Egy 50 éve publikált kriptográfiai tudományos cikk, mely több tudományterületen jelentős kutatásokat indított el,

az elektronikus aláírás alkalmazásának magyarországi elindulása

Szabó István
a matematikai tudomány kandidátusa,
ny. egyetemi docens, ELTE TTK Valószínűségelméleti és Statisztikai Tanszék

MELASZ alapító tag

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

Manuscript received June 3, 1976.

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

W. Diffie is with the Department of Electrical Engineering, Stanford University, Stanford, CA, and the Stanford Artificial Intelligence Laboratory, Stanford, CA 94305.

M. E. Hellman is with the Department of Electrical Engineering, Stanford University, Stanford, CA 94305.

Klasszikus kriptográfiai módszerek elve

Igény új elvű módszerekre

Lehetőségek új elvű módszerek alkalmazására

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

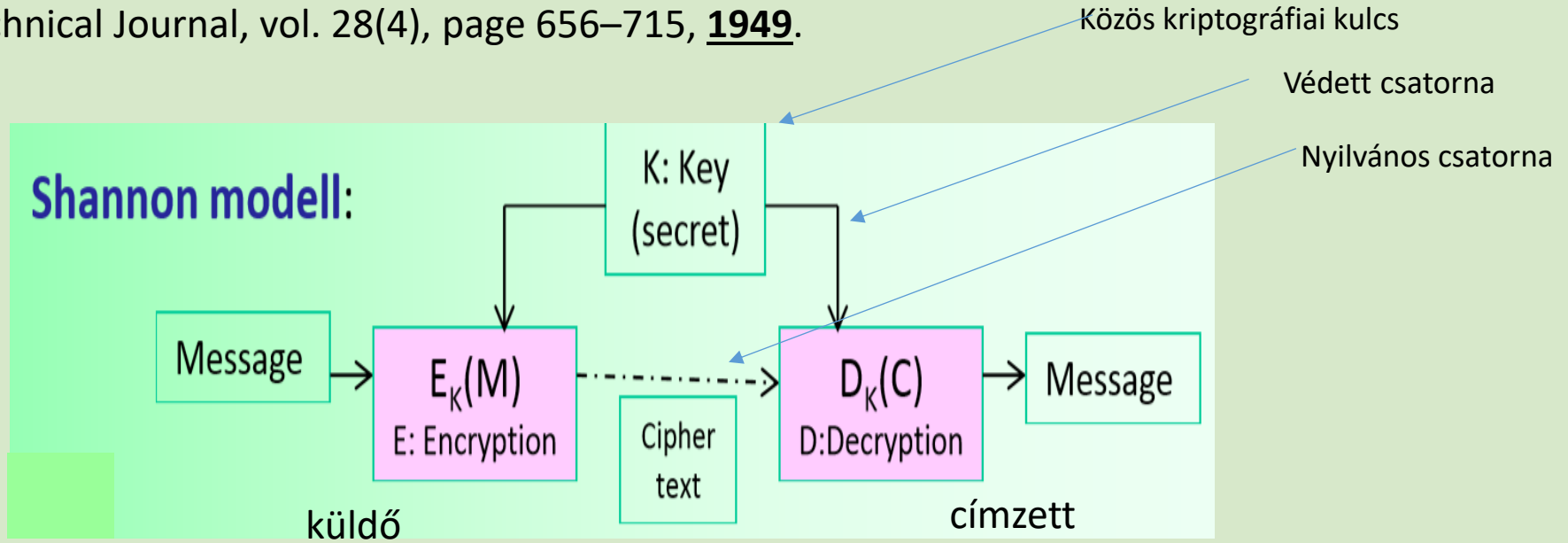
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Klasszikus kriptográfiai módszerek elve

Igény új elvű módszerekre

Lehetőség új elvű módszerek alkalmazására

Shannon-modell:
Shannon, Claude. "**Communication Theory of Secrecy Systems**",
Bell System Technical Journal, vol. 28(4), page 656–715, **1949**.



A fenti modellel működött a titkosítás a görögöktől az 1970-es évek végéig

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

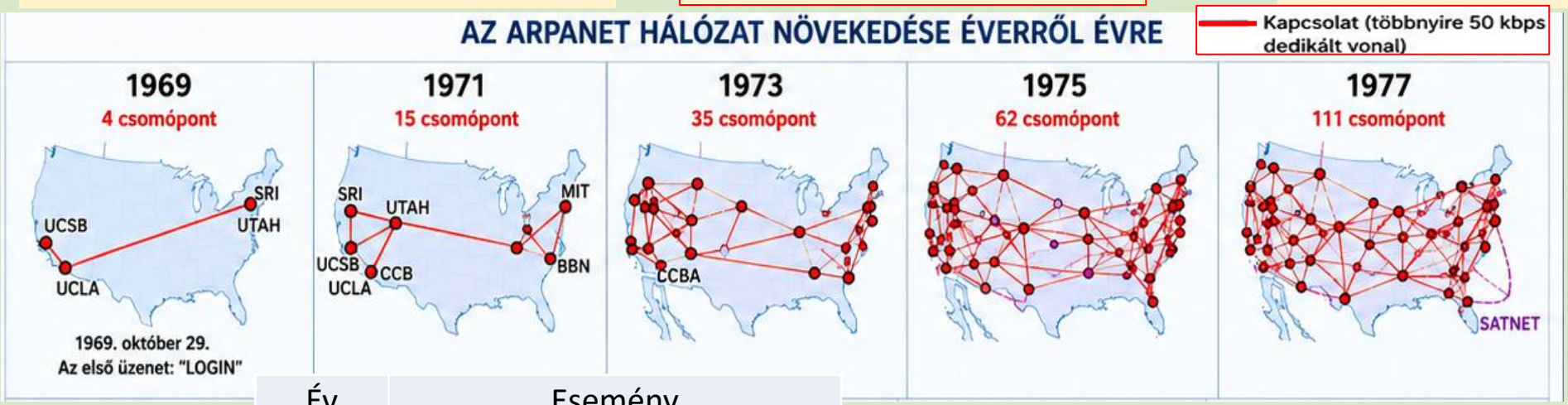
Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Klasszikus kriptográfiai módszerek

Igény új elvű módszerekre

Lehetőség új elvű módszerek alkalmazására



Rövidítés	Jelentés
UCLA	University of California, Los Angeles (Kaliforniai Egyetem, Los Angeles)
UCSB	University of California, Santa Barbara (Kaliforniai Egyetem, Santa Barbara)
UTAH	University of Utah (Utahi Egyetem)
SRI	Stanford Research Institute (Stanford Kutatóintézet)
BBN	Bolt, Beranek and Newman (Bolt, Beranek és Newman – mérnöki és kutatócég)

Év	Esemény
1969	ARPANET indulása
1971	első e-mail
1973	nemzetközi kapcsolat
1974	„Internet” fogalom megjelenése
1983	TCP/IP-re váltás
1990	ARPANET leállítása

Következtetés:

A klasszikus kriptográfia (Shannon modell) a közös titkos kulcsok minden kapcsolati párra védett csatornán történő cseréje a további fejlődés gátja:

meg kell oldani nyilvános csatornán a kulcsok cseréjét

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Klasszikus kriptográfiai módszerek

Igény új elvű módszerekre

Lehetőség új elvű módszerek alkalmazására

Számítástechnika fejlődése: nagyon bonyolult algoritmusok is megvalósíthatók, nincs technikai korlát (mint volt pl. Enigmánál)

1964: az IBM System/360 elindította a modern mainframe korszakot
1971: Intel bemutatta az Intel 4004 mikroprocesszort
1972–1974 között megjelentek az első „mikroszámítógépek”
1975–1977: az első valódi személyi számítógépek

A ***nyilvános csatornán egyeztetett titkos kulcsok kialakítására*** az 1970-es évek közepén 2 javaslat született:

Ralph Merkle ismerte fel először (1974), hogy szükséges és megoldható (a titkos kulcs-csere) probléma.

R. Merkle, "Secure communication over an insecure channel," submitted to *Communications of the ACM*.

Módszere: Merkle's Puzzles

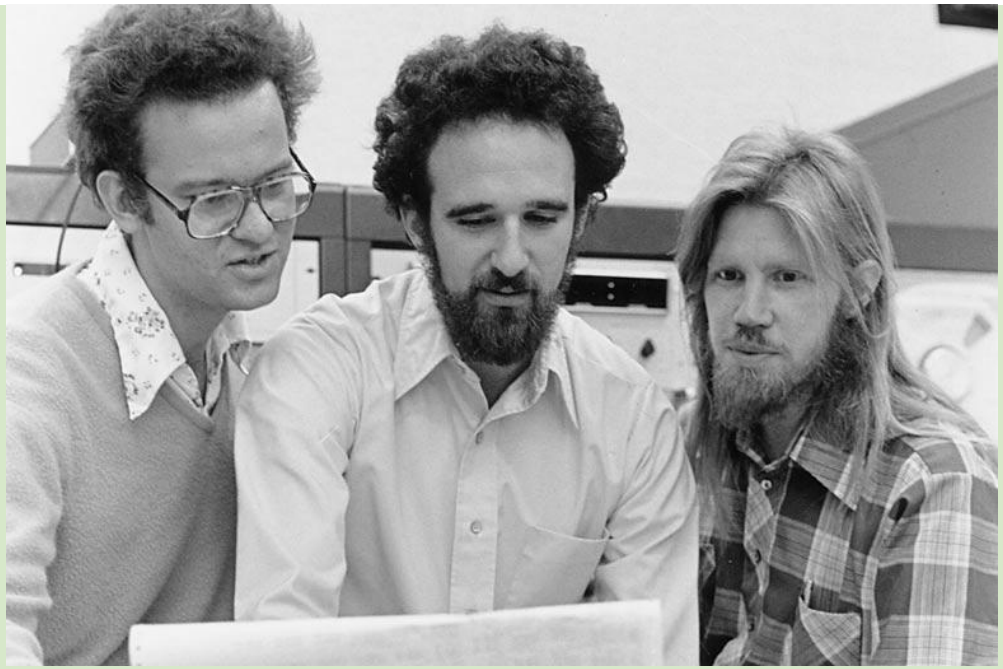
A Berkeley egyetemen beadta az ötletét, de nem fogadták el, és a neves CACM szaklap is visszadobta:
az egyik bíráló szerint ötlete kriptográfiai nonszensz, hibás tudomány, hiszen ***mindenki tudja, hogy a kriptográfiai kulcsokat titokban kell tartani***.
Csak 1978-ban tudta publikálni, a DH cikk után.

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE



Sokan a nyilvános kulcsú titkosítás fogalmát, kidolgozását együttesen Merkle, Diffie és Hellman neveihez kötik.

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

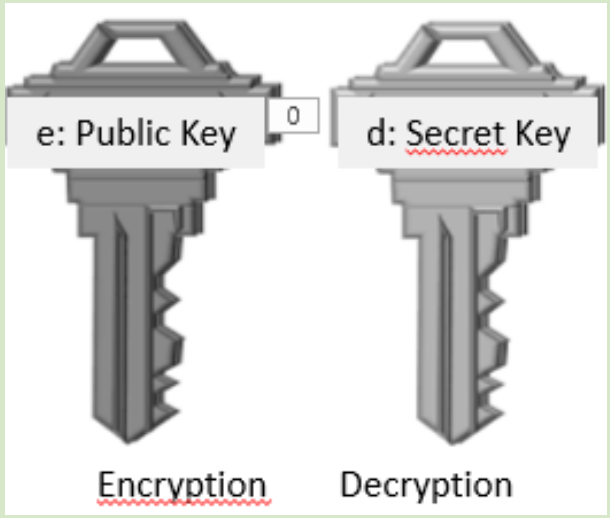
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A cikkben bevezetik a **PUBLIC KEY CRYPTOGRAPHY** fogalmát és ma is érvényes alapötleteit

Elvárás: kizárólag nyilvános csatornán kommunikálva az algoritmus biztosítani tudja a kommunikáció bizalmasságát

A cikkben erre az akkori ismeretek szerint „megoldhatatlannak” tűnő problémára D&H két megoldást javasolt:

a) Olyan kriptográfiai algoritmust, mely **két** (eltérő) **kriptográfiai kulcsot** alkalmaz titkosításra és megoldásra:



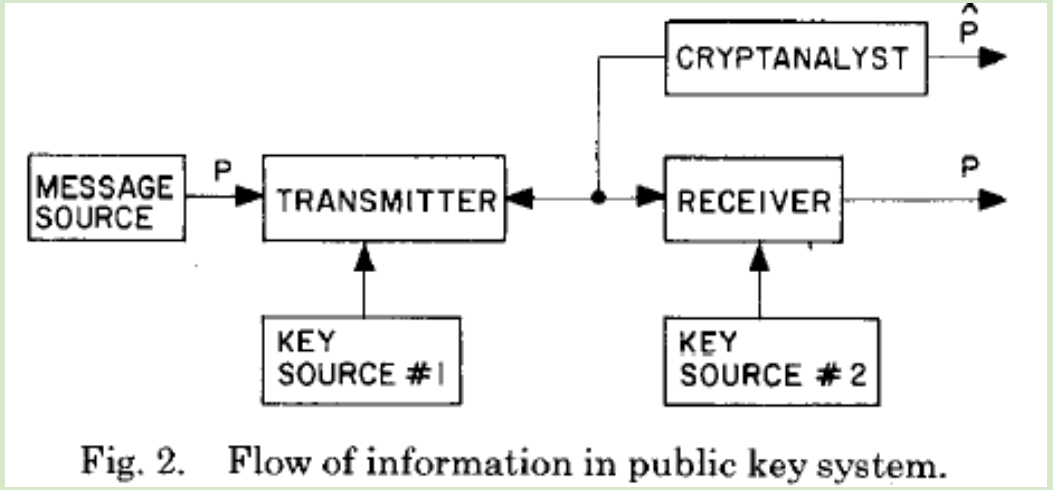


Fig. 2. Flow of information in public key system.

A kulcsgeneráláshoz bevezették az alábbi fogalmakat:

- **one-way function** (**egyirányú függvény**):
  y=f(x): x-ből y-t könnyű kiszámolni, de y-ból x-et nagyon nehéz;
  Cél: a nyilvános kulcsból ne lehessen kiszámolni a titkos (megoldó) kulcsot
- **trap door**: egy többlet információval a kulcs generátora viszont ki tudja a nyilvános kulcsból a titkos kulcsot kiszámolni

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

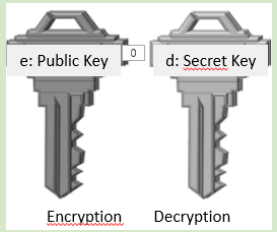
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A cikk bevezeti a **PUBLIC KEY CRYPTOGRAPHY** fogalmát és ma is érvényes alapötleteit

Elvárás: kizárólag nyilvános csatornán kommunikálva az algoritmus biztosítani tudja a kommunikáció bizalmasságát

A cikkben erre az akkori ismeretek szerint „megoldhatatlannak” tűnő problémára a III. fejezetben két megoldást javasoltak:

a) Olyan kriptográfiai algoritmust, mely két (eltérő) kriptográfiai kulcsot alkalmaz titkosításra és megoldásra:



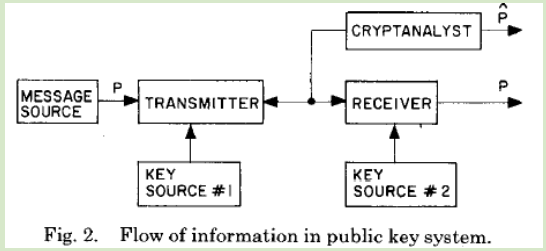


Fig. 2. Flow of information in public key system.

b) **egy** titkos kulcsot nyilvános csatornán egyeztető algoritmust (mely egyeztetett titkos kulccsal hagyományos algoritmussal biztosíthatja a bizalmasságot): „**Public key distribution systems**”

- küldő és címzett fél is generál (**titkos**) **random számot**
- ennek **egyirányú fv. képét** elküldik egymásnak
- a másik féltől kapott szám további egyirányú függvény képe lesz a **közös titkos kulcs**

D&H erre a felcserélhető sorrendű (kommutatív) egyirányú fv.-re a maradékos osztás számolásán alapuló hatványozást javasolták

Az algoritmus mai neve: **DH algoritmus**

Mindkét módszernél kiemelkedő probléma az üzenet küldőjének és tartalmának hitelessége:

(mely nem probléma a Shannon modellnél)

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

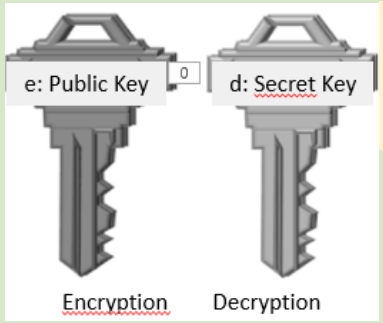
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

A cikkben bevezetik a **PUBLIC KEY CRYPTOGRAPHY** fogalmát és ma is érvényes alapötleteit

Elvárás: kizárólag nyilvános csatornán kommunikálva az algoritmus biztosítani tudja a kommunikáció bizalmasságát

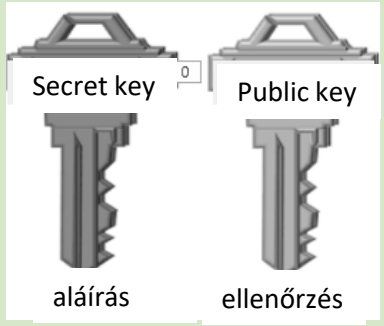
A cikkben erre az akkori ismeretek szerint „megoldhatatlannak” tűnő problémára a III. fejezetben D&H két megoldást javasolt:

a) **Két kriptográfiai kulcsot** alkalmazó titkosítás:



A kétkulcsos kriptográfia alapötlete lett az **elektronikus aláírás** algoritmusainak alapja:

a két kulcs funkciójának megváltoztatásával:
- **a titkos kulcs az aláíró kulcs,**
- **a nyilvános kulcs az aláírás ellenőrző kulcs**

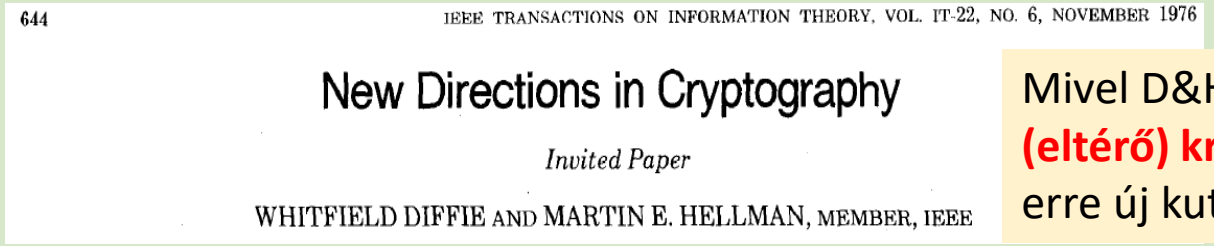


Ilyen kétkulcsos (aláírásra is használható) **kriptográfiai algoritmust a cikk szerzői még nem ismertek, de a cikk hatására nagyon sokan elkezdték kutatni a megoldást.**

b) DH (kulcsegyeztető) **algoritmus**

A **DH** algoritmus a kétkulcsos aláírási hitelesítéssel a mai **internet biztonságának alapvető algoritmusa**

Szinte **minden protokollban** (HTTPS, VPN, SSH) és **minden hálózati alkalmazásban** (banki, e-számla, web-kereskedelmi, államigazgatási stb. rendszerekben) **jelen van**.
Napi szinten milliárdszámra futnak DH-alapú, hitelesített kulcscserék a világ internetes infrastruktúrájában.

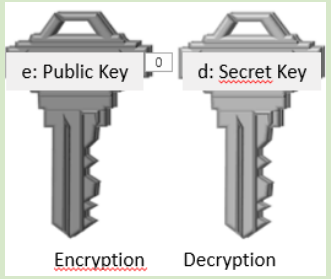

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

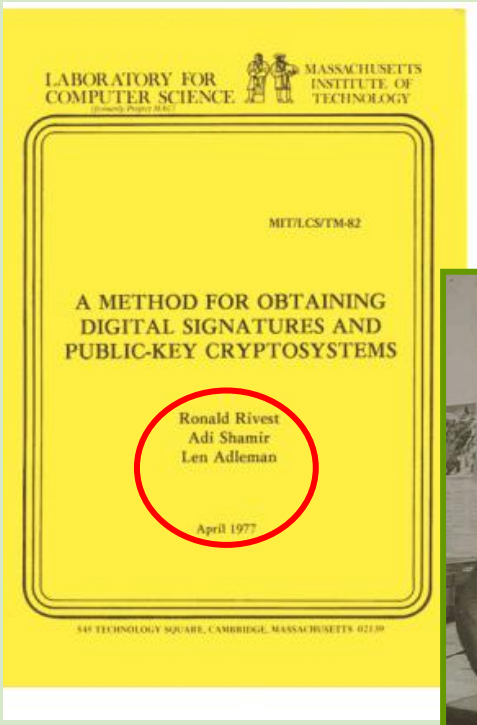
Invited Paper

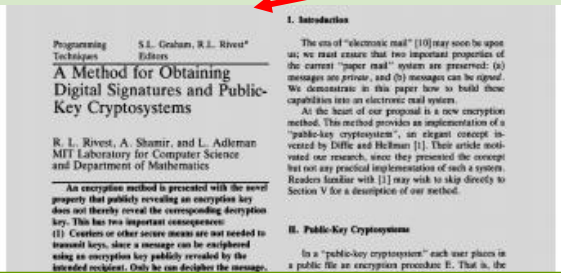
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Mivel D&H még nem ismert megoldást a **két (eltérő) kriptográfiai kulcsot** alkalmazó titkosításra, erre új kutatások indultak. Az első javaslat:

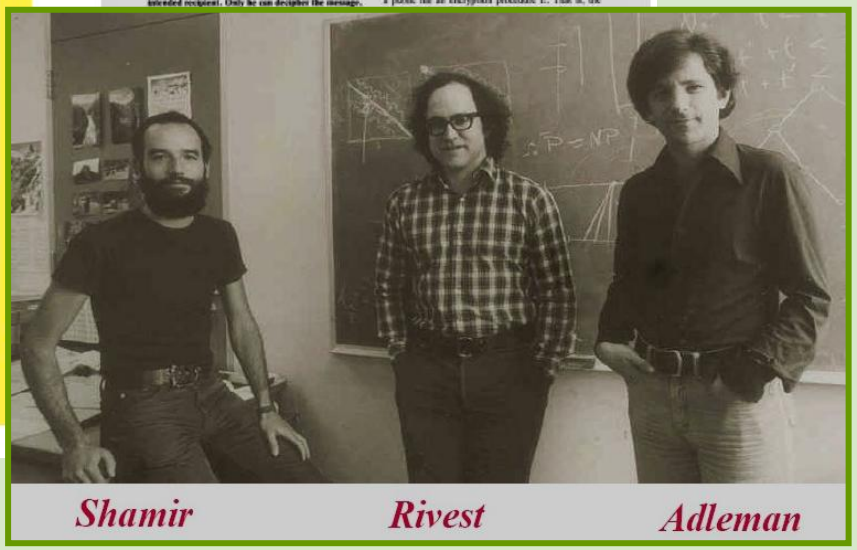


1977




A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

R. L. Rivest, A. Shamir, and L. Adleman
MIT Laboratory for Computer Science and Department of Mathematics



Az algoritmus ötlete a D&H által keresett

- egyirányú függvény: a nagy számok könnyű összeszorzása, (de szorzatból a prímtényezőket meghatározni nehéz);
- Csapda információ: a prímtényezők, melyek ismeretében az évszázadok óta ismert eljárással az ***e*** nyilvános (titkosító) kulcsból a ***d*** titkos (megoldó) kulcs kiszámolható

Felhasználták a modulo aritmetika (maradékos osztás) számelméleti eredményeit, melyek alapjait Fermat és Euler dolgozta ki


Pierre de Fermat
1601-1665


Leonhard Euler
1707-1783

Az algoritmus neve a kutatók kezdőbetűiből

RSA algoritmus

A betűszó sorrendjének oka:

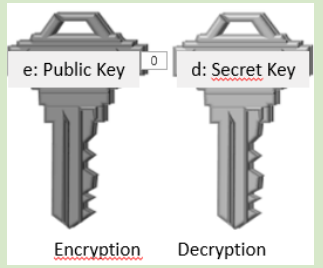
- Rivest dolgozta ki az algoritmust,
- Shamir matematikai ötletekkel járult hozzá
- Adleman elsősorban az algoritmus helyességének bizonyításában, és a cikk megírásában vett részt.

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

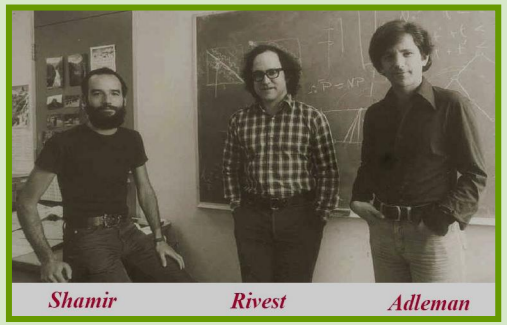
Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE



Javaslatok **két kriptográfiai kulcsot** alkalmazó titkosításra:

1977



1978

Ralph Merkel, Martin Hellman: „Hiding Information and Signatures in Trapdoor Knapsacks”

1985

Victor S. Miller, Neal Koblitz: **„Use of Elliptic Curves in Cryptography”**
(Az algoritmus rövid neve **ECC** lett)

Az elliptikus görbék általános alakja: $\mathbf{y^2=x^3+ax+b}$ (mod **p**)
(u.n. Weierstrass egyenlet)

- definiálták a görbéken az egész értékű (x,y) pontok összeadását és szorzását, majd ennek kriptográfiai alkalmazását
- Az (a,b,x,y) paraméterek több száz bites számok

Mind az RSA, mind az ECC széles körben elterjedt (mindengyikünk használja), mindkettőnek vannak előnyei, hátrányai.
Az ECC előnye a sebesség és kisebb paraméter-méretek


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Legjelentősebb hatása, hogy az addig titkosan kezelt területből **nyilvános kutatási terület lett**

„A kriptográfia demokratizálása”

- Diffie–Hellman publikációja előtt a fejlett kriptográfiát főként katonai és hírszerző szervezetek használták, fejlesztették
- a II. világháború alatt titkoban már matematikusok is segítették a feltörést, pl. az USA-ban Shannon; Angliában Turing.

Az NSA még sokáig próbálta korlátozni az „erős” titkosítás exportját:

- International Traffic in Arms Regulations (ITAR) szabályozta, a listán szerepelt a „cryptographic equipment and software” is:
- exportált szoftverekben gyakran csak **40 bites titkosítás** volt engedélyezett.

Érdekesség: még1991-ben is Phil Zimmermannt is beperelték a PGP (Pretty Good Privacy) erős titkosítás programjának publikálásáért.

Miután a kriptográfia **nyílt tudományos terület** lett egyetemeken és ipari kutatásban is gyors fejlődés indult.


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Legjelentősebb hatása, hogy az addigi titkosan kezelt területből **nyilvánosan kutatási terület lett**

A nyilvános tudományos kutatások új kriptográfiai területek fejlődését indították el, pl.:

- **Digitális aláírás biztonsága** és ökoszisztémája
- **Blind Signatures** (1982-, pl. eCash, e-szavazás,…)
- ZKP: **Zero- Knowledge Proof** (1985-, pl. jelszó nélküli hitelesítés, kriptovaluták,…)
- FHE: **Fully Homomorf Encryption** (1978-, pl. egészségügyi, banki titkosított adatokon végzett számítások)
- **Threshold cryptography,** MPC: **Multi-party cryptography** (titokmegosztási sémák)
- **Kleptography** (a kriptográfiai eszköz szándékosan olyan trap door-t tartalmaz, melyet csak a támadó tud kihasználni)
- **PQC**: Post-Quantum Cryptography (a kavantum-számítógépeknek is ellenálló kriptográfia)


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Matematikai kutatások

RSA

Nagy számok prímszámokra bontásával (faktorizáció) már sok évszázada foglalkoztak a matematikában, de **jelentős matematikai fejlődése az RSA publikálása után indult meg**:

Míg 1983-ban még „csak” **50** decimális jegyből álló (két prím szorzatát) számot tudtak faktorizálni,
2020- ban már **250** decimális jegyből (két prím szorzatából) álló számot:

21403246502407449612644230728393335630086147151447550177977549208814180234471401366433455190958046796109928518724709145876873962619215573630474547705208051190564931066876915900197594056934574522305893259766974716817380693648946998715784949759374979 37

A faktorizációs eredmények (a processzorok sebesség-növekedésén túl, ld. Moore tv.)
nagyrészt a **matematikai módszerek** jelentős fejlődésén alapultak:

CF: Continued Fractions
QS: Quadratic Sieve
NFS: Number-Field Sieve

→ Pl.: x,y ($x \neq y$) keresése, melyre
$x^2 \equiv y^2 \pmod n$

Jól ismert, az ilyen kutatási eredmények miatt kellett az alkalmazásokban az RSA n értékét folyamatosan növelni:
(n bitmérete: 1024 → 2048 → 3000 felett)

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Matematikai kutatások

ECC

Az elliptikus függvények, görbék kutatása Newton (1642-1727) és Leibniz (1646-1716) munkásságával nagyon régen kezdődött.

Az ECC publikálása után a matematikai kutatások sokkal intenzívebbé váltak, pl.:

- rengeteg kriptográfiailag gyenge görbét fedeztek fel, pl. supersingular és anomális görbéket,
- a Dual_EC_DRBG gyengeségének felfedezése 2007-ben (D. Shumow, N. Ferguson: „On the Possibility of a Back Door in the NIST SP800-90 Dual EC PRNG")

Érdekesség: az intenzív elliptikus görbe kutatások és eredményeik hozzájárultak az egyik leghíresebb matematikai sejtés: a Fermat sejtés bizonyításához.

Fermat **1637**-ben fogalmazta meg sejtését: az $x^n + y^n = z^n, \quad n > 2$ egyenletnek nincs pozitív egész értékekre megoldása.

Az 1984-ben Gerhard Frey („Links between Stable Elliptic Curves and Certain Diophantine Equations") megmutatta, hogy ha létezne egy nem triviális megoldása a Fermat-egyenletnek, akkor abból egy különleges elliptikus görbe konstruálható, mely ellentmondásra vezet.

Ezzel **az ECC alapegyenletének kutatásai is hozzájárultak az elméleti matematika egyik nehéz problémájának megoldásához**:

Andrew Wilesnak kb. 7 éves, titokban végzett kutatás alapján **1994**-ben sikerült bizonyítania a 350 éves matematikai problémát.


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Matematikai kutatások

Számítástechnikai, kutatások

- A kvantumszámítógépek ötletét Richard Feynman már **1982**-ben felvetette,
- **P. Shor 1994-ben (**„Algorithms for Quantum Computation: Discrete Logarithms and Factoring”) bemutatta, ha létezne kvantumszámítógép, akkor azzal az RSA és a DH algoritmus törhető lenne.
- Ez **felgyorsította és stratégiai jelentőségűvé tette a kvantumszámítógépek fejlesztését**, mivel így
  - jelentősen nőtt a kutatási támogatás,
  - bekapcsolódtak az állami és hírszerző, védelmi szervezetek,
  - megjelentek jelentős ipari beruházók.

IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére

Kriptográfia

Matematikai kutatások

Számítástechnikai, kutatások

Jogtudomány

Diffie és Hellman cikke a digitális hitelesítés lehetőségének megjelenítésével kikényszerítette az elektronikus aláírások elfogadásának jogi szabályozását.

- A kriptográfusok már az 1970-es évek végén tudtak biztonságos elektronikus aláírást készíteni, de
- a jogalkotók csak közel húsz évvel később kezdtek olyan nemzetközi szabályokat alkotni, amelyek kimondták, hogy egy digitális aláírás jogilag is egyenértékű lehet a kézzel írt aláírással.


IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

WHITFIELD DIFFIE AND MARTIN E. HELLMAN

II. A DH cikknek nagyon jelentős hatása volt több tudományterület fejlődésére :

Kriptográfia

Matematikai kutatások

Jogtudomány

Az ENSZ Közgyűlése **1966. december 17**-én hozta létre az **UNCITRAL**-t (**U**nited **N**ations **C**ommission on **I**nternational **Tra**de **L**aw – az ENSZ Nemzetközi Kereskedelmi Jogi Bizottságát) az ENSZ szakosított jogalkotási szervezetét.

UNCITRAL Model Law on Electronic Commerce (1996)

- az elektronikus dokumentum joghatású lehet,
- az elektronikus forma nem utasítható el csak, mert nem papír,
- az elektronikus üzenet bizonyítékként felhasználható,…

UNCITRAL Model Law on Electronic Signatures (2001)

EU 1999/93/EK irányelv az elektronikus aláírásra vonatkozó közösségi keretfeltételekről (1999)

Bevezette a köv. fogalmakat:

- elektronikus aláírás
- fokozott biztonságú elektronikus aláírás
- minősített tanúsítvány
- hitelesítés-szolgáltató

2001. évi XXXV. törvény az elektronikus aláírásról

Nagyrészt átültette az EU 1999/93/EK elvárásait és

- meghatározta a felügyelő hatóság feladatait,
- a szolgáltatók felelősségeit; ellenőrzését;
- az elektronikus aláírási termékek tanúsítását végző szervezetek feladatait stb.

eIDAS: AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2014. július 23-i 910/2014/EU RENDELETE

elektronikus azonosítás, - bélyegző, - időbélyeg, weboldal-hitelesítés,…

III. Az elektronikus aláírás alkalmazásának magyarországi elindulása

A magyar jogrendszerbe illesztéshez az Eat-hoz nagyon sok részletszabályozást kellett kiadni, pl.:

Idő	Jogszabály	Szerepe
2001	**2001. évi XXXV. törvény az elektronikus aláírásról (Eat.)**	A magyar e-aláírási alaptörvény: elektronikus aláírás, fokozott biztonságú aláírás, minősített aláírás, tanúsítvány, hitelesítés-szolgáltató, felügyelet.
2001	**16/2001. (IX. 1.) MeHVM rendelet** az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről	A hitelesítés-szolgáltatókra és e-aláírási szolgáltatásokra vonatkozó részletes követelmények: tanúsítvány, CRL, időbélyegzés, szabályzatok, biztonsági működés.
2002	**2/2002. (IV. 26.) MeHVM irányelv** a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről	A minősített e-aláírási szolgáltatások biztonsági követelményei; megjelentek az elfogadott kriptográfiai algoritmusok, BALE, HSZ, ISZ, PKI fogalmak.
2003	**2003. évi C. törvény az elektronikus hírközlésről**	A hírközlési hatósági háttér és az elektronikus aláírás felügyeleti környezetének intézményi alapja.
2004	**2004. évi LV. törvény az elektronikus aláírásról szóló 2001. évi XXXV. törvénymódosításáról**	Az Eat. jelentős módosítása; pontosította többek között az aláíró és kapcsolódó fogalmak szabályait.
2005	**3/2005. (III. 18.) IHM rendelet** az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről	A 16/2001-es rendelet korszerűsített utódja: szolgáltatók, hitelesítési rendek, szolgáltatási szabályzatok, technikai és szervezeti követelmények.
2005	**9/2005. (VII. 21.) IHM rendelet** az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról	Elektronikus aláírási termékek tanúsítását végző szervezetek kijelölése; BALE, kriptográfiai modulok, tanúsító szervezetek.
2005	**193/2005. (IX. 22.) Korm. Rendelet** az elektronikus ügyintézés részletes szabályairól	Az elektronikus ügyintézés részletes szabályai; az e-aláírás közigazgatási használatának tágabb eljárási környezete.
2005	**194/2005. (IX. 22.) Korm. Rendelet** a közigazgatási hatósági eljárásokban felhasznált elektronikus aláírásokra és az azokhoz tartozó tanúsítványokra, valamint a tanúsítványokat kibocsátó hitelesítés-szolgáltatókra vonatkozó követelményekről	közigazgatási elektronikus aláírások, közigazgatási gyökér-hitelesítésszolgáltató

III. Az elektronikus aláírás alkalmazásának magyarországi elindulása

A 2021. évi elektronikus aláírási törvény, valamint a végrehajtási rendeletek kidolgozásakor (példa értékűen) sok **konzultációt folytattak az államigazgatás és a gazdasági, tudományos terület szakértői**, **pl. a következő résztvevők**:

Informatikai Kormány-biztosság

dr. Dessewffy Anna: a törvénytervezet szakmai koordinátora

Sík Zoltán kormánybiztos: az elektronikus aláírási törvény kormányzati előterjesztésének felelőse

Informatikai és Hírközlési Minisztérium

dr. Sikolya Zsolt az elektronikus közigazgatás és a digitális aláírás alkalmazásának egyik tervezője

Hírközlési Fő-felügyelet, majd NHH, NMHH

dr. Rényi István a hazai PKI infrastruktúra, hitelesítési rendek kialakításának, ellenőr-zésének szakértője, KGYHSZ vezetője

dr. Sylvester Nóra pl. a hitelesítés-szolgáltató felügyeleti kérdéseinek szabályozása

IM: Jogszabályi egyeztetések

dr. Rátai Balázs az elektronikus aláírás hazai jogi kereteinek szakértői támogatása

Első magyar hitelesítés-szolgáltatók

NetLock,
Microsec
MÁV Informatika

Tanúsító szervezetek

Mátrix Kft
Hunguard Kft.

2004 –ben megalakult a Magyar Elektronikus Alá-írás Szövetség (**MELASZ**), alapítók: 23 magán-személy és 7 szervezet.

Első vezetőség:
Elnök: Almási János
Ügyv.: Rózsahegyi Zsolt,
Balázs István,
Brehel József
Csapodi Márton

Fejlesztők

Például: eGroup, Polysys, Noreg stb.

III. Az elektronikus aláírás alkalmazásának magyarországi elindulása

Az elektronikus aláírás bevezetésnél sok nehézséget okozott, hogy az alkalmazók ismeretei nagyon hiányosak voltak és rendszereik sem voltak még kellően felkészültek. **Néhány példa a „kezdetekből”:**

1. Sokan nem értették, miért hívják aláírásnak (ha ez biológiai tulajdonsághoz nem kapcsolódó, nem látható bitsorozat)?

2. Több vitatéma volt: pl. digitális aláírás (technológiai szakma) **vagy elektronikus aláírás** (jogi szakértők)
(indokolást ld. pl. dr. Kósa Ferenc tavalyi eSignDay előadásában: „Digitalizáció kihívásai”)

3. A törvény elfogadása után egy hivatali elektronikus aláírási projektben így **szabályozták a folyamatot**:

1) Dokumentum elkészítése Word-ben
2) PDF generálása
3) Minősített elektronikus aláírás ráhelyezése
4) Dokumentum kinyomtatása
5) Kézi aláírás
6) Visszaszkennelés
7) Irattározás

4. Egy cég elektronikusan aláírt szerződést küldött egy partnernek.
A partner visszaírt: „A dokumentum hitelessége ellenőrizve. Az aláírás érvényes. De a biztonság kedvéért kérünk egy faxot is.”
Ez volt az első „**hibrid protokoll”** (RSA + fax hibrid).

5. Az elektronikus számlázás bevezetésekor sok könyvelő bajban volt:
Az egyik könyvelő kérdése: – „Hol van az eredeti példány?”
A válasz: – „Az elektronikus.”
A könyvelő: „De akkor mit teszek a dossziéba**?”**

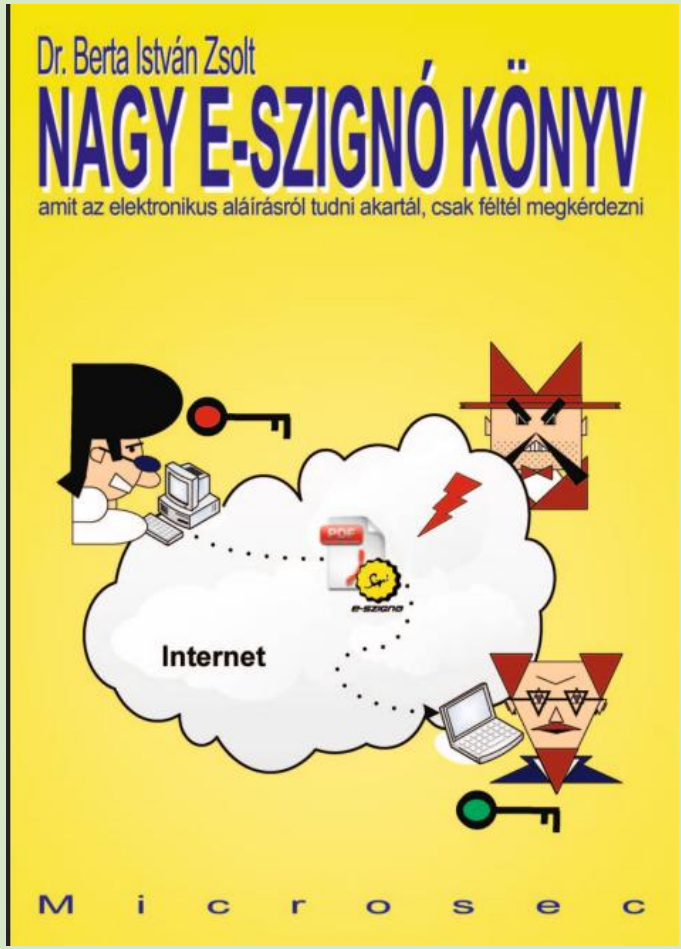
Ma már minden internetező használja az elektronikus aláírást…
csak legtöbben nem tudják, hogy nap mint nap használják, és hol.

III. Az elektronikus aláírás alkalmazásának magyarországi elindulása

Nagy szükség volt az elektronikus aláírással kapcsolatos ismeretterjesztésre, oktatásra.

Ma természetes, hogy pl. az egyetemi informatikai, műszaki, matematikai oktatás része.

A MELASZ, a hitelesítés-szolgáltatók is részt vettek és vesznek az ismeretterjesztésben, valamint nagy számú segítő könyvet is kiadtak, pl.:



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

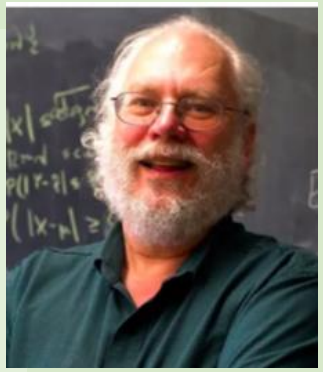
Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

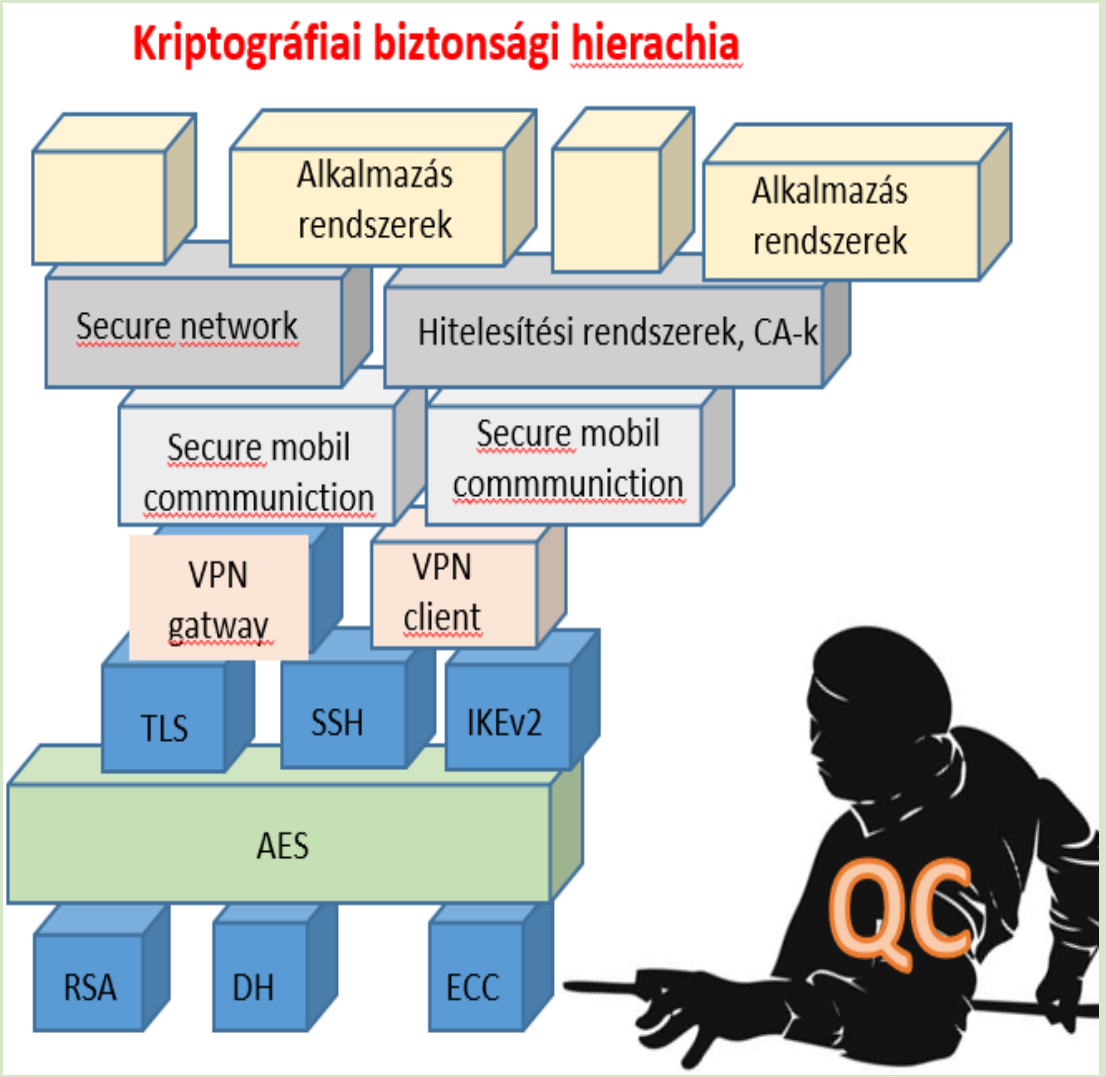
IV. A DH cikk hatása a jövő kriptográfiájára

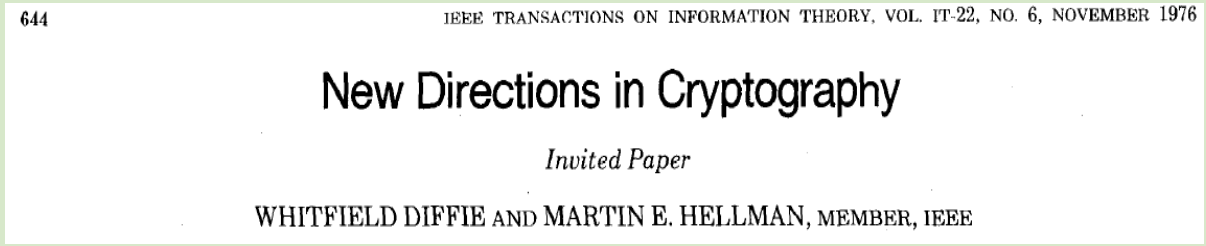
Niels Bohr-nak tulajdonítják a mondást:
„A jóslás nehéz, különösen ha a jövőre vonatkozik.”

a) Közismert, hogy a **CRQC** (**Cryptographically Relevant Quantum Computer**) megjelenésével (röviden: „**Q-Day**”) a ma használt **informatikai rendszereink biztonsága megkérdőjeleződik**.



P. Shor 1994-ben publikált módszere (mivel ez általános eredmény, az ú.n. véges Abel-csoportok rejtett periódusának, a Hidden Subgroup Problem meghatározására vonatkozott), kvantum-számítógépen **mindhárom alapvető nyilvános kulcsú algoritmusra** (DH, RSA, ECC) **alkalmazható.**




644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

IV. A DH cikk hatása a jövő kriptográfiájára

a) Közismert, hogy a **CRQC** az RSA, a DH alg. és az ECC már nem nyújt megfelelő védelmet.

b) Fel kell készülni a Q-day-re (CRQC-k: a kriptográfiailag hatékony kvantumszámítógépek) megjelenésére

A Q-day előtt, már ma is a rendszereink már kvantumszámítógéphez kapcsolódó biztonsági kockázatokkal rendelkeznek

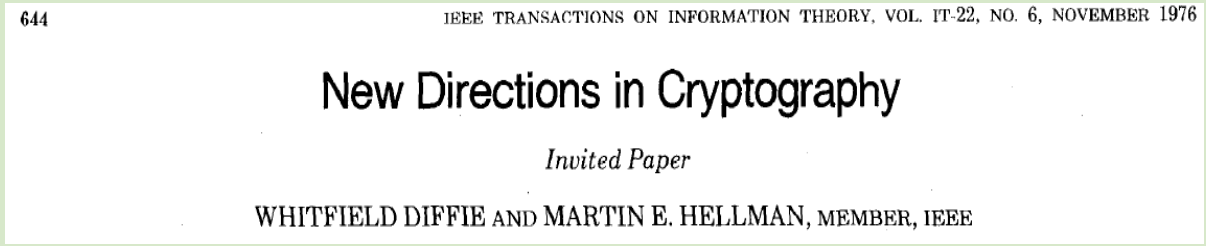
A kockázat egyik oka, hogy **a felkészülés és áttérés** a kvantumszámítógépeknek is ellenálló (ú.n. **PQC**: poszt-kvantumtitkosí-tási) rendszerekre mind a bizalmasság, mind a hitelesség szempontjából **nagyon hosszú időt vehet igénybe**.

A bizalmasság védelme szempontjából ezt a kockázati időt jelentősen (akár sok évvel) növelheti, hogy a hosszú ideig védendő információkat a **HNDL:** Harvest Now, Decrypt Later Attack veszélyezteti.

A kockázat becslését az ú.n. Mosca tétel segíti (ld.pl. https://eprint.iacr.org/2015/1075.pdf).

A **NIST** (National Institute of Standards and Technology)
NSA (National Security Agency)
CISA (Certified Information Systems Auditor),
ETSI (European Telecommunications Standards Institute) és
ENISA (European Union Agency for Cybersecurity)

PQC-migrációs dokumentumai mind ajánlják (vagy előírják):
nem a Q-Day bekövetkeztekor kell elkezdeni az átállást, hanem minél előbb el kell kezdeni a felkészülést.



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

IV. A DH cikk hatása a jövő kriptográfiájára

a) Közismert, hogy a **CRQC** az RSA, a DH alg. és az ECC már nem nyújt megfelelő védelmet.

b) Felkészülés a Q-day-re: a NIST, NSA, CISA, ETSI és ENISA PQC-migrációs dokumentumai eltérő ütemtervet dolgoztak ki

A **NIS Cooperation Group** (NIS: Network and Information Systems), melyet az **EU NIS2 Irányelv 14. cikke hozott létre** a Bizottság, az ENISA és a tagállamok képviselőiből) **2025. júniusában kiadta** a következő ajánlást:

EU PQC Workstream: A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography v1.1

https://digital-strategy.ec.europa.eu/en/library/coordinated-implementation-roadmap-transition-post-quantum-cryptography?utm_source=chatgpt.com

3 ütemet javasolnak: **első ütem határideje: 2026.12.31.**, melyben javasolt **feladatok** között kiemelten szerepel a QRCQ-val sebezhető **kriptográfiai eszközök és beszállítóinak feltérképezése és nyilvántartása**.

Ez nem könnyű feladat, mivel ma a világon naponta ellenőrzött digitális aláírások több mint 99%-a nem ember által aláírt dokumentumhoz kapcsolódik, hanem gép–gép kommunikációhoz.

Fontos kriptográfiai nyilvántartási területek pl.:

- Software Systems, Applications
- Cryptographic Libraries
- Network Security Protocols
- Email and Document Signing
- User and Machine Authentication
- Code Signing
- Supplay Chain,
- Cloud Security
- CA's, Security Certificates,
- Hardware Accerelations
- IoT and Home Office Equipments,…

644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

IV. A DH cikk hatása a jövő kriptográfiájára

a) Közismert, hogy a **CRQC** az RSA, a DH alg. és az ECC már nem nyújt megfelelő védelmet.

b) Felkészülés a Q-day-re: a NIST, NSA, CISA, ETSI és ENISA PQC-migrációs dokumentumai eltérő ütemtervet dolgoztak ki

c) PQC algoritmusok szabványosítása és sok területen az átállás is már megkezdődött.

Több kripto-könyvtárban (pl. OpenSSL, wolfSSL, BouncyCastle), felhőszolgáltatásban (AWSLibCrypto) stb. már működnek szabványosított PQC algoritmusok, van amelyeket már validáltak is.

Az átállás szempontjából fontos az **ENISA** (European Union Agency for Cybersecurity) **2025. áprilisi** előírása (melyet a 2026-os még DRAFT kiadás is tartalmaz):

Note 40-Hybridization. LWE or MLWE based cryptographic mechanisms shouldn't be used in a standalone way to provide the intended security functionality, but should be combined with a well established classical cryptomechanism.

Ez vonatkozik mind a FIPS 203 kulcs-titkosító, mind a FIPS 204 aláíró szabványra

enisa

European Cybersecurity Certification Group
Sub-group on Cryptography

Agreed Cryptographic Mechanisms

Köszönöm a figyelmet