Titkosítási algoritmusok
- a hagyományos titkosítás végnapjai

Dömösi Pál (Intelligens Technológiák Kft., Debrecen)
intelligenstechnologiak@gmail.com

„Hagyományos" titkosítás= napjaink számítógéppel vagy napjaink valamiféle okos eszközével (okos telefon, okos karóra, okos mosógép, okos lakás, önjáró autó, stb) támogatott titkosítás

IBM (1975) : DES (Data Encryption Standard**)-** azt hitték, hogy feltörhetetlen marad – 1990 óta feltörhető

- 3 DES (1995) a DES-nél biztonságosabb, de ez is feltörhető (2017)

- Joan Daemen és Vincent Riljdael (2000) : NIST pályázat győztesei
Advanced Encryption Standard, AES (2001)
(talán) biztonságos (egyelőre)

Ron Rivest (1987) : RC4 – 2013 óta feltörhető

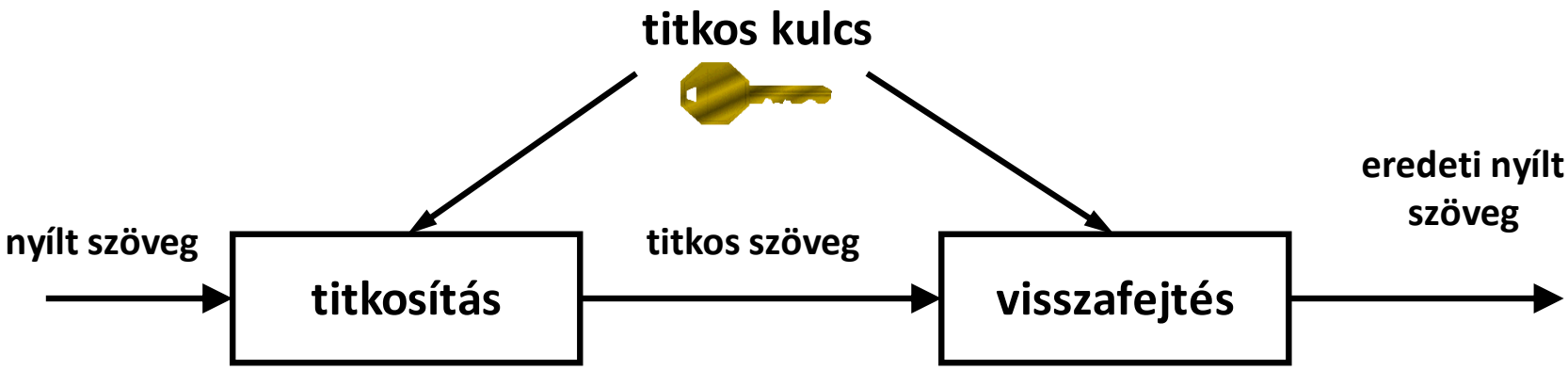
Whitfield Diffie és **Martin Hellman (1976)** szabadalmat nyújtottak be (és "New Directions in Cryptography" címmel tudományos dolgozatot publikáltak), melyben a nyilvános kulcsú titkosítás ötletét írták le. Ugyancsak benyújtották az úgynevezett egyirányú függvényekkel történő személyi azonosítás ötletét.

Ron Rivest, Adi Shamir és **Len Adleman (1976)** : RSA nyílt kulcsú titkosító algoritmus (Diffie és Hellman elgondolása alapján, de más elven működik)

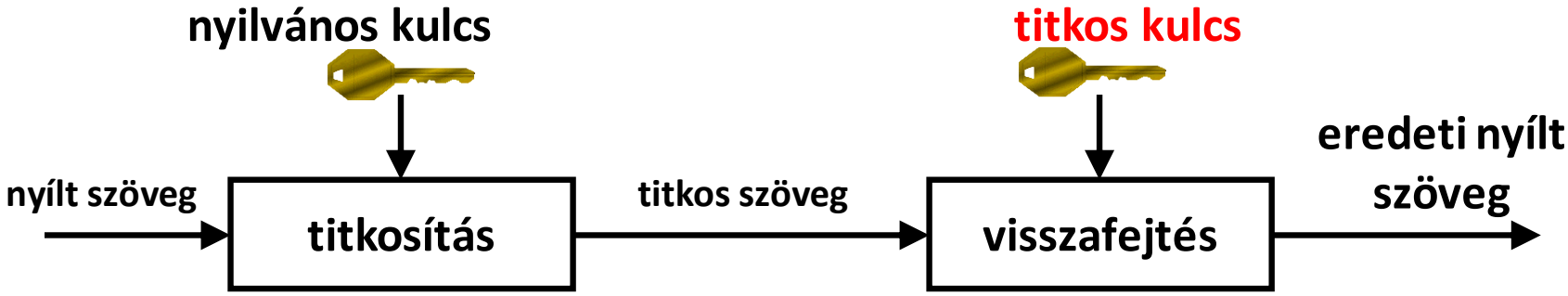
2. A szimmetrikus és aszimmetrikus rendszer összehasonlítása

titkos kulcs megosztás:

szimmetrikus (egy kulcsú) rendszer :



aszimmetrikus (két kulcsú) rendszer:



nyilvános kulcs: csak titkosításra

titkos kulcs : csak visszafejtésre

Szimmetrikus (egy kulcsú) rendszer :

1. **Folyamtitkosító:** titkosítás és visszafejtés karkaterenként/bitenként

2. **Blokktitkosító:** titkosítás és visszafejtés blokkonként (rendszerint 16 bájt vagyis 128 bit hosszúságú bitlánconként)

Folyamtitkosítás előnye: a titkos szöveg nem tartalmaz üres (feltöltő) karaktereket
Blokktitkosítás előnye: lavinahatás

Lavinahatás: egy nyílt szöveg blokk egyetlen karakterének/bitjének megváltoztatása a hozzá tartozó titkos blokk nagy mértékű megváltoztatását eredményezi.

Folyamtitkosítás hátránya: nincs lavinahatás
Blokktitkosítás hátránya: a titkos szöveg tartalmazhat üres (feltöltő) karaktereket (ha az üzenet hossza nem a blokkhossz többszöröse)

3. PGP rendszer (Pretty Good Privacy) Phillip Zimmermann (1991)

1. Küldd el nekem a nyilvános kulcsodat

2. OK küldöm és akkor küldd el nekem a tiedet

4. Júlia nyilvános kulcsa megy Romeohoz

titkos kulcs

Romeo nyilvános kulcsa megy Júliához

nyílt szöveg

titkosítás

titkos szöveg

nyilvános kulcs

titkos kulcs

nyílt szöveg

titkosítás

titkos szöveg

visszafejtés

eredeti nyílt szöveg

4. VESZÉLYEK:

Peter W. Shor (1994): *"Algorithms for quantum computation: discrete logarithms and factoring„ tudományos dolgozata alapján mind a Diffie-Hellmann, mind pedig az RSA kvantumszámítógéppel feltörhető.*

GOOGLE (2019): 53 kvantumbites kvantumszámítógép

Honeywell (2020): 64 kvantum mennyiségű
(vita van arról, hogy melyiknek nagyobb a számító kapacitása)
A Diffie-Hellmann, valamint az RSA rendszerek néhány éven belül használhatatlanok lesznek.

Nem igazi a veszély (?): vannak olyan nyilvános kulcsú rendszerek (például McEliece 1978-ban publikált rendszere), melyek kvantumbiztosak, azaz kvantumszámítógéppel nem törhetők fel. Igaz, számítás igényesebbek, de a processzorok fejlődésével ez nem fog igazi gondot jelenteni.
(Megjegyzés: a kvantumszámítógép csak az aszimmetrikus rendszerekre Jelent igazán veszélyt)

Hátradőlhetünk? Hát nem!
P. Kocher, 1996: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, And Other Systems

Oldalcsatornás támadások: a számítógépes rendszer megvalósításából származó információkon alapul , nem pedig a megvalósított algoritmus gyengeségein
Például: energiafogyasztás, elektromágneses szivárgás, hang, hő, stb)

Kapersky (2018). Az intelligens otthonok világában akár egy villanykörtén keresztül is leüríthetik a bankszámlánkat, és biztosak lehetünk benne, hogyha figyelmetlenek vagyunk, meg is teszik.

Védekezés(?) : Faraday-kalitkába helyezzük az eszközt.

Nem igazán 21. századbeli megoldás

IOT eszközök Faraday kalitkában?

Eredmény: okostelefon, okos óra, okos otthon, stb súly és terjedelemnövekedése.
Vagy: okos villanykörte Faraday kalitkában?
Más megoldás nem lehet?

XOR titkosítás : a nyílt szöveget bitlánccá alakítjuk, s egy ugyanolyan hosszúságú valódi vagy álvéletlen bitlánccal bitenként alkalmazzuk rá a kizáró vagy (XOR) műveletet. Ha Mondjuk a nyílt szöveg soron következő bitje a és a véletlen vagy álvéletlen bitlánc soron következő bitje b, akkor a titkos szöveg soron következő bitje a XOR b. Nyilvánvaló, hogy az a XOR b XOR b =a azonosság miatt a titkos szövegre és a véletlen vagy álvéletlen bitlánc bitenkénti XOR-ozásával visszakapjuk az eredeti szöveget.

Claude Shannon (1949): bizonyos feltételek teljesülése esetén a XOR titkosítás feltörhetetlen.

Sajnos ezzel is gond van.

Ismert nyílt szöveg alapú támadás: tegyük fel, hogy a támadó (hacker, rendszergazda, stb) megszerez egy nyílt szöveg-titkos szöveg párt. XOR titkosítás esetén a titkosítás kulcsa visszanyerhető, s ennek segítségével az eredeti üzenet helyett hamis üzenet küldhető. Ezen a helyzeten sajnos a többfordulós titkosítás sem segít.

Van kiút (ügyvezető társammal, dr Horváth Géza egyetemi docenssel közös alapötlet): mind a titkosításhoz, mind a visszafejtéshez megszerkeszthető egy-egy speciális táblázat úgy, hogy a XOR művelet helyett ezen táblázatokból történő kiolvasás műveletét alkalmazzuk:

Titkosításkor a XOR b helyett a T b -t vesszük, ahol is a T b jelöli a titkosításnál alkalmazott T táblázat a-val jelölt sorindexű és b-vel jelölt oszlopindexű elemének kiolvasását
Visszafejtéskor a XOR b helyett a V b –t vesszük, ahol is a V b jelöli a visszafejtésnél alkalmazott V táblázat a-val jelölt sorindexű és b-vel jelölt oszlopindexű elemének kiolvasását.

Eredmény: egy olyan hatékony folyamtitkosító, mely

- rezisztens mind az oldalcsatornás támadásra, mind pedig az ismert nyílt szöveg alapú támadásra
- gyors titkosítás, gyors visszafejtés, kis tárigény (mint a XOR-os titkosítók esetén)
- alkalmasan választott többfordulós változata átmegy az NIST teszten (US National Institute of Standards and Technology security tesztje)

Ezen (folyamtitkosító) találmányunk 2020-ban EU szabadalmat nyert, melyet 2021-ben Magyarországon, az Egyesült Királyságban, Franciaországban, Németországban, Svájcban hatályosítottunk.

Folyamtitkosító találmányunk USA szabadalmaztatása folyamatban van.

További fejlesztésünk: egy blokktitkosító, mely

- rezisztens az oldalcsatornás támadásra
- gyors titkosítás, gyors visszafejtés, kis tárigény
- alkalmasan választott többfordulós változata átmegy az NIST teszten
- lavinahatás

Blokktitkosítónkra 2021-ben nemzetközi (PCT) szabadalmi bejelentést tettünk.

Összegzés

Alap probléma: a napjainkban széleskörűen elterjedt titkosítási rendszereket a XX. Században fejlesztették ki, s nem igazán alkalmasak a XXI. században felmerülő Titkosítási problémák áthidalására.

A debreceni Intelligens Technológiák Kft néhány lépést tett ennek áthidalására

KÖSZÖNÖM A FIGYELMET.