MICROSEC
Számítástechnikai Fejlesztő Kft.

Hírek kriptográfiai algoritmusok biztonságáról

Dr. Berta István Zsolt <istvan.berta@microsec.hu>
K+F igazgató

Microsec Kft.

Miről fogok beszélni?

- Bevezetés
- Szimmetrikus kulcsú algoritmusok
  - Blokk-kódolók
  - Folyamkódolók
- Nyilvános kulcsú algoritmusok
- Hash függvények
- Mennyire biztonságos?

Az algoritmus nyilvánossága

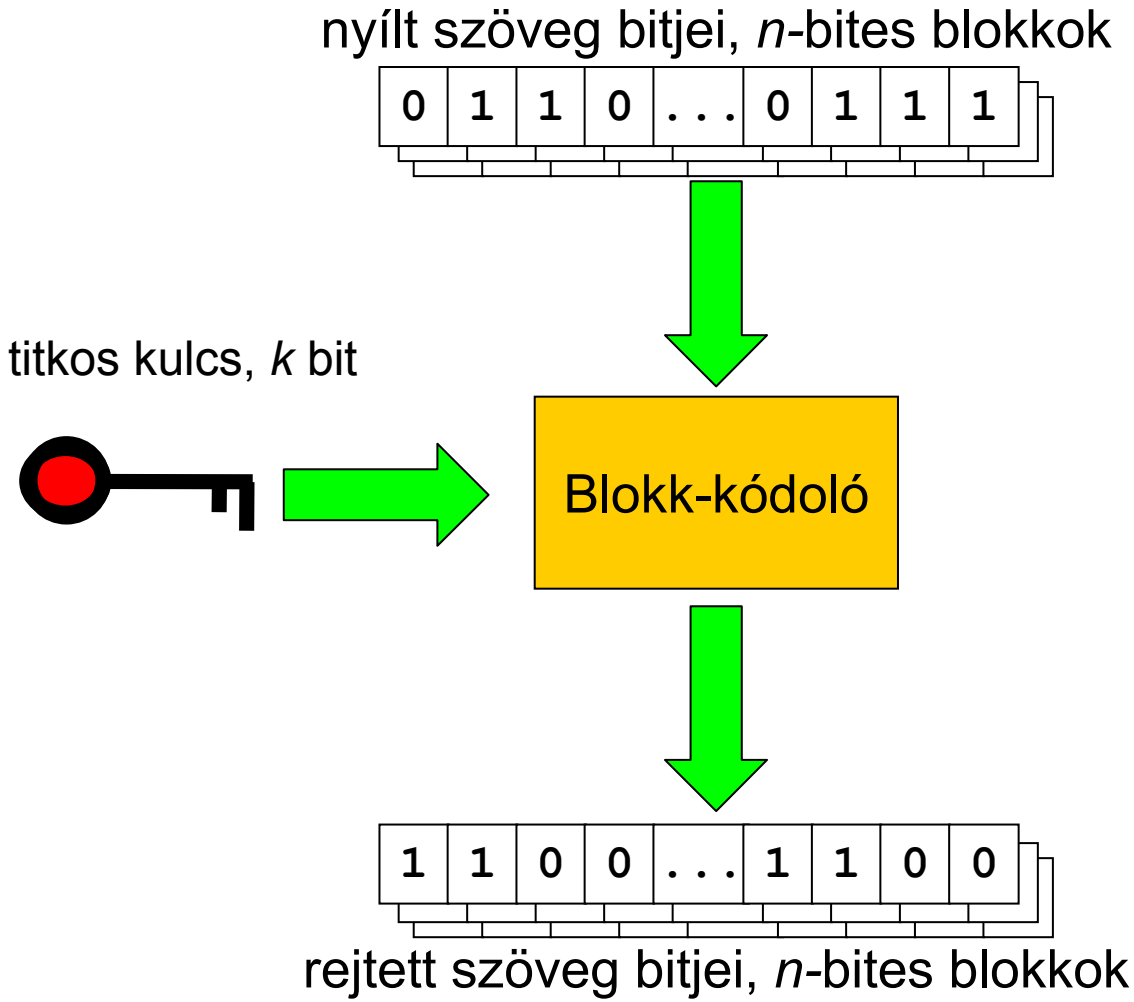
- Kerckhoffs feltétel (1883): egy jó algoritmus akkor is biztonságos, ha a támadó minden részletét ismeri, és egyedül a „kulcs” a titok
- „Gyanús”, ha egy algoritmust titokban kell tartani
- Egyes súlyos hibákat ki lehet mutatni kriptográfiai algoritmusokon, de
- Nem lehet megállapítani, hogy nincs-e hibája az algoritmusnak (kivéve spec. eseteket)

- **Ismert, publikált algoritmusokat kell használni, amiket már sok hozzáértő próbált támadni**

Mit jelent: „megtörtek” egy algoritmust?

- Valaki megfejtett egy kulcsot?
- „Törés” lehet pl.: kulcsok/üzenetek visszafejtése, aláírás hamisítása stb.
- Mi szükséges a töréshez?
  - Bárki egy másodperc alatt tud törni, a program kint van a gonoszvagyok.hu oldalon?
  - Az ország összes számítógépe 10 év alatt tud törni?
  - Az ország összes számítógépe 10 év alatt 1 % valószínűséggel tud törni?
  - A titkosszolgáltatok fel tudják törni?
- Valószínűsíthető, hogy néhány éven belül a fentiek valamelyike bekövetkezik?
- Matematikusok kitaláltak egy olyan módszert, ami gyorsabb/hatékonyabb az összes kulcs kipróbálásánál?
- ... ?

Blokk-kódoló



- Fix hosszúságú blokkok
- A blokkméret pl. 64 bit vagy 128 bit
- Blokkméretnél hosszabb üzenet esetén célszerű összefűzni blokkokat (pl. CBC üzemmód)

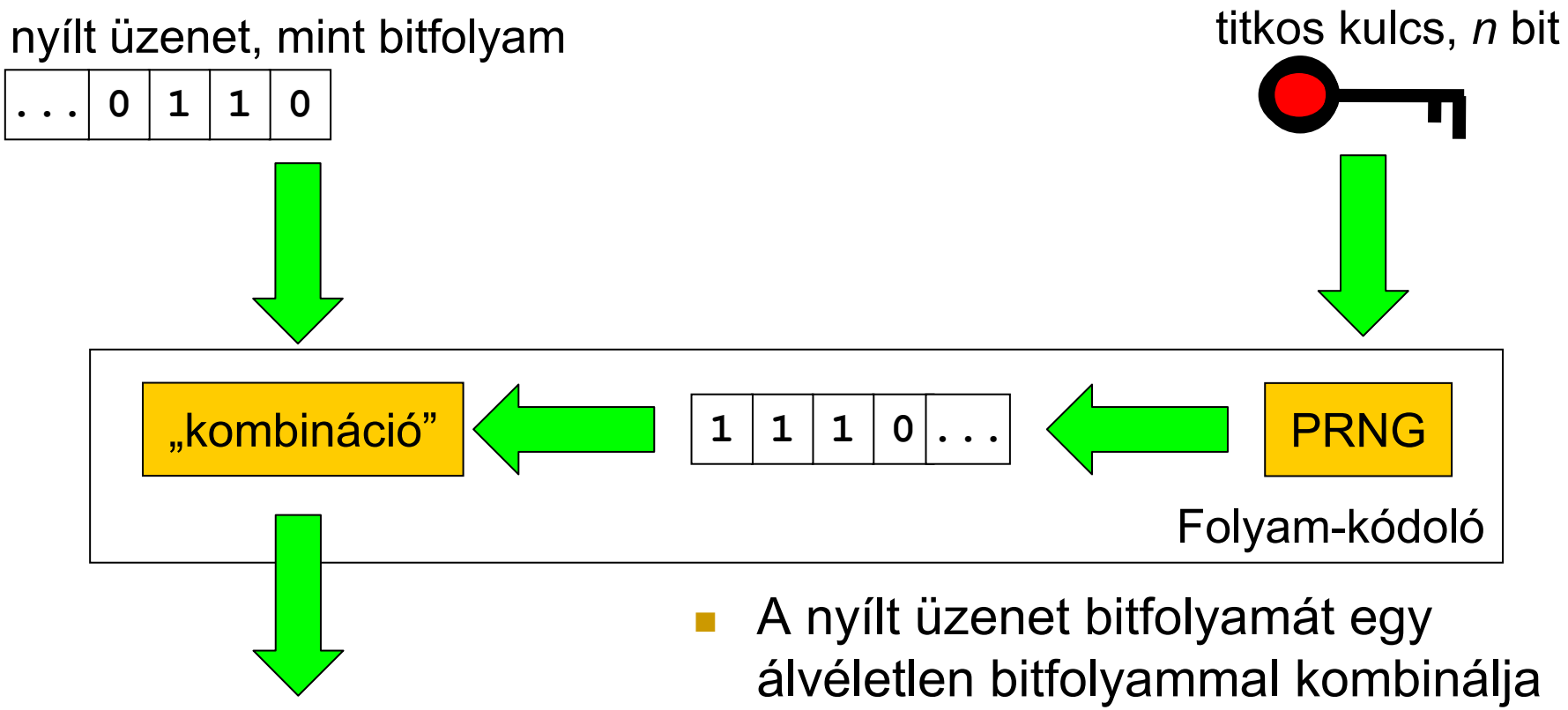
Blokk-kódolók ma…

- DES (1976): az 56 bites kulcs ma már kevés
- Ma biztonságos, tipikus kulcsméretek:
  - 112 bit, 128 bit, 256 bit stb.
- 3DES: 112 vagy 168 bites kulcs, de ez lassú
- AES (Rijndael)
  - pályázat, 2001
  - 128 bites blokkméret, kulcs: 128, 192 vagy 256 bit
- Sok erős blokk-kódoló létezik, pl:
  - Blowfish (1993), Twofish, Serpent, RC6, …

Támadások az AES ellen (2009)

- Biryukov és Khovratovich (2009)
  - AES-256 – 2^{119} lépésből, AES-192 – 2^{123} lépésből
  - a támadás nem minden környezetben működik
  - nagy tárkapacitás szükséges hozzá (2^{119} kompl.)
  - így az AES-128 nem feltétlenül erősebb náluk
  - az AES-192 most erősebb, mint az AES-256 ☺
- Biryukov, Dunkelman, Keller, Khovratovich és Shamir (2009)
  - egyszerűsített, kevesebb fordulóból álló AES-256 variánsok ellen mutattak támadásokat

Folyam-kódoló

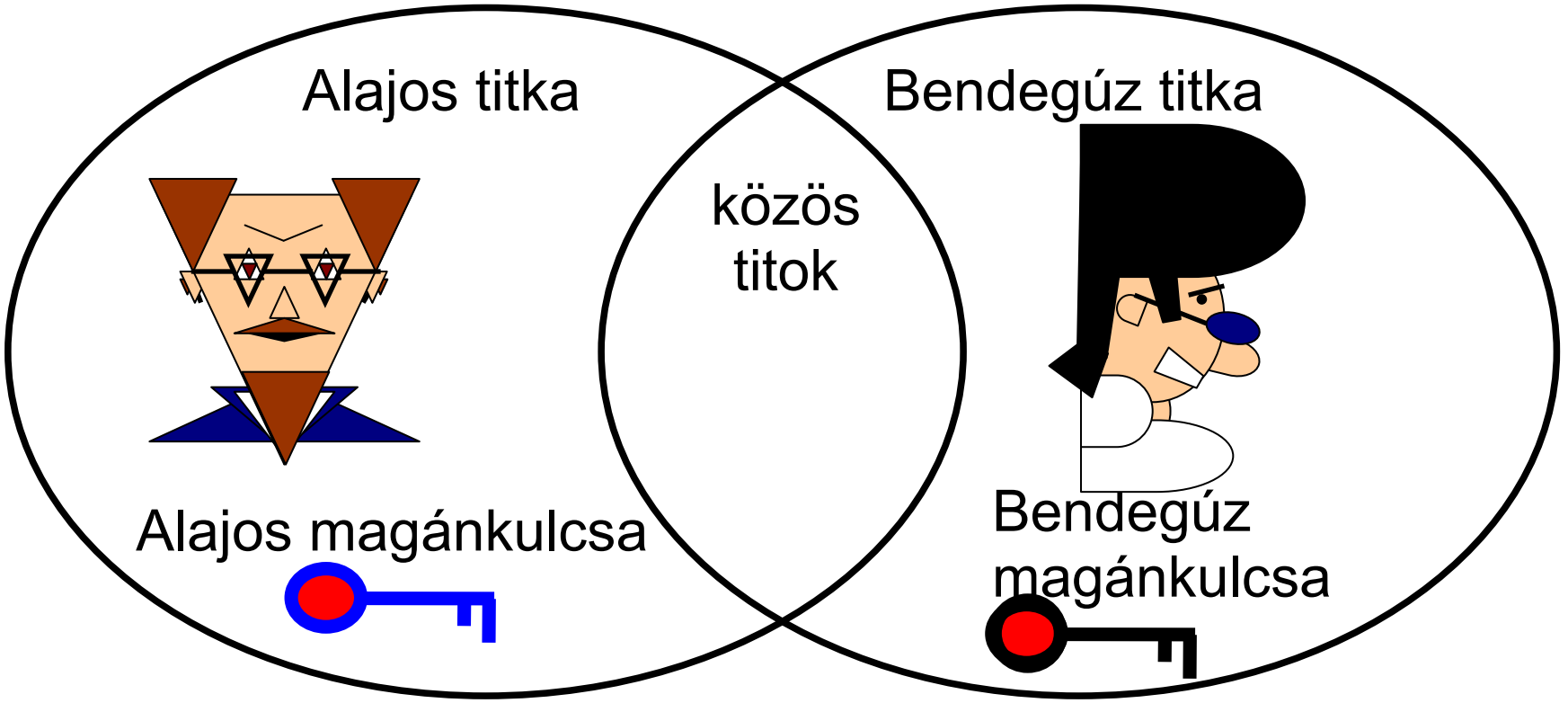


- A nyílt üzenet bitfolyamát egy álvéletlen bitfolyammal kombinálja (pl. XOR művelettel)
- Általában gyorsabb, és egyszerűbb, mint egy blokk-kódoló

Folyam-kódolók ma…

- RC4 / arcfour (1987), különösen népszerű (volt)
  - WEP, WPA, SSL (opt), Bittorrent
  - megtörték, már ne használjuk
- NESSIE (2000-2003): minden folyam-kódoló elbukott
- eSTREAM (2008): Grain, Rabbit, Salsa20, …
- Mobil környezet:
  - A5/1,2: titkos alg., visszafejtették, megtörték (1997)
  - A5/3 (Misty1→Kasumi): megtörték (2005, 2010)
  - CMEA, CMEA-I: megtörték (1997, 2008)
- Csak kevés maradt talpon, azok túl frissek ☹

Nyilvános kulcsú kripto: titkosítás, aláírás



Alajos nyilvános kulcsa

Bendegúz nyilvános kulcsa

NYILVÁNOS ADATOK

Nyilvános kulcsú algoritmusok

- Mindig egy „nehéz” matematikai problémára épülnek:
  - IFP, egész számok faktorizálhatósága – RSA
  - DLP, diszkrét logaritmus probléma – DSA, ElGamal, DH
  - ECDLP, elliptikus görbék pontjai feletti diszkrét logaritmus probléma – ECC (ECDSA, EC-ElGamal, EC-DH)
- „Kevés” nyilvános kulcsú kriptográfiai algoritmust ismerünk
- Aláírni csak nyilvános kulcsú alapon lehet

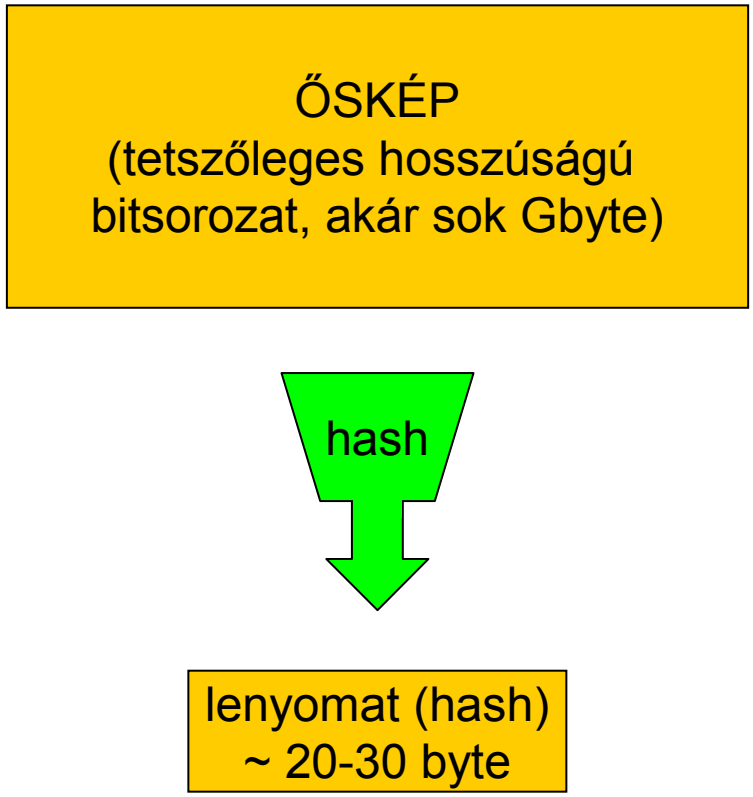
RSA (Rivest, Shamir, Adleman)

- Ma ez a legelterjedtebb nyilvános kulcsú algoritmus
- Már régen léteznek a véletlen próbálkozásnál sokkal gyorsabb (de még nem hatékony) támadások
- 768 bites RSA-t már törtek (2009)
- 1024 bites kulcs: kivezetés alatt (!)
  - NIST Special Publication 800
  - ETSI: „ALGO paper” – ETSI TS 102 176, V2.0.0
  - Microsoft, Mozilla, … NHH
  - Nem tudunk publikált támadásról
- RSA esetén legalább 2048 bites kulcsot célszerű használni

ECC (elliptic curve cryptography)

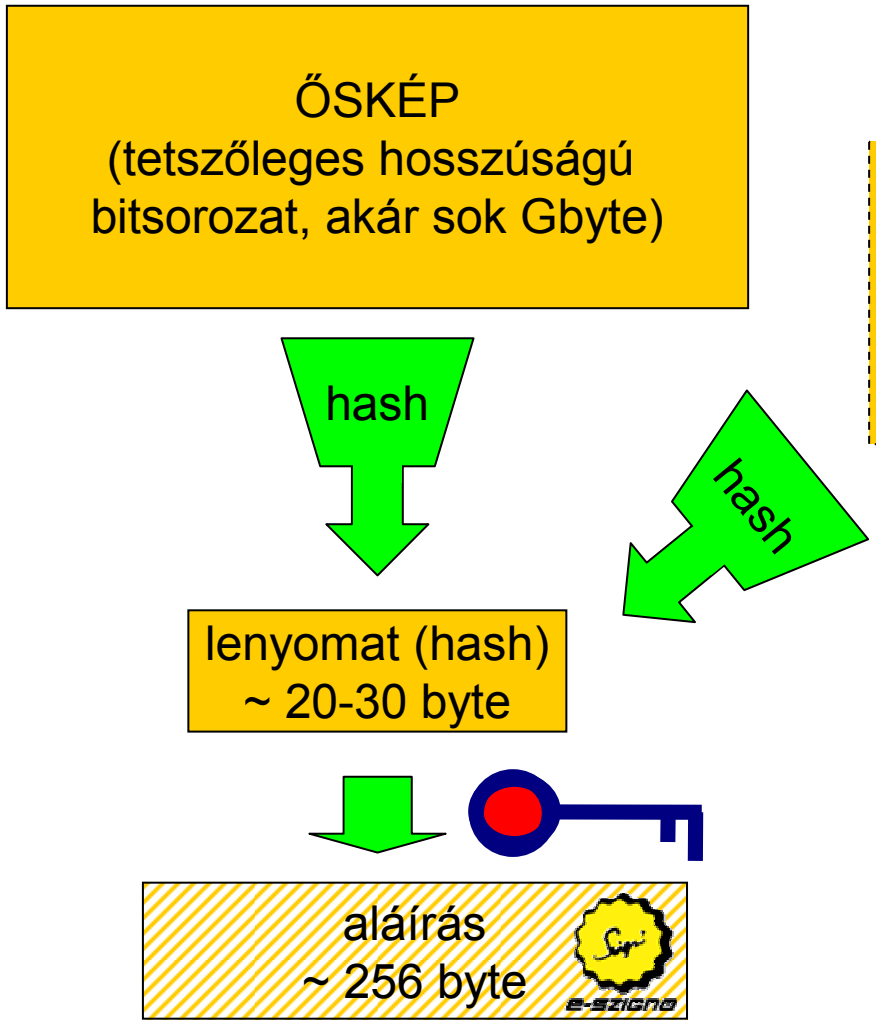
- Más alapokra épül, mint az RSA
- Kevésbé hatékony támadások léteznek ellene, ma rövidebb kulcsokkal nyújt az RSA-val ekvivalens biztonságot
- Bonyolultabb számításokra van szükség, így nem feltétlenül gyorsabb az RSA-nál
- Ma biztonságos kulcsméret: 224 vagy 384 bit
- NSA, Suite B Crypto (2009): áttérés ECC-re (!)
- Szabadalmak (Certicom)

Kriptográfiai hash függvény



- Szűkítő leképezés (tetszőleges hosszú bitsorozatról fix hosszúságú bitsorozatra)
- Őskép ellenállóság (adott lenyomathoz „nehéz” hozzá tartozó ősképet találni)
- Ütközés ellenállóság („nehéz” két olyan ősképet találni, amelyekhez azonos lenyomat tartozik)

Az ütközés ellenállóság jelentősége



- Ha a hash függvény nem ütközésellenálló, másik dokumentum is előállítható, amelyhez ugyanaz az aláírás tartozik.

Hash függvények ma...

- MD5 – súlyos gyengeségek, nem ütközés-ellenálló!
  - Ronald Rivest (1991)
  - már nem ütközés-ellenálló (2004), „rouge CA” (2008)
- SHA-1 – új rendszerben már ne
  - 20 byte-os lenyomat
  - NSA, 1995 /SHA-0, 1993/
  - sikeres támadás, ütközés, 2^{52} lépésből (2009)
- SHA-2 – ez a jövő
  - az NSA fejlesztette ki (2001)
  - SHA-224, -256, -384, -512
  - SHA-256: 32 byte-os lenyomat
- SHA-3
  - pályázat, még nincs ilyen ☺ (Skein, CubeHash, ~~MD6~~, …)

Milyen algoritmust célszerű használni?

- Blokk-kódoló: AES (bármilyen kulcsméret), 3DES, Blowfish, Twofish, Serpent stb.
- Folyam-kódoló: ? (blokk-kódoló alapon)
- Nyilvános kulcsú algoritmus:
  - RSA, minimum 2048 bites kulcs
  - ECC, minimum 224 bites kulcs
- Hash függvény:
  - SHA-2 (és SHA-1, ha nagyon muszáj)

Az XYZ szervezet fel tudja törni...?

- Ha erős algoritmust használunk, a titkosítást/aláírást
  - *a tudomány mai állása szerint*,
  - *valószínűleg*

  senki nem tudja „feltörni”.
- Ezért az XYZ szervezet valószínűleg úgyis más pontokon támadná a rendszert...
  - a kulcsgondozást,
  - a használt szoftverek implementációs hibáit,
  - az emberi felhasználót,
  - a szervezeti folyamatokat,
  - ...

További információ

- Az én blogom: www.berta.hu
- e-Szignó tudásbázis: www.e-szigno.hu/?lap=tudasbazis
- Kulcsméretekkel, algoritmusokkal kapcsolatos ajánlások gyűjteményei:
  - www.keylength.com
  - ETSI TS 102 176 (ALGO paper)

MICROSEC
Számítástechnikai Fejlesztő Kft.

Hírek kriptográfiai algoritmusok biztonságáról

Dr. Berta István Zsolt <istvan.berta@microsec.hu>
K+F igazgató

Microsec Kft.