronic surveillance equipment. I am familiar with the Internet and with surveillance devices used for the Internet.

2. If authorized by this court, I or other technicians intend to install a program called Carnivore to obtain the information sought in this order. The program will be installed on EarthLink's network, most likely on a "router" used by EarthLink. A "router" is a transmission device that processes packetized network information. Both the router and EarthLink's network are connected to the telephone lines and transmit packetized network information over the telephone lines. The Carnivore software program watches the incoming telephone traffic to EarthLink and looks for the targeted subscriber's log-in name or electronic mail account name. If it finds the target's log-in name, the program follows the target while the target is on line. The program then captures only the header information for electronic mail messages sent or received by the target while the target is on line. If the program finds the target's electronic mail account name, it will capture the header information associated with that electronic mail message. Specifically, the program will capture the time, date, and the addressing information (i.e., Internet identity) for electronic mail messages sent to or from the account. The program will not

capture the subject or regarding line on the electronic mail message, nor does it capture the content of the message or any information concerning the target's other on line activity.

3. Although the program is capable of capturing more than the information authorized under the order, I or the installing technicians will configure the program in a manner that will prevent the program from capturing any information that is not authorized under the order. In addition, the computer used to run the program has limited memory capacity and limited ability to process information. Because of these limitations the computer used to run the program would be overloaded within a few minutes if it attempted to collect all of the information on EarthLink's 8 to 10 million e-mail messages. Moreover, the program will be installed on a particular entry point into EarthLink's network, and as such would not have access to all of EarthLink's customers.

4. The program should not create a security risk for EarthLink. Although the Carnivore program is remotely accessible, it has several security provisions that prevent an intruder from obtaining unauthorized access to EarthLink's system. Even if an intruder did obtain such access, the program lacks a TCP/IP protocol stack, which means that the intruder would be unable to communicate with EarthLink's system from the government's computer. I and other agents with whom I work have installed this program at many other service providers (including AT&T) and have not had security problems or objections from the providers.

01/01/00 14:55 FAX

5. I have participated in the installation of several pen register and trap and trace devices on Internet electronic mail accounts and am aware of several others.

I declare under the penalty of perjury that the foregoing is true and correct. Executed January 31, 2000 in Quantico, Virginia.

Edward Hill

26

A 21. század információalapú társadalmának tehát kulcskérdése a hatalom és a civil társadalom közötti egyenrangú és egyenszilárdságú információbiztonság. Ennek megvalósításához vezető úton az első lépés az lenne, hogy megfogadjuk N. Wiener azon intelmét, amelyet a NAGY TESTVÉR megszületésével egyidőben fogalmazott meg:
„Az amerikai világban az információ sorsa az, hogy áru lesz. Nem az én dolgom elbírálni, hogy ez a kereskedői szemlélet erkölcsös-e vagy sem, az én dolgom az, hogy megmutassam, ha ez a szemlélet érvényesül, az az információ és a vele kapcsolatos fogalmak félreértéséhez és főleg félrekezeléséhez vezet."
Norbert Wiener idézett gondolata tehát nem csupán az információra, hanem az információalapú társadalomra is igaz. A Wiener által jelzett „félreértések" és „félrekezelések" társadalmi méretekben végzetesek lehetnek, ami egyértelműen arra a következtetésre vezet, hogy A JÖVŐ BIZTONSÁGOS TÁRSADALMA NEM LEHET ÜZLETI VÁLLALKOZÁS!

Ezen gondolatokra azonban az élet történelmi választ produkált, amikor 2001. szeptember 11-én a Földünket körülvevő ECHELON információpajzs, akárcsak a természetes védelmet nyújtó ózonpajzs, kilyukadt! Az elmúlt majd 10 évben a szeptember 11-i terrortámadásról született elemzések olvasása után felvethető a kérdés: *Vajon az ECHELON információpajzsán tátongó lyuk 2001. szeptember 11-én keletkezett, vagy a kezdetektől ott volt, csak a rendszer működésében érdekeltek nem akarták észrevenni?*

„A telekép egyszerre volt vevő és adókészülék. …
Bizonytalan volt, hogy a Gondolatrendőrség milyen gyakran és milyen rendszer szerint kapcsolódik be egy-egy magán-teleképkészülékbe.
Még az is elképzelhető volt, hogy mindenkit állandóan figyelnek. Mindenesetre akkor kapcsolódhattak be akárkinek a készülékébe, amikor csak akartak.
Az embernek abban a tudatban kellett élnie –
s abban a tudatban is élt, ösztönné vált megszokásból-, hogy minden hangját hallják, s kivéve, ha sötét van, minden mozdulatát megfigyelik."
([ORWELL 1989] 8.old.)

10.10. Polgári szabadságjogok, vagy „terrorizmus elleni küzdelem" ?

Egészen megdöbbentő, hogy a demokrácia és a polgári szabadságjogok paradicsomaként, a Föld többi országa számára példaképül szolgáló USA-ban, a STOA jelentések nyilvánosságra kerülése után is, csupán egy névtelenül nyilatkozó biztonságtechnikai szakember próbálta a nyilvánosság előtt elismerni: *„A legtöbb szakmabeli, aki az USA-ban tud az ECHELONról és más elektronikus lehallgatási technikákról, kapcsolatban áll az NSA-val, vagy más állami ügynökséggel és ezek tanácsára nem feszegetik a témát. Eddig egyedül az Európai Unió merte hivatalosan vizsgálni ezeknek a rendszereknek a működését."*

Ennél csak a Pew Internet & American Life Project 2001-ben közzétett vizsgálata megdöbbentőbb, mely szerint az USA polgárok 54%-a szerint jó dolog, hogy az FBI figyeli az e-mail forgalmat, míg ezt csupán 34% utasítja el.

Ezt a csipkerózsika álomba ringatott polgárságot igyekezett felébreszteni az American Civil Liberties Union (ACLU), azaz az Amerikai Polgárjogi Unió 2001. tavaszán indított kampánya. Ugyanis az ACLU szerint a Carnivore és az ECHELON (amelynek létezését hivatalosan még el sem ismerik) veszélyezteti a polgárok magánélethez való jogát, és azt az alkotmánykiegészítést, amely védi az amerikai polgárt az indokolatlan kormányzati megfigyeléstől. A The New Yorker magazin 2001. április 15-i és a New York Times április 16-i számában megjelenő hirdetések egy mobiltelefont ábrázolnak, amely felett a *„Háromirányú hívás: te, a hívott fél és a kormány”* felirat olvasható.

Az ACLU hírdetése a New York Tmes 2001. április 16-i számában

Az ACLU kampány célja az volt, hogy jogszabályi keretek közé szorítva, átfogó ellenőrzésnek vessék alá az amerikai kormányzat által működtetett digitális megfigyelési rendszereket. A szervezet a fentihez hasonló egészoldalas hirdetéseket adott fel, hogy felrázza a gyanútlan amerikai tömegeket. A hirdetések szövege tehát sokkolóan igyekszik felhívni az olvasók figyelmét, hogy ***„A telefonhívás immár háromirányú! Ön, a hívott fél, és a kormány között folyik!”*** A hirdetés felszólítja az olvasót (sajnos kevés sikerrel), hogy látogasson el az ACLU weboldalára, ahol rendelkezésére áll egy link, melynek segítségével tiltakozó üzenetet tud küldeni a kongresszusi képviselőknek.

Ma már tudjuk, hogy a sikeres 2001. szeptember 11-i terrortámadás egyértelműen a hatalmas titkosszolgálati apparátust támogató ECHELON fiaskója volt, amelynek sok százmilliárd dolláros költségvetése hivatalosan a „terrorizmus elleni küzdelmet” célozta. A fiaskót azonban a kormány nem arra használta fel, hogy új nemzetbiztonsági filozófiát dolgozzon ki, sőt a fiaskó elemzése éppen az ACLU polgári szabadságjogok védelmére irányuló törekvései ellen hatott.
Ugyanis a tragédia után két nappal elfogadott antiterrorista törvénycsomag keretében elsőként az Egyesült Államokban kapták meg a szükséges törvényi támogatást az Interneten zajló privát kommunikációt is állami ellenőrzés alá helyező technológiák, elsősorban a Carnivore (később a DCS–1000 kódnévre átkeresztelt) e-mail megfigyelőrendszer, amelyet ekkor már

két éve fejlesztett a Szövetségi Nyomozóiroda. A Carnivore tömeges bevetésére korábban alkotmányossági problémák miatt nem kerülhetett sor az USA-ban.

A kémtechnológiák kifejlesztésében élen járó Amerikai Egyesült Államokban ugyanis rendkívül szigorúan szabályozták a belföldi elektronikus kommunikáció lehallgatásának lehetőségeit. Miközben a második világháború óta fejlesztett ECHELON világszerte ellenőrzi, rögzíti és szűri a kommunikáció teljes spektrumát, az országon belül – legalábbis a terrortámadásig – meg volt kötve a hatóságok keze. Amikor 2000-ben nyilvánosságra került, hogy az FBI belföldi e-mail megfigyelő technológiát fejleszt és tesztel, kongresszusi botrány lett az ügyből, mert a Carnivore az ECHELON-nál már bevált módszerrel, a teljes adatforgalom rögzítésével, illetve kulcsszavas szűrésével operált, tehát aligha volt tekinthető eseti és célzott megfigyelő eszköznek. Mégis a *„terrorizmus elleni küzdelem” zászlajátlobogtatva* befektetett sok százmilliárd (adó)dollár ellenére, elszalasztották bin Ládent és az USA elszenvedte eddigi történelmének egyetlen, megrendítő terrortámadását!

2001. szeptember 11. után azonban az EU-ban is felülkerekedtek a lehallgatáspártiak. Az Európai Parlament május végén elfogadta a magánjellegű adatok elektronikus védelméről szóló 1997-es irányelv 15. bekezdésének megváltoztatását. A két legnagyobb képviselőcsoport – az Európai Néppárt és az Európai Szocialisták – kompromisszuma nyomán megszavazott szabályozás szerint, ezt követően a magántitok védelme a nemzet- vagy közbiztonság védelme érdekében felfüggeszthető, amennyiben az *„a demokratikus társadalmi rendből következően szükséges, helyénvaló és arányos intézkedés”*.

Ezek után a lehallgatás műszaki feltételeinek megteremtésére irányuló erőfeszítések törvényes volta kétségbevonhatatlan: titkosszolgálati lehallgatóberendezések üzemelnek minden vezetékes- és mobiltelefon-szolgáltatónál. A kérdés az, milyen mértékű hozzáférést biztosítanak ezek az eszközök a felhasználók személyes adataihoz, hiszen a műszaki lehetőség az Interneten sem korlátozódik egyes beszélgetések, levélváltások célzott figyelésére. A belföldi, illetve a nemzetközi forgalmat bonyolító vonalakon gyakorlatilag az összes információ áthalad, ami egy internetszolgáltatónál egyáltalán megfordulhat: a weboldallekéréseken túl az elektronikus levelek, a csevegőfórumokon elhangzó publikus vagy magánbeszélgetések egyaránt, a felhasználókra vonatkozó személyes adatokkal és az őket azonosító IP-címekkel együtt. Ha az Internetnek a törvény által lehetővé tett lehallgatása az „amerikai módszerrel”, tömeges adatgyűjtés és az eredmény számítógépes kiértékelése formájában valósul meg, vagyis nem eseti vagy specifikus, hanem totális jellegű, a begyűjtött információtömeg feldolgozásának és kiértékelésének, magánszemélyekre vagy cégekre vonatkozó akták összeállításának csak a lehallgató technológia fejlettsége, az adatokat feldolgozó számítógépek kapacitása szab határt. A ma már sajnos kisebbségbe került szakértői vélemények szerint *a tömeges információgyűjtés a kódoltan kommunikáló terroristák ellen hatástalan, az átlagpolgár civil szféráját viszont súlyosan sérti.*

Léteznek olyan módszerek, amelyek magát a lehallgatást akadályozzák vagy teszik lehetetlenné, de ezeket éppen azok a csoportok használják fel nemtelen céljaik elérése érdekében, akik ellen a hivatalos deklaráció szerint a lehallgatást alkalmazzák. Meg kell állapítanunk tehát, hogy ezen az egész életünket alapvetően befolyásoló területen is az a globalizálódott anti-bűnmegelőzési filozófia érvényesül, amelyet a *„hogyan fog az elméleti fizikus oroszlánt a sivatagban?”* gondolatkísérlet jól illusztrál: *„Szitáljuk át a sivatagot egy elegendően nagy és megfelelő lyukméretű szitán. Ami kihullik az a homok, ami fennmarad az az oroszlán.”*

„Szitáljuk át a sivatagot egy elegendően nagy és megfelelő lyukméretű szitán. Ami kihullik az a homok, ami fennmarad az az oroszlán."

Az eljárás gyakorlati kivitelezhetetlenségének első racionális gondolata után, a még oly absztrakt gondolkodású olvasóban is felvetődik, hogy az algoritmus nem igazán hatékony, de mégis elgondolkodtató. Hiszen sok milliárd homokszem megmozgatását igényli, egyetlen oroszlán miatt. A modell analógia világossá válik, ha az oroszlán a terroristákat (bűnözőket), a homokszemek pedig a sok-sok békésen, becsületesen élő embertársunkat reprezentálják. Vagyis, ha a modell arányokra vonatkozó aspektusát tekintjük, akkor a NAGY TESTVÉR típusú anti-bűnmegelőzési filozófia így foglalható össze: ***„Tekintsd a 99.9% becsületes embert bűnözőnek, hogy a 0.1% bűnözőt megpróbáld kiszűrni!"***[70]

Eme filozófia költség és hatékonyság viszonyát, valamint emberi személyiségjogainkra és polgári szabadságjogainkra mért megalázó csapását, igyekeztem vázlatosan bemutatni. Meggyőződésem, hogy maga G. Orwell örülne a legkevésbé annak, hogy 60 év után társadalmunkban ***az újbeszél szelleme kísért.***

A biztonság konvergencia-programja című cikkemben megmutattam, hogy lehetséges alternatív filozófia, melynek lényege a *Találd ki!* filozófia *Találd meg!* filozófiára cserélése. Eszerint az egész ECHELON rendszer a *Találd ki!* kriptográfiai filozófiára épül, azaz alapvetően feltételezi, hogy a kommunikációs csatornákon a nyílt, vagy rejtjelzett üzenetek „közlekednek". Így a jól alkalmazott *Találd meg!*, azaz a digitális sztegonográfiai módszerek ellen szinte teljesen védtelen.

Az ECHELON rendszer mentségére szolgál, ugyanakkor a mögötte álló anti-bűnmegelőzési filozófia rendkívüli gyengeségét mutatja, hogy egy olyan „ellenőrző" (lehallgató) rendszer létesítése reménytelen, amely a kommunikációs forgalom minden (szöveg, kép, hang) üzenetét „fedő üzenetnek" tekinti. Egy ilyen elemző rendszerhez ugyanis nem csak a jelenlegi kapacitások nem elegendőek, de elméletileg sem megvalósítható, vagy ha mégis, akkor az az egész e-kommunikációs rendszer bénulásához vezetne.

---

[70] A kriptológiában (titkosítás tudomány) az ilyen típusú eljárásokat „brute force", azaz „nyers erő", vagy „teljes kipróbálás" névvel illetik. Bár gyakorlati felhasználása a mai kriptográfiai eljárások esetén (szakmai körökben köztudomásúan) értelmetlen, mégis előszeretettel alkalmazzák ezen eljárások biztonságának demonstrálására. Így lehet a laikus közfelfogásban hamis biztonságérzetet kelteni az exponenciális robbanás segítségével. Mintha a 32 betűn alapuló magyar nyelv változatosságát azzal bizonyítanánk, hogy például a lehetséges 5 betűs szavak száma matematikailag 32^5=33.554.432, ami óriási szám, azonban tudjuk, hogy ezek legnagyobb része teljesen értelmetlen betűkombináció (pl.: aaaaa, bbbbb, …, aabbb, ababa, …)!

Vagyis a modern, digitális sztegonográfia olyan titkosítási módszercsalád és eszközrendszer, amely rossz kezekbe kerülve valódi *„csodafegyver”*, míg jó kezekben „csoda”, azaz új lehetőség egy emberközpontú, biztonságos információ alapú INFOSANCE[11] társadalom létrehozására. Talán ez lehet az igazi tanulsága szeptember 11-énekk, amely nem csupán szimbolikusan dupla felkiáltójel a jövő terrorizmus elleni küzdelméhez!

Mégis minden jel szerint, napjainkban a tőke globális hatalma a GLOBÁLIS NAGY TESTVÉR e-társadalmának kialakításában érdekelt. Így azok számára akik a sivatag homokszemeinek, a 99.9%-nak valódi biztonságát szeretnék az emberiség perspektívájaként elérni, továbbra is az a hivatásunk, hogy felhívjuk a 99.9% figyelmét valódi helyzetükre. Vagyis, hogy *valósággá vált N. Wiener előzőkben idézett aggodalma és napjaink információsnak nevezett e-társadalmában az információ árucikké vált és bekövetkezett az információ teljes félrekezelése!*

10.11. NAGY TESTVÉR a 21. században, avagy a biztonság „visszalő”

Az eddigiekben végigkövettük G. Orwell 60 éve megszületett irodalmi utópiájának megelevenedését, és az ördögi gondolatot messze túlszárnyaló megvalósulását. Az 50 évig szigorú titokban fejlesztett ECHELON rendszer ímmár 10 éve a nyilvánosság számára is létezik és egyre nyilvánvalóbb, hogy a NAGY TESTVÉR (ma már a globalizálódott hatalom) SZEMMEL TART!

Az érett középkorában lévő NAGY TESTVÉR nem fárad, sőt egyre aktívabban terebélyesedik és hoz létre olyan utódokat, amelyekről G. Orwell nem is álmodhatott. A STOA jelentésekből kiderül, hogy a Föld feletti (kém)műholdak az évtizedek során kiegészültek a tengermélyi optikai kábel megcsapoló hüvelyekkel, majd az Internet világméretű elterjedésével „húsevőként” fészkelte be magát. Mindezt a ***„terrorizmus elleni védekezés”***, azaz a ***„biztonságunk megteremtése”*** jelszavak hangos ismételgetése közepette használja fel a számunkra megfoghatatlan hatalom arra, hogy dollár százmilliárdokat vegyen ki az adózók zsebéből.

Mindezek ellenére, 2001. szeptember 11-én a Földünket körülvevő titkos információpajzs, akárcsak a természetes védelmet nyújtó ózonpajzs, kilyukadt! Az ECHELON szimbolikus jelentései (harcvonal, harcrend) valóságossá váltak és a sok milliárd dolláros titkos befektetés, valamint ***a globalizálódott anti-bűnmegelőzési filozófia nyilvánvaló kudarcot szenvedett***. A szeptember 11-i események dupla felkiáltójellel vetették fel a globális e-kommunikáció, a globális e-társadalom kockázatának kérdését, melynek lényege a NYÍLT GLOBALIZÁCIÓ ELLEN, REJTETT HÁBORÚ paradoxonban foglalható össze.

A történelem dupla felkiáltójellel hívta fel mindannyiunk figyelmét arra, hogy a titokról, a globális e-kommunikációról, az e-világ biztonságáról alkotott addig „egyértelmű" képet kényszerül az emberiség „átfesteni”.

Ha a 20. század utolsó évtizedeire az *információrobbanás* volt jellemző, akkor a 21. század első évtizedét nevezhetjük az *„információs láncreakció”*évtizedének. Az egyének, a legkülönbözőbb társadalmi csoportok, szervezetek egyre több szálon kötődnek eme globális (idő és térbeli korlátokat átívelő) e-rendszerekhez, így kialakult az információ-függőség, hasonlóan a civilizált társadalmakban már létező „elektromosság-függőséghez”. Azonban, míg az elektromosság fizikai létünket határozza meg alapvetően, addig az információ teljes

személyiségünk, pszichikai, egzisztenciális létünk „digitális leképezésére képes", amelynek birtoklása soha nem látott hatalomkoncentrációt eredményez.

2001. szeptember 11. után a számítógépes megfigyelőrendszerekkel kapcsolatos hozzáállás alapvetően megváltozott: jelentősen felértékelődött például a New Jersey-i Visionics szoftvercég korábban sokat bírált arcfelismerő rendszere, a FaceIt, amelyet a 2002-es Super Bowl-döntőn teszteltek először nyilvánosan. Akkor a kamerák több apróbb bűncselekményért keresett személyt szúrtak ki a tömegben, de letartóztatás nem történt. Később a floridai Tampa városának szórakozónegyedét pásztázó biztonsági kamerákat kötötték össze a rendszerrel, amelyet itt vetettek be először közterületen. Az ACLU állásfoglalása szerint a rendszer súlyosan sérti a polgárok szabadságjogait, azóta viszont a szövetségi légügyi hatóság érdeklődését is felkeltette és terveik szerint az összes amerikai repülőtéren bevezetik, csakúgy, mint a kaliforniai Identix ujjlenyomat- felismerő rendszerét. Ugyanígy az USA a világ többi országára is nyomást gyakorol a biometrikus adatokat tartalmazó útlevél bevezetése érdekében.

A GLOBÁLIS NAGY TESTVÉR mindenkit figyelő anti-bűnmegelőzési filozófiájának eredménye tehát egyáltalán nem elhanyagolható: 2001. szeptember 11., Londonban, Madridban és a világ számtalan pontján napjainkban is felbukkanó merénylők, akiknek tevékenysége „fillérekből" fityiszt mutat a NAGY TESTVÉRNEK, és végül de mindenek előtt a mindennapi rettegésben élő, a biztonságérzet helyett sivatagi homokszemekként kezelt emberek milliárdjai! És még nincs vége …

A *„biztonságunk védelme érdekében"* Földünk felett, óceánok mélyén, a kommunikációs hálózatokba bújva vigyázó GLOBÁLIS NAGY TESTVÉR tovább növesztette hétköznapi életünket átölelő csápjait: érzékelők, térfigyelő kamerák és műholdas nyomkövetők (GPS), biometrikus azonosítók a dokumentumainkon és természetesen a hatalom által tárolt adatbázisokban. És íme a 21. század első évtizedének legújabb biztonságtechnikai csápja, amely már szinte a bőrünk alá is beereszti tapadókorongját: a ***rádiófrekvenciás azonosítás (Radio Frequency Identification = RFID)***

10.12. A GLOBÁLIS NAGY TESTVÉR „beporozza a világot"

G. Orwell 60 évvel ezelőtti utópisztikus világát messze megelőzi napjaink és a belátható jövő adattárolási és továbbítási eszközrendszere. Az RFID technológia ma már porszem nagyságú, viszonylag olcsó chipjeinek csak az alkalmazók fantáziája szab határt. Tömeges megjelenésük egészen új távlatokat nyithat a szállítás, gyártásoptimalizálás, kereskedelem, termék vagy akár a felhasználó ember azonosítása területén. Új korszak kezdődhet tehát, amelyben a GLOBÁLIS NAGY TESTVÉR már nem távolról figyel, hanem porszemnyi RFID chipjeivel „beporozza a világot".

Mi az RFID?

Leegyszerűsítve, az RFID felfogható interaktív vonalkódként. Azaz automatikus azonosításhoz és adatközléshez használt technológia, melynek *lényege adatok tárolása és továbbítása RFID címkék és eszközök segítségével*. Három alapelemből áll: az azonosítandó dologra ráhelyezett *aprócska címkéből* (angolul *tag*), az ezen elhelyezett *információból*, valamint a *leolvasó mechanizmusból*, amely mindezt értelmezi, listázza vagy rögzíti. A

rádiófrekvenciától és az antenna méretétől függően a címke és a leolvasó közti távolság 10 centimétertől pár méterig változhat, de egyes különleges típusok akár 50-100 méter távolságból is olvashatóak.

Az RFID tehát tárgyak, vagy élőlények azonosítóját továbbítja vezeték nélkül, rádióhullámok segítségével egy leolvasóhoz. A vonalkódhoz képest hatalmas előnye, hogy használatához a legtöbb esetben emberi beavatkozás sem szükséges. Az adatok könnyen, gyorsan és teljesen automatikusan jutnak el a feldolgozó számítógépre, illetve manapság egyre inkább az Internetre.

A gyakorlatban az RFID-chipek három típusát (passzív, félpasszív, aktív) különböztethetjük meg. A legfontosabb különbség az áramfelvételükben mutatkozik, hiszen a passzív chipek nem tartalmaznak áramforrást.

Itt a chip köré épített áramkör a bejövő rádióhullámokból indukál áramot, így gyakorlatilag a leolvasó hozza működésbe az eszközt és a benne lévő adatokat az egyben antennaként is funkcionáló áramkörön keresztül sugározza vissza a leolvasó egységnek. A megoldás hátránya, hogy a rádióhullámok által keltett alacsony feszültségen korlátozott mennyiségű adat továbbítható, ugyanakkor az elhelyezése egyszerű, előállítása pedig olcsó.

Az *aktív transzponderek* olvasási távolsága 100 méter körüli, legtöbbször saját áramforrással és saját adóval rendelkeznek.

RFID történelem

Az a különleges szerencse, hogy a NAGY TESTVÉR születésének helye és ideje egyértelműen meghatározható, az RFID esetében nem áll fenn. Azonban mégis szerencsésnek mondható, hogy az RFID eredetének történeti forrásai két különleges személyiséghez vezetnek el. Mivel az RFID mindennapjaink és várhatóan közeli jövőnk meghatározó technológiája, amelynek jelentősége talán a mobiltelefonéhoz mérhető, e két történet külön figyelmet érdemel.

A két történelmi szál külön érdekessége, hogy gyökereik jóval a NAGY TESTVÉR megszületése előtti időkre nyúlnak vissza és két egészen különböző tudományos, illetve technikai alapgondolat vezetett a közel azonos eredményhez. Az egyik szál a Szovjetúnió 1920-as éveiből, míg a másik a II. világháború Egyesült Királyságából ered.

10.13. Leon Theremin alias Lev Szergejevics Tyermen[71] (1896-1993)

Leon Theremin alias
Lev Szergejevics Tyermen
(1896-1993)
röviddel halála előtt

Az orosz tudós 1920-ban találta fel a róla elnevezett *teremin*-t, a világ első térvezérlésű elektronikus hangszerét. Az akkor újonnan felfedezett elektroncsövekkel oszcillátorokat épített, ezek állították elő a hangszer hangját. A hang erejét és magasságát az oszcillátorokat tápláló elektromos áram feszültségének változtatásával kontrollálta. A feszültség változtatását nem gombok, vagy kapcsolók segítségével oldotta meg, hanem a hangszer körül kialakuló elektromágneses erőtér manipulációjával. Így hát a teremin-t nem kellett megérinteni ahhoz, hogy megszólaljon.

A készülék dobozából két antenna állt ki, amelyek erőterében a játékos kezei mozgatásával (közelítve, vagy távolítva kezeit) szabályozta a hang erejét és magasságát. Az eredeti teremin hangja az emberi énekhang és a vonóval játszott fűrész hangjának ötvözete. Leon Theremin 1921-ben, a Moszkvában megrendezett Nyolcadik Összoroszországi Mérnök Kongresszuson mutatta be először találmányát a nagyközönségnek. A tudós nemcsak fizikus, de képzett csellóművész is volt. A kongresszuson jelen volt Lenin is, aki nagy tetszéssel fogadta Theremin professzor bemutatóját.

Leon Theremin saját készítésű tereminen játszik

A teremin hangszer elméleti alapjait és műszaki megvalósítását felhasználva, a professzor mozgásérzékelőket, lehallgató berendezéseket, távközlési eszközöket fejlesztett ki. Találmányainak prototípusait, tervrajzait az orosz, később szovjet, majd újra orosz titkosszolgálat a legutóbbi évekig rejtegette a nyilvánosság elől. A professzor az 1920-as évek elején az orosz titkosszolgálat alkalmazásába lépett, majd 1927-ben titkosszolgálati hatásra, nevét Lev Szergejevics Tyermenről, Leon Thereminre változtatta.

Theremin hangszerének híre eljutott az Amerikai Egyesült Államokba, ahova meghívást kapott. Nagysikerű koncert turnéján az amerikai arisztokrácia kedvence lett, az akkori politikai és művészvilág jeles képviselői fogadták barátságukba (Albert Einstein, Arturo Toscaníni, Charlie Chaplin, Leopold Stockowski és a később amerikai elnökké választott Dwight Eisenhower). Kalandos amerikai tartózkodásából visszatérve, 13 évet töltött a tudósok fogvatartására létesített szibériai fogolytáborban, amelyet Szolzsenyicin írásaiból ismerhetünk. A fogvatartott tudósok titkos katonai célokra és kémkedéshez szükséges készülékek kifejlesztésén dolgoztak.

[71] Lev Szergejevics Tyermen (1896-1993) munkásságának és a teremin hangszernek, illetve az ebből kifejlesztett szintetizátornak rajongója és kitartó kutatója Najmányi László, akinek munkáiból részletesen tájékozódhat az olvasó mindezekről a témákról (lásd [NAJMÁNYI 2006]).

Theremin feladata lehallgató-berendezések, távirányítók és robot-repülőgépek tervezése és építése volt. Legközelebbi munkatársa a repülőgéptervező Tupoljev lett, akivel több, mint egy évtizedig dolgoztak ugyanabban a munkabrigádban. Leninnel ellentétben Sztálin nem rajongott a teremin hangszerért, annál inkább örömét lelte munkatársai beszélgetéseinek lehallgatásában, így megbízták Theremint, hogy telepítsen lehallgató-berendezéseket Sztálin Kreml-beli lakásába. A 6 méter vastag betonfalon is áthatoló, Burán nevű lehallgatóberendezés kifejlesztéséért 1950-ben kegyelmet és Sztálin díjat kapott.
Az 1970-es években a The New York Times Moszkvába akkreditált újságírója, a konzervatórium folyosóján sétálva felfedezte Professzor Theremin névtábláját az akusztika tanszék ajtaján. Interjút készített a régen halottnak hitt tudóssal. Theremin nem beszélt hosszú évekig tartó fogvatartásáról, csak legújabb találmányait ismertette lelkesen, majd az interjú megjelent az amerikai újságban. Másnap eltávolították a konzervatóriumból, tervrajzait, számításait, alkatrészeit, szerszámait elkobozták, találmányait pedig a titkosrendőrség emberei megsemmisítették. A tudós a következő húsz évet egy másfél szobás, moszkvai panel-lakásban, háziőrizetben töltötte. Annak ellenére, hogy tiltották a kísérletezéstől, régi rádiókészülékekből és a lakótelep környékén található lomokból újabb teremineket épített, közöttük olyanokat is, amelyeken a szemek mozgatásával lehetett játszani.

Az 1946-ban elkészített *The Thing* fantázianevű készüléke, amellyel a Szovjetúnióban állomásozó amerikai nagykövetet hallgatták le, a passzív elektromágneses indukció elvét alkalmazta. Csak akkor lépett működésbe, ha 330 Hz-es mikrohullámokkal bombázták, emellett nemcsak apró volt, hanem áram sem kellett hozzá és készenléti állapotában jelet sem sugárzott. Joggal mondhatjuk tehát, hogy az RFID első ősének tekinthető eszközt Leon Theremin orosz fizikus és feltaláló alkotta meg.

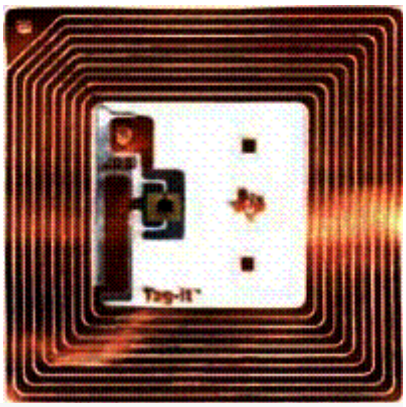
10.14. Sir Robert Alexander Watson-Watt (1892-1973)

Sir Robert Alexander Watson-Watt (1892-1973)

Skót fizikus, fiatal meteorológusként rövidhullámú rádióvevőket alkalmazott a villámlások helyének meghatározására. 1935-ben felfedezte a RADAR-t (RAdio Detection And Ranging). A felfedezés forradalmasította a repülést, azonban felmerült a repülőgépek megkülönböztethetőségének problémája. Amely jelentős nehézséget okozott a katonai repülésnél, mivel nem lehetett megkülönböztetni a saját, illetve ellenséges repülőgépeket.

A II. világháború idején R.A. Watson-Watt vezetésével egy titkos projekt keretében a britek kifejlesztették az első aktív barát-ellenség repülőgép felismerő rendszert (IFF = Identify Friend or Foe). Egy adót helyeztek el minden brit repülőgépre. Amikor ez jeleket vett a földi radarállomástól, speciális egyedi módon kódolt (titkosított) jeleket kezdett sugározni, amit a földi állomás érzékelt és azonosította a repülőgépet. Mivel az **RFID** ugyanezen az elven működik, ezt a módszert is nevezhetjük az aktív RFID rendszer ősének.

10.15. RFID az 1960-as évektől napjainkig



RFID-chip (lapka)

A hatvanas években jelentek meg az első kereskedelmi alkalmazások, amelyek főképp a bolti lopások megakadályozására szolgáltak. A kezdetleges megoldások 1 bites technológiával dolgoztak, ezért elég korlátozott lehetőséget biztosítottak a bevezető cégeknek, de akkor mégis csúcstechnológiának számított bevezetésük.

A 70-es években azonban már komoly fejlesztések folytak, mind Amerikában, mind Európában. Ekkoriban elsősorban mezőgazdasági, állattenyésztési célokra, állatok nyomon követésére készültek alkalmazások. Az első valódi RFID szabadalmat 1973-ban jegyezték be az Egyesült Államokban, *passzív transzponder*néven, s ajtózárakhoz használták a kulcs kiváltására.

Vajon, ha az RFID módszer több mint 60 éve ismert, alkalmazási lehetőségei szinte korlátlanok, miért váratott magára a tömeges alkalmazás a 21. századig?

A választ a tudomány és technikatörténetben oly gyakran előforduló jelenség adja, mely szerint az igazán nagy gondolatok (tudományos eredmények) megelőzik saját korukat, így be kell várni azokat a technikai feltételeket, amelyek alkalmasak a műszaki megvalósításra. Így járt C. Babbage a programvezérelt számítógép megalkotásával[13], mivel csak halála után 11 évvel, 1882-ben állította üzembe Edison a világ első villanytelepét. Vagy Gábor Dénes, aki 1947-ben írta le a holográfia elméletét, azonban koherens fényhullámok híján 13 évet kellett várni az első hologram elkészítéséig, amikor 1960-ban az első lézert az amerikai Theodore H. Maiman kifejlesztette.

Hasonló okoknak tulajdonítható, hogy az RFID-technológia csak az elmúlt években tett szert nagyobb közérdeklődésre, mivel a gyártási módszerek fejlődésével lehetővé vált a miniatűr szerkezet viszonylag alacsony áron való előállítása, illetve az adattárolási lehetőségek megnövekedésével igény támadt a vonalkódokon túl mutató megoldások bevezetésére egyes területeken. Az RFID komoly előnye a nyomon követhetőség mellett, az újraírható adattárolás lehetősége.

A mai eszközök már elég komoly adatmennyiséget képesek tárolni és a jelentősen megnövelt hatótávolság sem jelent problémát. A technológia előnyei miatt a vonalkód leváltását eredményezheti, viszont a passzív rendszerek teljes leváltásáig még számos akadálynak el kell hárulnia.

10.16. Néhány lehetséges RFID alkalmazás

A rádiófrekvenciás azonosító technológia felhasználási lehetőségei szinte végtelenek.[72] A logisztikától a kereskedelemig, az egészségügytől a határőrizetig, az oktatástól a biztonsági és nyilvántartási feladatokig, mind több területen jelennek meg RFID megoldások. Egyértelmű, hogy a chip-gyártási költségek csökkenésével, az egyre olcsóbban előállítható lapkák bizonyos területeken akár az általánosan elterjedt vonalkódokat is kiszoríthatják.

Az RFID technológia a korszerű helymeghatározó rendszerekkel (GPS) kombinálva lehetővé teszi a közúti, légi és vízi szállítás teljes nyomon követését, optimalizálását. Bizonyos országok értékes termékeiket, gyártmányaikat ilyen módon védik meg a veszélyektől. A postai gyorsszolgálatok nagy része a technológia előnyeinek köszönhetően percre pontosan tudja, hogy éppen merre jár a kézbesítendő küldeményünk.

Az RFID vállalati környezetekben a készletnyilvántartási rendszerek, intelligens vállalatirányítási rendszerek és a folyamatoptimalizáló rendszerek hatékony támogatása miatt is egyre népszerűbbek.

Kísérletek folynak az automatizált üzletek kialakítására, illetve számos helyen bevezették már a RFID alapú autópálya fizetési megoldásokat világszerte.

Moszkvában, Delhiben, Hong Kongban, New Yorkban és a világ legnagyobb városaiban már általánosan bevett gyakorlat az intelligens tömegközlekedési igazolványok - bérletek, jegyek - alkalmazása. Sőt a nagyobb hitelkártya kibocsátók is megjelentek általánosan elfogadható micro-payment megoldásaikkal, amelyek főképp az aprópénz használat kiváltásra született elektronikus fizetési lehetőséget biztosítanak felhasználóiknak.

Az autóipar is felismerte, hogy az RFID új lehetőségeket teremthet a biztonsági megoldások területén, így manapság már legtöbb indításgátló és elektronikus kulcs már ezzel a technológiával dolgozik.

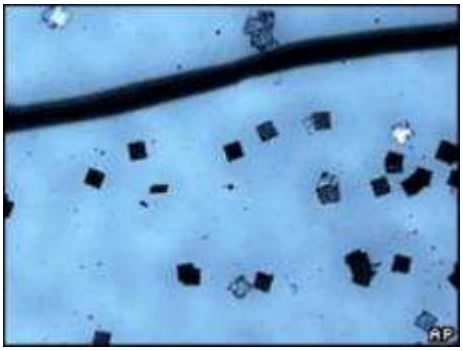
10.17. Porszem nagyságú RFID chipek

Az RFID technológia tömeges elterjedésének kezdetét, valóságos infrastrukturális robbanást jelent a Hitachi cég 2007. évi bejelentése, mely szerint kifejlesztett egy Mu-chipnek nevezett RFID-lapkát, amely 0,4x0,4 milliméter nagyságú. A porszem méretű aprócska jeladók elég vékonyak ahhoz, hogy akár egy papírlapba is beültethetőek legyenek, hátrányuk csupán az, hogy működésükhöz külső antennára van szükség. Egyelőre azonban még a legkisebb antenna is mintegy nyolcvanszor akkora, mint az egyes jeladók.

A személyiségi jogok védelmezői már többször szót emeltek az RFID-jeladók ellen, mondván, ezek segítségével könnyedén megfigyelhetővé válnak az állampolgárok, ráadásul a tudtuk és beleegyezésük nélkül.

---

[72] Bencsik Anikó szakdolgozatában kitűnően foglalta össze napjaink RFID technológiáit és azok alkalmazásait. (lásd [BENCSIK 2007])



RFID lapkák egy emberi hajszál mellett

10.18. RFID a NAGY TESTVÉR szolgálatában

Az azonosítási és biztonsági lehetőségeit egyre inkább kihasználják a modern útlevelek, a digitális azonosítók és a legújabb fizetési megoldások.

RFID útlevéllel elsőként 1998-ban Malajzia látta el állampolgárait, s azóta a legtöbb európai ország, az USA, Japán, Ausztrália és Korea is kibocsátotta saját digitális adatokat is tartalmazó útlevelét. Noha hatalmas vita folyik az elektronikus útlevél biztonságáról, mégis általános tendenciának látszik a terjedése.

A hétköznapokba is bevonuló megoldások legtöbbje utópisztikusnak hangzik, s némelyek még vitatottak is, de egyértelmű hogy az RFID terjedése megállíthatatlan. Pár ezer forintért már itthon is négylábú kedvenceink bőre alá rejthetjük a chipet rejtő kis kapszulát, sőt elég horrorisztikus megoldásként az egyik kutató saját kezébe építette a bejárati ajtajának elektronikus kulcsát is.

Egyesek szerint nincs messze az az idő, amikor a termékek vásárlóit egyértelműen profilozzák majd a digitális címkék, hiszen a vásárlók vásárlási szokásait így össze lehet kötni lakhelyükkel, foglalkozásukkal, hobbijukkal, korukkal is. Az aktív címkék alkalmazása főképp itt kerül a viták kereszttüzébe, hiszen a különböző hivatalok már így is túl sokat tudnak rólunk. Az RFID technológia általános használatához mindenképpen szükség van a technológia használati, adatvédelmi és jogi szabályainak szigorú szabályozására.

A Washingtoni Egyetem kampuszán ötven önkéntessel szimuláltak egy olyan jövőbeli világot, ahol minden embert másodpercre és centiméterre pontosan le lehet követni: a főnök pontosan, kamerák nélkül is láthatja, hogy alkalmazottjai mikor álltak fel az asztaltól és mikor tértek oda vissza, hova mentek vagy éppenséggel kivel találkoztak. A rendszer lelkét az RFID *rádiófrekvenciás azonosító* adja, amely már egy ideje megtalálható amerikai útlevelekben, jogosítványokban, illetve egyes ruhákban, kocsikulcsokban vagy fizetésre használt kártyákban is.
Az egyetemi rendszeren az önkéntesek figyelemmel követhetik, hogy ki és mikor nézte meg az általuk kibocsátott adatokat, valamint módosítható is - így megszabható az is, hogy két fél csak akkor lássa egymást, ha például 10 méter távolságban vannak csak egymástól. Az ötlet könnyen továbbgörgethető egészen a közösségi oldalakig is: a fejlesztők RFIDDER nevű szoftvere folyamatosan informálja az általuk használt közösségi hálót, hogy éppen hol vannak

és mit csinálnak: ez weben és mobilkészüléken is használható, valamint hozzáköthető a közösségi oldalakhoz is.
Az RFID használata komolyabb biztonsági és adatvédelmi problémákat is felvet. Ugyanis például az amerikai útlevelek vagy jogosítványok úgy lettek kialakítva, hogy több információt tartalmaznak, mint amire szükség lenne. A dél-kínai Senzsenben pedig a kormány RFID-olvasókat telepít, hogy pontosan lekövethesse a városlakók hollétét, mindezt pedig amerikai technológiával, írja a New York Times. A kínai személyazonosító kártyákban emellett az alapinformációkon kívül az illető teljes munkavállalói története, előző tanulmányai, vallása, priusza vagy jogi ballépései és családtagjaival kapcsolatos adatok is olvashatóak.

Nem elhanyagolható biztonsági probléma, hogy bár az RFID chip passzív, azaz csak akkor olvasható, amikor egy olvasóberendezés olvasási kérelmet indít felé, egy erős elemmel rendelkező berendezés akár 10 méterről is képes leolvasni a lapkát. Éppen az ilyen illetéktelen leolvasások (támadások) kivédése miatt látták el az IFF repülőgép felismerő rendszereket igen komoly kriptográfiai védelemmel, ami pillanatnyilag a tömegesen használt RFID chipekből hiányzik, így a lapkákat könnyen lehet klónozni, ami beláthatatlan biztonsági rést nyit az alkalmazásokon.

Félelmetes elgondolni, hogy a kellő biztonsági óvintézkedések hiányában az RFID címkékből kinyert adatokból teljes profilt lehet összeállítani bárkiről anélkül, hogy az tudna róla, vagyis *„Egy teljes portrét lehet úgy festeni valakiről, hogy az tudatában lenne, hogy végig modellt állt valakinek.”*
A jövőben tehát elegendő bevásárlóközpontok vagy repülőterek környezetében RFID leolvasókat telepíteni, majd a telepítést végző szervek[73] (az ECHELONnal ellentétben, egyre kisebb befektetéssel telepíthető RFID rendszerek tulajdonosai!) az utazási mintákból, a vásárlási szokásokból, egészségügyi, oktatási és munkaügyi alkalmazásokból, bankkártya- vagy bármely más felmerülő adatból igen pontos profilt készíthetnek bárkiről.

Ez maga a 21. századi GLOBÁLIS NAGY TESTVÉR !!!
… de kié lesz a GLOBÁLIS TITOK ???

[73] A „szervek” most már a GLOBÁLIS NAGY TESTVÉR-t szolgálhatják ki úgy, hogy az ECHELON-nal ellentétben, az RFID rendszerek napról-napra egyre kisebb befektetéssel telepíthetők! Ezekben az esetekben tehát nincs szükség a „terrorizmus elleni küzdelem” zászlaját lobogtatva, százmilliárd dolláros költségvetési támogatásra. Sőt az igazán hasznos polgári alkalmazások álcájával, magántőkével is kényelmesen létrehozható RFID rendszerek így észrevétlenül válhatnak a 21. század globális információs „csodafegyvereivé”! Ez az érvelés („hasznos polgári alkalmazások”) egyrészről indokolttá teszi az EU-ban is folyamatban lévő szabványosítási törekvéseket, amelyek ugrásszerűen megnövelik a tömeges nemzetközi elterjesztés lehetőségét, hiszen a termékek ára rohamosan csökken a lapkák és olvasó berendezések tömegtermelése miatt.

10.19. ZÁRSZÓ, ami nem mondható el *újbeszélül*

***Fel kell nyitni az emberiség szemét (és agyát)**, hogy ma már Orwell képzeletét jóval túlszárnyalta a valóság. Ma már, ha az információk tömegét birtoklók akarják, akkor sötétben is mindent lát és hall a GLOBÁLIS NAGY TESTVÉR!*

Fel kell nyitni az emberiség, a 99.9% szemét (és agyát), és rá kell mutatnunk arra a különös összefüggésre, miszerint az ECHELON rendszer százmilliárd dollárokat felemésztő költségvetésének legfőbb indoklása a ***terrorizmus elleni küzdelem (védekezés)***, vagyis az ózonpajzs mintájára, egy *„Földünket körülvevő információ pajzs”*, mégis máig megmagyarázatlan tény a 2001.szeptember 11-i terrortámadás és a nap mint nap, a Föld különböző pontjain felbukkanó terrortámadások réme!

Fel kell nyitni az emberiség, a 99.9% szemét (és agyát), és tényekre alapozva bemutatni, hogy milyen is ez a nem utópisztikus, hanem mára véres valósággá vált GLOBÁLIS NAGY TESTVÉR kora, a Földet behálózó és ma már a civil lakosságra és szervezetekre is kiterjedő lehallgatások és az erre elköltött hatalmas összegek mellett mégis „virágzó” terrorizmus korszaka!

Fel kell nyitni az emberiség, a 99.9% szemét (és agyát), hogy a 0.1% GLOBÁLIS NAGY TESTVÉRE ellen folyik a 99.9%-ot rettegésben tartó REJTETT HÁBORÚ!

Még elszomorítóbb és egyben megdöbbentő G. Orwell 60 évvel ezelőtti gondolatainak aktualitása. Talán éppen az alábbi idézet széleskörű elterjesztése akadályozhatná meg, hogy az ebben megfogalmazott látnoki gondolatok ne legyenek aktuálisak 2050-ben!

„Vegyük például a Függetlenségi Nyilatkozat jól ismert részletét:

Magától értetődőnek tartjuk ezeket az igazságokat: hogy minden ember egyenlőnek teremtetett, hogy teremtője olyan elidegeníthetetlen jogokkal ruházta fel az embert, amelyekről le nem mondhat, s ezek közé tartozik a jog az élethez és a szabadsághoz, valamint a jog a boldogságra való törekvéshez. Ezeknek a jogoknak a biztosítására az emberek kormányzatokat létesítenek, amelyeknek törvényes hatalma a kormányozottak beleegyezésén nyugszik. Ha bármikor, bármely kormányforma alkalmatlanná válik e célok megvalósítására, a nép joga, hogy az ilyen kormányzatot megváltoztassa vagy eltörölje, és új kormányzatot létesítsen...

Ezt teljes egészében lehetetlen úgy visszaadni újbeszélül, hogy az eredeti értelme megmaradjon. A legtöbb, amit tenni lehet vele, az, hogy az egész szöveget egyetlen szóban, a bűngondol-ban összegezzük. Teljes átültetése csakis ideológiai átültetés lehetne, ezáltal viszont Jefferson szavai az abszolutisztikus kormányzat dicshimnuszává változnának.

A múlt irodalmának nagy részét már át is alakították ilyen módon. Presztízsszempontok kívánatossá tették bizonyos történelmi személyek emlékének megőrzését úgy, hogy tetteiket egyidejűleg kapcsolatba hozzák az Angszoc filozófiájával. Több író, mint például Shakespeare, Milton, Swift, Byron, Dickens és mások műveinek átültetése folyamatban van; ha a feladatot megoldották, az eredeti műveket, minden egyéb művel együtt, amely a múlt irodalmából fennmaradt, el fogják pusztítani. Az átültetés lassú és nehéz munka, s befejezését legkorábban a huszonegyedik század első vagy második évtizedére várják. Nagy mennyiségű,

pusztán hasznossági célokat szolgáló mű is van - nélkülözhetetlen technikai kézikönyvek és hasonlók -, amelyeket ugyanilyen kezelésnek kell alávetni. Elsősorban azért is tűzték ki az újbeszél végleges bevezetésének határidejét oly későre - 2050-re -, hogy időt hagyjanak az átültetés munkájának elvégzésére." ([ORWELL 1989] 340-342.old.)

MELLÉKLETEK a 10. fejezethez

1. Nicky Hager

Nicky Hager (1958-) író és oknyomozó újságíró, Újzélandon Levinben született, jelenleg Wellingtonban él.

Hager írásaiban főleg a hírszerzőhálózatok környezeti és politikai kérdéseivel foglalkozik, a fizika és filozófia doktora. Új-Zéland vezető oknyomozó újságírójaként tartják számon.

Nicky Hager, 2008. júliusában

Nicky Hager 2001. áprilisában beszélt az Európa Parlament Echelon Bizottságában. Éppen öt hónappal a szeptember 11-i terrortámadás előtt, igyekezett a Bizottság figyelmét felhívni „a terrorizmus elleni küzdelem" zászlaja alatt működő Echelon rendszer diszfunkcionális működtetésére. Ami öt hónappal később tragikusan bebizonyosodott!

Főbb munkái

- *Secret Power, New Zealand's Role in the International Spy Network*; Craig Potton Publishing, Nelson, NZ; ISBN 0-908802-35-8; 1996
- *Secrets and Lies: The Anatomy of an Anti-Environmental PR Campaign* (with Bob Burton); Craig Potton Publishing, Nelson, NZ; ISBN 0-908802-57-9; 1999
- *Seeds of Distrust: The Story of a GE Cover-up*; Craig Potton Publishing, Nelson, NZ; ISBN 0-908802-92-7; 2002
- *The Hollow Men: A study in the politics of deception*; Craig Potton Publishing, Nelson, NZ; ISBN 1-877333-62-X; 2006

2. Duncan Campbell

Duncan Campbell angol oknyomozó újságíró és televíziós producer, aki hírszerzési kérdésekre specializálódott. 1987-ben elkészítette *Secret Society* (Titkos Társadalom) című dokumentum sorozatát a BBC-nek, amely a kormány részéről igen ellentmondásos fogadtatásban részesült. A sorozat ugyanis egy *Zircon* kódnevű titkos kémműhold projectről szólt.
1978-91 között állandó szerzője és helyettes szerkesztője volt a *New Statesman* folyóiratnak.

Főbb munkái

1. **Campbell, Duncan** (1988-08-12), "Somebody's Listening", *New Statesman*, http://duncan.gn.apc.org/echelon-dc.htm, retrieved 2007-06-19
2. **Campbell, Duncan** (1999-04), *Interception Capabilities 2000*, European Parliament, Directorate General for Research, Directorate A, The STOA Programme, http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm, retrieved 2007-06-19
3. **Campbell, Duncan** (2005-07-01), "Operation Ore Exposed", *PC Pro*, http://www.pcpro.co.uk/features/74690/operation-ore-exposed/page3.html, retrieved 2007-06-19
4. **Campbell, Duncan** (2007-04-01), "Sex, Lies and the Missing Videotape", *PC Pro*, http://ore-exposed.obu-investigators.com/PC%20Pro%20article%20June%202007%20.pdf, retrieved 2007-06-19

3. Jeffrey Richelson

Jeffrey Talbot Richelson (1949-) amerikai író és tudományos kutató, a hírszerzés és a nemzetbiztonság területével foglalkozik. Richelson 1975-ben a University of Rochester-en szerezte a politikatudományok doktori címét, majd a University of Texas (Austin) és az American University egyetemeken tanított. Jelenleg a National Security Archive vezető munkatársa.
Tíz könyv és számos cikk szerzője, amelyek közül több a National Security Archive forrásdokumentuma.

Könyvei

- *A century of spies: intelligence in the twentieth century*. Oxford University Press. 1995. ISBN 01-9507-391-6 paperback 01-9511-390-X
- *The Wizards of Langley: inside the CIA's Directorate of Science and Technology*. Westview Press. 2001. ISBN 08-1336-699-2
- *Spying on the bomb: American nuclear intelligence from Nazi Germany to Iran and North Korea*. Norton. 2006. ISBN 03-9305-383-0
- *Foreign intelligence organizations*. Ballinger Publishing Co. 1988. ISBN 0887301215

- *America's space sentinels: DSP satellites and national security* University of Kansas Press. 1999. ISBN 07-0060-942-3
- *The U.S. intelligence community.* Westview Press. 1995. ISBN 08-1332-376-2
- Jeffrey Richelson and Desmond Ball. *The ties that bind: intelligence cooperation between the UKUSA countries* Allen & Unwin. 1985. ISBN 00-4327-092-1
- *America's secret eyes in space: the U.S. keyhole spy satellite program.* Harper & Row. 1990. ISBN 08-8730-285-8
- *Social choice theory and Soviet national security decisionmaking.* Center for International and Strategic Affairs UCLA. 1982.
- *United States strategic reconnaissance: photographic/imaging satellites.* Center for International and Strategic Affairs UCLA. 1983.

4. James Bamford

James Bamford (1946-) amerikai író és újságíró, aki főleg az USA hírszerző ügynökségeiről ír. Natickből (Massachusetts) származik, a Vietnámi háború idején három évet töltött az USA haditengerészeténél, mint hírszerző. The Puzzle Palace című kötete az egész világon bestszeller lett, amelyben az elsők között tárta a nyilvánosság elé az amerikai titkosszolgálatok demokrácia ellenes tevékenységét.

Könyvei

- Bamford, James (1982). *The Puzzle Palace: a Report on America's Most Secret Agency*. Houghton Mifflin. ISBN 0140067485.
- Bamford, James (2001). *The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization*. Viking Pr.ISBN 0140231161.
- Bamford, James (April 30, 2002). *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency*. Anchor. ISBN 0385499086.
- Bamford, James (May 10, 2005). *A Pretext for War: 9/11, Iraq, and the Abuse of America's Intelligence Agencies*. Anchor. ISBN 140003034X.
- Bamford, James (September 16, 2008). *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Doubleday.ISBN 0385521324.

11. ZÁRSZÓ UTÁN

Meg kéne állni egy percre és elgondolkodni!
„Lilatehén effektus” vagy INFOSANCE a 21. század jövője?

„Az embernek már mind az öt érzékszerve eltompult az állatokéhoz képest,
kivéve ha az ember specifikumát, a gondolkodás szervét,
azaz az agyat speciális „érzékszervnek” tekintjük.
A 20. századi rohamos elektronizáció és számítástechnika által
azonban jó úton haladunk, hogy ezt az előnyünket is elveszítsük.”
(Szent-Györgyi Albert)

Szent-Györgyi Albert (1893-1986)

Nem véletlen, hogy e kötet előszavának mottója ugyanattól a gondolkodó óriásunktól származik, mint e záró fejezeté. Hiszen az elmúlt 10 fejezet gondolatainak mélyén végig ott lappangtak *Szent-Györgyi Albert* (1893-1986) gondolatai, melyek közé rímpárként igyekeztem saját gondolataimat fűzni. Eme fenti mottó azért is illik e zárszószerű fejezethez, mert (amint e kép is tanúsítja) utolsó magyarországi látogatásakor adott tévé riportban mondta. Eddig –valószínűleg sokad magammal- hordoztam magamban ezt, az akkor még a 20. századnak szóló nagyon mély gondolatot, és mivel úgy gondolom, hogy intelmét az a század nem fogadta meg, így most továbbadom. Ha könyvemmel hozzá tudtam járulni ahhoz, hogy Szent-Györgyi Albert szellemiségéhez híven, felhívjam a figyelmet arra, hogy *Meg kéne állni egy percre és elgondolkodni!*, akkor boldogan teszem le a tollat és búcsúzom a kedves Olvasótól.

Kérem, ezt a percet még töltse el velem, hogy az utolsó szó jogán elmondhassam:

A.M. Turing 1950-ben megjelent dolgozatában, gondolat-lavinát indított el egyetlen egyszerűnek tűnő kérdéssel: *„Szeretném, ha elgondolkodnának azon, hogy tudnak-e a gépek gondolkodni?”*

Alig több mint 60 év telt el azóta, és ma már az ebben a cikkben leírt és azóta Turing-tesztnek nevezett kísérlet az e-társadalmak napi gyakorlatává vált.
Turing eme kísérlet elemzésével nem csupán a mesterséges intelligencia kutatásokat indította el, hanem megalkotta a Turing-gépet is, amely az összes mai számítógép általános elméleti modellje. Egyben bebizonyította, hogy vannak olyan problémák, amelyeket e gép számára le tudunk írni, de a gép véges számú lépésben nem képes azt megválaszolni.
Nos, a 21. század információalapú globális infokommunikációs társadalmainak nélkülözhetetlen alapfeltétele a soha nem látott mennyiségű információ, a digitálisan leképezett „személyiségek” biztonságos tárolása, továbbítása, illetéktelenek által hozzáférhetetlenné tétele, vagyis a GLOBÁLIS TITOK megőrzése. A 21. század e-társadalma tehát egészen új kérdéssel kell, hogy szembenézzen:

Szeretném, ha Ön is elgondolkodna azon, vajon eldönthető-e,
hogy valós vagy virtuális információ van a globális információs rendszerek fekete dobozaiban?

Íme, a digitálisan leképezett virtuális világ alapaxiómái (ellenőrizhetetlen alapinformációi) a hit világába kerülnek. Ezt a jelenséget nevezem *„lilatehén effektus”*-nak, hiszen a mai gyerekek szinte már csak hit alapján képesek eldönteni, hogy a Milka lila tehene valóság, vagy csak virtuális állat?!

Íme a LILA TEHÉN EFFEKTUS szimbóluma!

Tehát napjaink abszolút technikai szempontok (és üzleti érdekek) szerint felépített társadalmai egy virtuális értékrendet alakítottak ki, sőt jobban belegondolva kiderül, hogy -én ezt hívom egyértékű társadalomnak-, ezekben az egyértékű társadalmakban nincs is értékrendszer, csupán egyetlen univerzális (csere)"érték". Tehát napjaink értékválságának már nem az a problémája, hogy kicserélődött az értékrendszer struktúrája, hanem az, hogy megszűnt létezni, virtualizálódott.

Azaz a pénzre, mint univerzális csereeszközre való érték konvertálás totálisan szünteti meg az ember differenciaspecifikumát jelentő humán értékeket.

Ez a *„van annyi pénz”*, egyértékű társadalmi modell képezi ma a világ fejlettnek nevezett társadalmainak egyre globalizálódó mintáját. Ebben a modellben a klasszikus emberi értékeket a gazdasághoz hasonlatos nullaösszegű játékként fogják fel, ami óriási hiba és az emberi társadalom önfelszámolásához vezet.

Mi lehet a kivezető út ebből az értékválságból?

Meglepő párhuzamosságokat találtam a reneszánsz kialakulásának okai és forradalmi céljai, valamint a jelen információalapú korunk között. A reneszánsz újra kinyitotta a középkori egyház által uralt, egészen beszűkített gondolkodást és a valós világ sokoldalú, kreatív szemléletére „nyitott ablakot”. Fellazult az egyház által ellenőrzött, egyetlen szálon függő információ-monopólium, amely az ismeretek és ezáltal a gondolkodás teljes uralmát jelentette. A gondolkodó ember „eldobta a dogmák mankóját”, mellyel éppen csak „járni” volt képes, és újra szabadon szárnyalhatott a gondolat.
A 20. század, amely száz év alatt több ezer évnyi technikai (eszköz)fejlődést hajszolt át a „civilizált” társadalmakon, újra „mankóra” ítélte az emberi gondolkodást (ettől óvott Szent-

Györgyi Albert fent idézett godolta!). Csak most az egyház helyett a technikai eszközök narkotikus függősége, a fogyasztói társadalom mesterséges rohanása kényszerítette rá az emberekre az elektronikus, digitális eszközök kiszolgáltató „mankóját".

Annak reménye, és egyben esélye, hogy e „mankókat" eldobhatjuk és ismét szabadon, könnyed léptekkel „járhatunk", az e-társadalom nagy lehetősége egy modern információs reneszánsz kor, az INFOSANCE megteremtése: az emberi értékek, az alapvető természeti és társadalmi törvények sokoldalú megközelítése, a modern technika eszközeinek támogatásával.

Az INFOSANCE kor, tehát a szabadon gondolkodó ember klasszikus képességeinek optimális egyesítése a mindent átszövő, globalizálódó e-technikával és az egyre teljesebb, biztonságosabb információ birtoklásával. Az INFOSANCE elnevezés egy olyan e-társadalom képét rajzolja fel, amelynek középpontjában egy új, modern *renaissance e-mber* áll. Az INFOSANCE *e-mber* lehetősége tehát „új ablaknyitás", amely a felhalmozott óriási technika, a globális kommunikációs és informatikai rendszerek lehetőségeit egyesíti a reneszánsz mintájú szabad, szárnyaló, kreatív, emberi gondolkodással. Az INFOSANCE társadalma kreatív társadalom, amely akárcsak az emberi kreativitás, a társadalmi túlélés alapfeltétele.
Nos, ezek a gondolatok, ez a különös, mégis mély analógia adta az alapot ahhoz, hogy az ezredforduló pillanatában, a jelen és valószínűleg az egész 21. századi korszakot INFOSANCE-nak, azaz *INFOrmációs renaisSANCE* kornak nevezzem el. Vagyis Jókai nagyszerű regényére asszociálva: az INFOSANCE a jelen század reménye!

Századunk hátralévő évtizedeire javaslom új mottóként:

*A **gondolkodás**,*
a gazdasággal ellentétben, nem nullaösszegű játék,
mert …

*A **gondolat**, akárcsak a **szeretet**,*
korlátlanul osztható és mindig van maradéka!

IRODALOMJEGYZÉK

[BARABÁSI 2008] Barabási Albert-László: Behálózva, Helikon Kiadó, 2008

[BENCSIK 2007] *Bencsik Anikó: Az RFID technológia alkalmazása a termék nyomkövetésben (szakdolgozat) Debreceni Egyetem, Agrártudományi Centrum, 2007.* http://odin.agr.unideb.hu/magisz/Palyazat/Diploma2007/Bencsik%20Aniko.pdf

[COLLING 2000] *Collingwood, John, Carnivore Diagnostic Tool, 16.8.2000, FBI-Press-Room http://www.fbi.gov/*

[CZEIZEL E. 2011] Czeizel Endre: Matematikusok – Gének –Rejtélyek (A magyar matematikus-géniuszok elemzése), Galenus Kiadó, Budapest, 2011.

[DAVIES 1982] Davies, D. W. - Barber, D. L. A. - Price, W. L. - Solomonides, C. M. (1982): Számítógép-hálózatok és protokollok, *Műszaki Könyvkiadó, Budapest, 1982.*

[DAVIES 1984] Davies, D. W. - Price, W. L. (1984): Security for Computer Networks: An Introduction to Data Security in Teleprocessing and, Electronic Funds Transfer Chichester, John Wiley & Sons, 1984.

[DIFFIE 1976] Diffie, W., Hellman, M. (1976): New Directions in Cryptography *IEEE Transaction on Information Theory, November 1976. (644-645)*

[DONALD 2000] *Kerr, M. Donald, Congressional Statement on Carnivore Diagnostic Tool, 6.9.2000, http://www.fbi.gov*

[EU-REP 2001] *REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) EUROPEAN PARLIAMENT Session document (A5-0264/2001), 11 July 2001*

[FARKAS J. 1999] Farkas János: Az információs társadalom küszöbén, Magyar Tudomány, 1999/12.

[GÁBOR 1976] Gábor Dénes: Válogatott tanulmányok, Gondolat, Budapest, 1976.

[HILL 2000] *Hill, Edward (2000). Declaration. Retrieved January 30, 2008, from Epic Government Documents Web site:http://epic.org/privacy/carnivore/fbi_dec1.jpg*

[HOFFMAN 1995] Lance J. Hoffman: Building in Big Brother, Springer-Verlag, New York, 1995.

[KALMÁR 1986] Kalmár László: Integrállevél, Gondolat, Budapest, 1986.

[LUKÁCS GY. 1918] Lukács György: Hét mese. In: Balázs Béla és akiknek nem kell. Összegyűjtött tanulmányok. Kner Izidor nyomdája, Gyoma, 1918.

[MAGYAR M. 1933] Magyar Miklós: Az ember és a gép harca, Királyi Magyar Egyetemi Nyomda, Budapest, 1933.

[NAJMÁNYI 2006] *Najmányi László: THEREMIN Enciklopédia Kiadó, 2006.,* http://thereminiad.webs.com/

[NEUMANN 1972] Neumann János: A számológép és az agy, Gondolat Könyvkiadó, Budapest, 1972.

[ORWELL 1989] *G.Orwell: 1984, Európa Könyvkiadó, Budapest, 1989.*

[RÉNYI 73] Rényi Alfréd: Ars Matematica, Magvető Kiadó, Budapest, 1973.

[SHANNON 1948] C.Shannon: The Mathematical Theory of Communication, Bell System Technical Journal, 1948.

[SHANNON 1949] C.Shannon: Communication Theory of Secrecy Systems, Bell System Technical Journal, 1949.

[SIMM 91/1] G. J. Simmons (ed): Contemporary Cryptology., IEEE Press, New York, 1991

[SIMM 91/2] G. J. Simmons: Identification of data, devices, documents and individuals. Proc 25th Annual IEEE Carnahan Conf. On Security Technology 1991, IEEE, New York, pp. 197-218.

[STOA-REP 1999] Interception Capabilities 2000, Report by : Duncan Campbell IPTV Ltd. Edinburgh, Scotland : April, 1999

[TARJÁN 58] Terján Rezső: Gondolkodó gépek, Bibliotheca Kiadó, Budapest, 1958.

[TURING 37] A.M.Turing: On computable numbers with an application to the Entscheidungsproblem, Proc.Lond.Math.Soc., 1937. (ser. 2) 42, 230-265

[TURING 39] A.M.Turing: Systems of logic based on ordinals, Proc.Lond.Math.Soc., 1939. 45, 161-228

[TURING 50] A.M.Turing: Computing Machinery and Intelligence, Mind, 9(1950), 433-460

[VASVÁRI 2009] Vasvári György: A társadalmi és szervezeti (vállalati) biztonsági kultrúra, AD-LIBRUM Kiadó, Budapest, 2009.

[WIENER 74] Norbert Wiener: Válogatott tanulmányok, Gondolat Kiadó, 1974.

[Wu 1999] Wu, W. W.: Vezeték nélküli multimédia hálózatok megbízhatósága. *Magyar Távközlés 10. (1999) április, 8-13.*

T.Dénes Tamás tárgyhoz kapcsolódó publikációi

[TDT 1978] Graph theoretical approach to structural representation of systems
Proceedings of the Fourth International Conf. for Pattern Recognition, Kyoto, Japan 1978.

[TDT 1979] On the use of mathematics to sociology today
In: Sociology of Science and Research, Akadémiai Kiadó, 1979.

[TDT 1986] The Role of Exceptions in Scientific Cognition, Creativity in Research
Science of Science, The Polish Academy of Sciences,
vol.6. 1986. august

[TDT 1988] S-gráf modell és diagnosztikai alkalmazása a vezetési rendszer elemzésében
In: Noszkay Erzsébet: Egészséges vagy beteg?
A vállalat diagnosztikai modellje 145.o.-
Közgazdasági és Jogi Könyvkiadó, 1988.

[TDT 2001/1] Biztonságos Információ(s) Társadalom (Két paradoxon egy címben)
INFO TÁRSADALOMTUDOMÁNY, 2001/53.

[TDT 2001/2] ECHELON az e-társadalom információpajzsa?
Híradástechnika, 2001/6. 14-19

[TDT 2001/3] SZTEGONOGRÁFIA - rejtett információk rejtjelzés nélkül
Híradástechnika, 2001/8. 15-21

[TDT 2002/1] „Rejtett csodafegyver”!
Népszabadság, 2002. június 6. /Fórum rovat/

[TDT 2002/2] INFOSANCE, a jövő INFOrmációs renaisSANCE társadalmának esélye
eVilág, I.évfolyam 4.szám, 2002/július

[TDT 2002/3] A globális e-társadalom és a terrorizmus „szövettana” a kriptográfia mikroszkópján át
(Gondolatok 2001.szeptember 11-e első évfordulóján)
CEO Magazin, III.évf. 2002/4.

[TDT 2002/4] e-MBER avagy egy új veszélyeztetett faj keletkezése
eVilág, I.évfolyam 6.szám, 2002/szeptember

[TDT 2002/5] A globális e-társadalom „kódolt” kockázata
Társadalomkutatás, 20.kötet 2002/3-4.szám 247-265

[TDT 2003/1] Turing-teszt az információs társadalomban, avagy
valós vagy virtuális e-társadalom?
Társadalomkutatás, 21.kötet 2003/3.szám 275-310

[TDT 2003/2] e-dokumentumok és személyesség
CEO Magazin, IV.évf. 2003/5.

[TDT 2003/3] Globális információ és személyes titkosítás
eVilág, II.évfolyam 11.szám, 2003/november

[TDT 2004/1] Információbiztonság az e-társadalomban
eVilág, III.évfolyam 6.szám, 2004/június

[TDT 2004/2] Információbiztonság kontra polgári szabadságjogok 1.rész
eVilág, III.évfolyam 8.szám, 2004/augusztus

[TDT 2004/3] Kódolatlan gondolatok (2001. szeptember 11-e harmadik évfordulóján)
eVilág, III.évfolyam 9.szám, 2004/szeptember

[TDT 2004/4] Globális fenyegetettség ellen globális információbiztonság
CEO Magazin, V.évf. 2004/3-4.

[TDT 2004/5] Információbiztonság kontra polgári szabadságjogok 2.rész
Az e-társadalom bizonytalanságáról
eVilág, III.évfolyam 11.szám, 2004/november

[TDT 2005/1] A dokumentumvédelem új módszerei
(Személyhez kötött és tömeges dokumentumok)
eVilág, IV.évfolyam 4.szám, 2005/április, 26-29

[TDT 2005/2] Biometrikus azonosítás,
avagy a személy egyedisége és a dokumentum személyessége
eVilág, IV.évfolyam 5.szám, 2005/május, 34-38

[TDT 2005/3] Információbizonytalanság az e-társadalomban. avagy
a Közös Fiók Rendszer (Common Boksz System), mint egy új, biztonságos
e-levelezési rendszer vázlata
Társadalomkutatás, 23.kötet 2005/2.szám 263-279

[TDT 2005/4] Digitális aláírás,
avagy a dokumentum tartalmának és tulajdonosának hitelessége
eVilág, IV.évfolyam 6.szám, 2005/június, 6-10

[TDT 2005/5] Digitális ujjlenyomat,
avagy a dokumentumvédelem periódusos rendszere
eVilág, IV.évfolyam 7.szám, 2005/július, 20-24

[TDT 2005/6] Digitális csőlátás, vagy az információs társadalom felkiáltójelei
eVilág, IV.évfolyam 12.szám, 2005/december, 24-29

[TDT 2006] Az Internet és a globális hálózatok biztonságáról
CEO Magazin, VII.évf. 2006/3. Melléklete (16 o.)

[TDT 2007] A biztonság konvergencia-programja
eVilág, VI.évfolyam, 2007/június, 1-8

[TDT 2010] (Információ)biztonság a Nagy Testvér 60. születésnapján
Társadalomkutatás, 28.kötet 2010/4.szám 447-463

Könyvek

[TDT 2002-k] TitokTan Trilógia 1.rész
Kódtörő ABC (Kriptográfia Mindenkinek)
Bagolyvár Könyvkiadó, Budapest,2002. *ISBN 963-944-704-8*

[TDT 2003-k] Titkos-számítógép-történet
Aranykönyv Kiadó, Budapest, 2003. *ISSN 1785-4318*

[TDT 2004-k] TitokTan Trilógia 2.rész
Klasszikus REJTÉNYEK (Kriptográfiai ARCképcsarnok)
Bagolyvár Könyvkiadó, Budapest,2004. *ISBN 963-944-726-9*

[TDT 2005-k] TitokTan Trilógia 3.rész
Újkori REJTÉNYEK (REJtélyek és TÉNYEK a titkosításról)
Bagolyvár Könyvkiadó, Budapest,2005. *ISBN 963-944-777-3*

[TDT 2010] Titkosítás … és Szépirodalom
Magánkiadás, Budapest, 2010. *ISBN 978-963-08-0182-9*