ZMNE Bolyai Kar
Informatikai és
Hírközlési Intézet
Informatikai Tanszék

Kriptográfia és biztonság

Robothadviselés 9
Tudományos Konferencia

Információbiztonság szekció

Kovács Attila, 2009. november 24.

Tartalom

1. Paradigmaváltás, információbiztonság a 21. században
2. Informatikai biztonság és kriptográfia
3. Kriptorendszerek osztályozása
4. A kriptográfia evolúciója
5. Algoritmusok
6. Mit hoz a jövő?

Társadalmi, gazdasági, kulturális paradigmaváltás ...

A biztonságos erődítménytől… ***a metropoliszig***

Zárt, izolált

Alapelv: védekezés, védelem a zónahatárokon, bizalmatlanság

Információt titkolni, adatok felhasználását korlátozni kell

Nyílt, összekapcsolt, bonyolult

Alapelv: bizalom, kreativitás, innováció, elszámoltathatóság

Információt meg kell osztani, adatok felhasználását szabályozni kell

Személyes adatok védelme

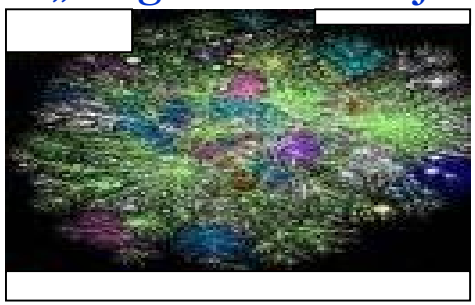
Információbiztonság a 21. században




Mobil eszközök,

Komplex, Tera bps sebességű hálózatok,

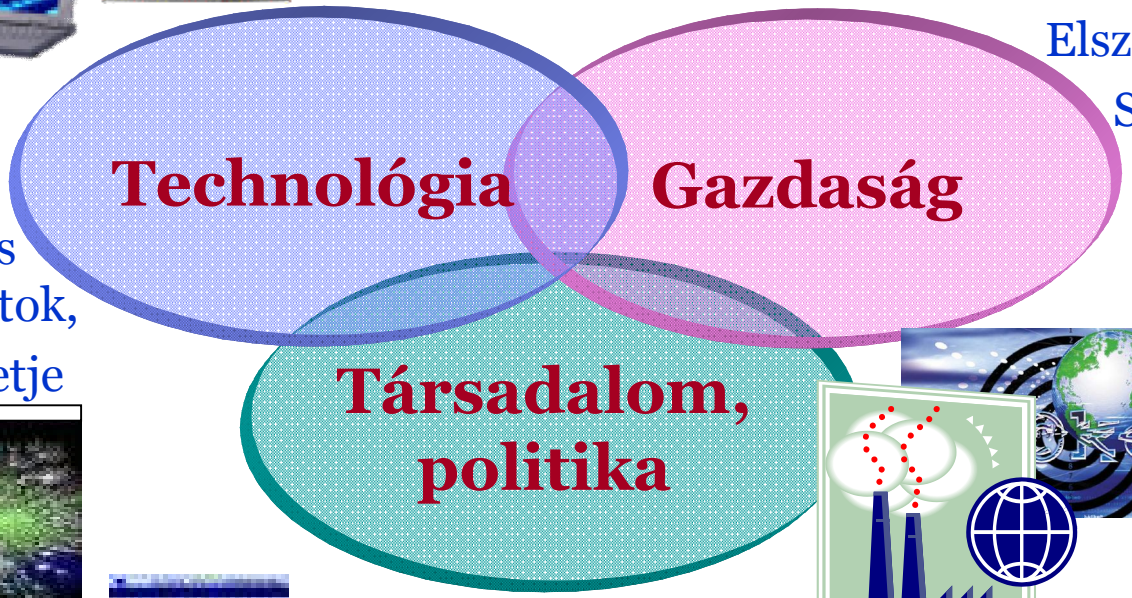
A „dolgok” internetje



Kritikus infrastruktúrák védelme,

Elszámoltathatóság,

Szolgáltatások és alkalmazások biztonsága

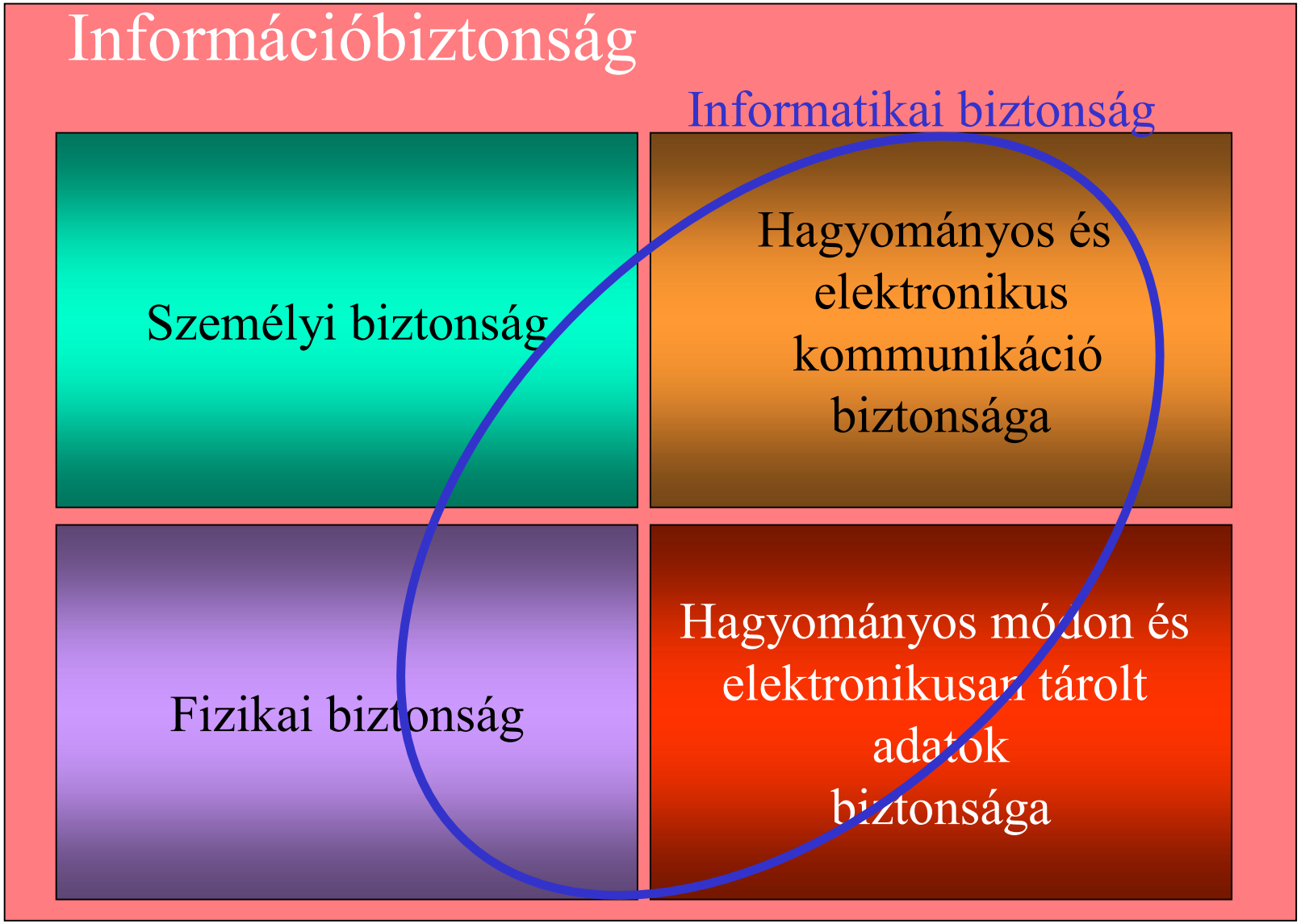


Globalizált társadalom

Állampolgár: információ-megosztás, fogyasztóvédelem, önállóság, jogorvoslat

Kormányzat: Bűn (terrorizmus) megelőzés, határellenőrzés, elszámoltathatóság, transzparencia, auditálhatóság, e-kormányzat, e-oktatás, e-egészségügy

Informatikai biztonság



Kihívások és veszélyek

Fontosabb kihívások

- Védekezés a külső/belső támadások ellen
- Védekezés az ipari kémkedés ellen
- Biztonságos elektronikus szolgáltatások
  - e-közigazgatás,
  - e-egészségügy,
  - e-kereskedelem,
  - e-bank
- Szellemi tulajdon védelme

Veszélyek

- Hálózat
- Nem biztonságos technológiák (pl. wireless)
- Érzékeny adatok tárolása
- Papírmentes társadalmi törekvés
- Emberi vonatkozások (social engineering)
- Jogi háttér

Paradigmaváltás az információ védelmében

1976 és 2009 évek összehasonlítása

1976: A kriptográfia (titkosírás) egyfajta „fekete mágia”
2009: A kriptográfia feltörekvő, népszerű tudomány
(könyvek, filmek, pl. „Da Vinci kód”)

1976 DES: Tervezési részletek titkosak (64 bites blokk, 56 bites kulcs)
2009 AES: Folyamatos, nyilvános vizsgálat
(128 bites blokkok és 128, 192, vagy 256 bites kulcsok)

1976: Szigorú exporttilalom
2009: A „legerősebb” algoritmusok is szabadon elérhetőek

Létezik „erős” algoritmus?

- Napjaink algoritmusai ~30 évig biztonságosak maradnak az ISMERT támadásokkal szemben a HAGYOMÁNYOS számítógépeken, megfelelően NAGY KULCSOK használata esetén.
- Mi történik az eddigiektől különböző támadásokkal?
- Mi az eset a kvantumszámítógépekkel?
  - A kvantum-számítógépek törik napjaink számelméleti alapokon nyugvó nyilvános kulcsú kriptográfiai algoritmusait;
- Probléma a kulcsokkal: néhány kivételtől eltekintve nincs bizonyítottan biztonságos algoritmus. Az a tény, hogy egy algoritmust nem törtek még fel, semmit nem mond annak erősségéről.

Kriptorendszerek osztályozása

- **Az algoritmus titkossága alapján**
  - Szűkebb körű
  - Általános

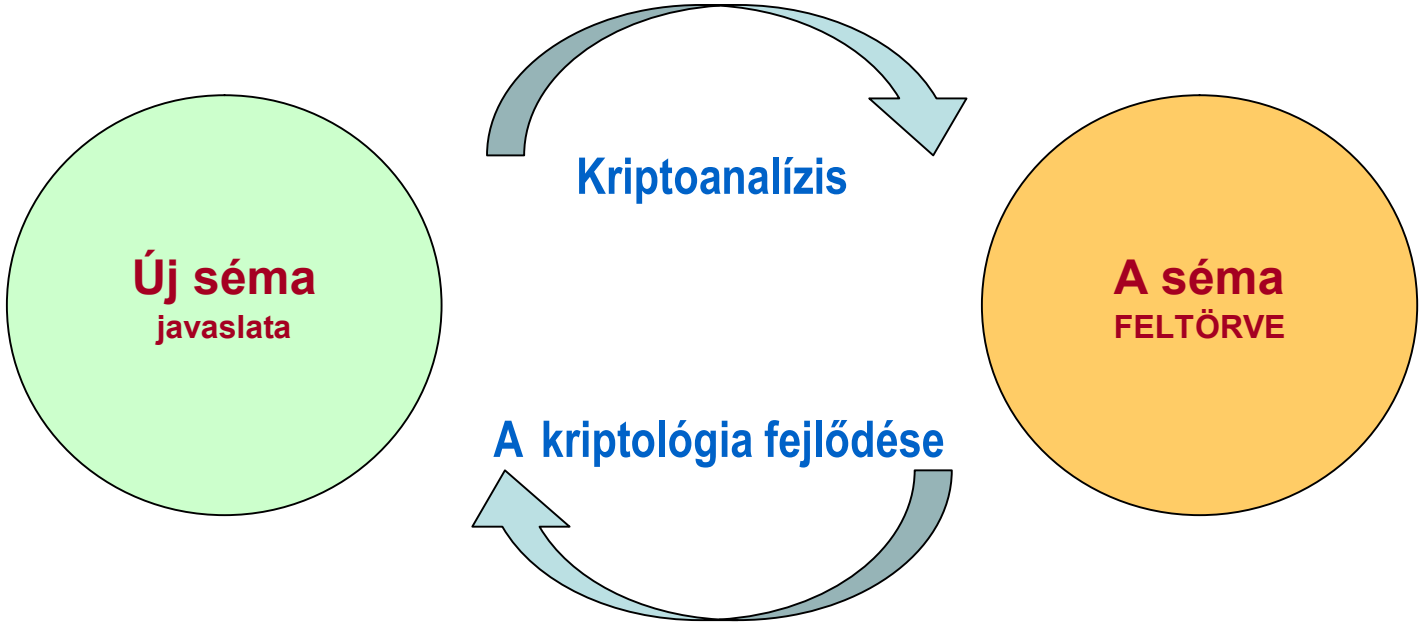
Kerckhoff-elv

- **A kulcsok száma alapján**
  - Kulcs nélküli + Egykulcsú + Kétkulcsú + Sok-kulcsú
- **Törhetőség alapján**
  - Bizonyíthatóan feltörhetetlen
  - Feltételezhetően feltörhetetlen
- **A kulcs tárolásának típusa alapján**
  - Smart-card + e-token + Windows regiszter + Fájlrendszer
- **A megvalósítás alapján**
  - Szoftver + Hardver + Szoftver ÉS hardver
- **Tanúsítvány alapján**
  - Hiteles + Nem hiteles

Kriptorendszerek elleni támadások osztályai

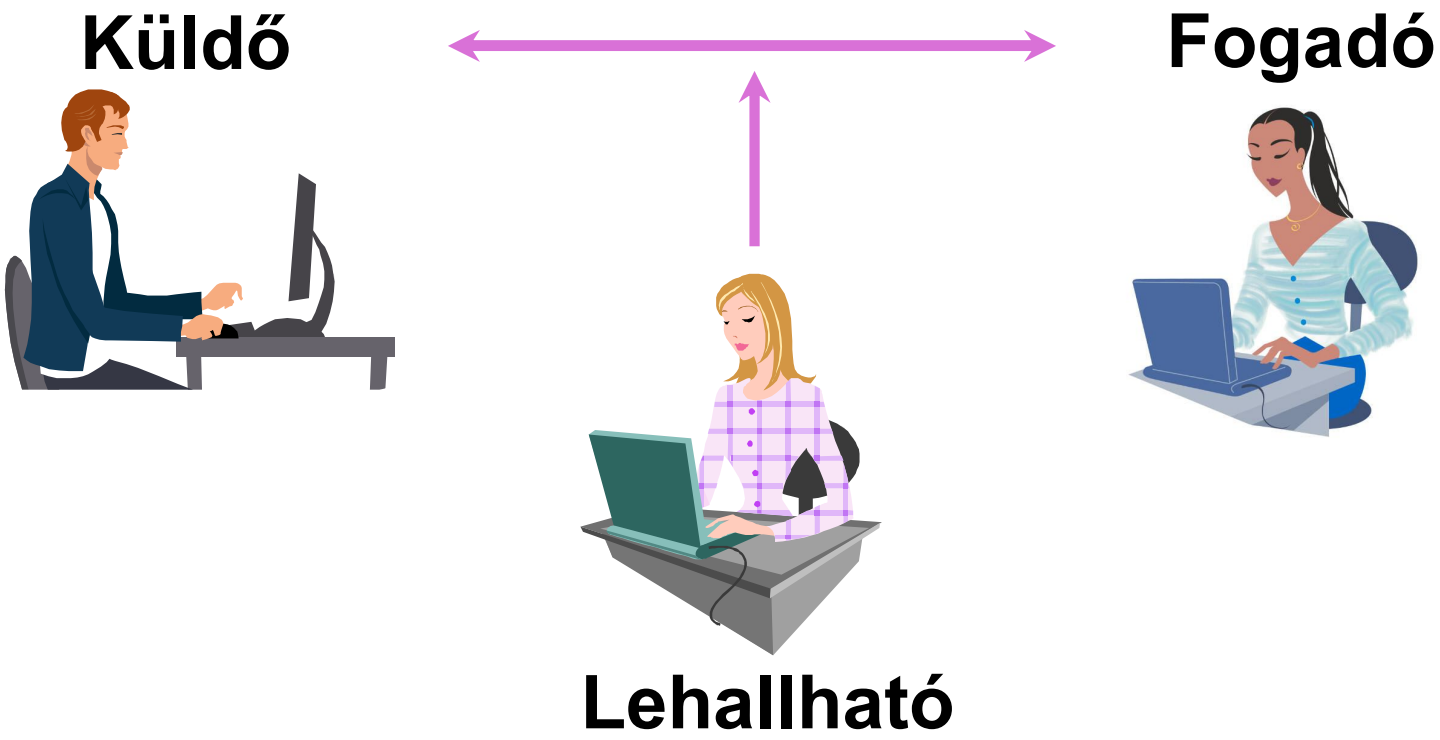
- **A nyílt szöveg és a titkosított szöveg elérhetősége alapján**
  - Csak a titkosított szöveg ismert
  - A nyílt szöveg is ismert
  - Választható nyílt szöveg
  - Side-channel
- **Az eredmény alapján**
  - Teljes törés
  - Részleges törés
- **A támadás automatizálási szintje alapján**
  - Manuális
  - Félautomatikus
  - Automatikus
- **A szükséges erőforrások alapján**
  - Tár
  - Idő
- **A következmény alapján**
  - Confidentiality
  - Integrity
  - Availability

A kriptográfia evolúciója



Vajon mi a bíráló szerepe, amikor egy új algoritmust tartalmazó publikáció bírálatára kérik fel?
Mi a helyzet akkor, ha valaki nem publikál egy lehetséges törést?
Mi lett volna, ha a 80-as években valaki töri a DES-t?

A „jó” és a „rossz”...



De kik a „jó fiúk” ?

Kriptográfia és algoritmus

"Many cryptographic systems rely on the inability of mathematicians to do mathematics".

(Donald Davies)

Egy algoritmus helyességének bizonyítása még nem garancia annak gyakorlati alkalmazhatóságára.

Az algoritmusoknak hatékonyan implementálhatónak kell lenniük.

Ami „bevált” …

- Nyilvános kulcsú kriptográfia
  - PKCS #1 v1.5 RSA
  - Diffie-Hellman, DSA (discrete logarithm)
  - elliptic curve cryptography
- Digitális aláírás
  - Aláírás és ellenőrzés
- AES, 3DES
- HMAC (Hash-based Message Authentication Code)
  - Hash (K_1 || Hash (K_2 || M))
- Shamir secret sharing
  - k of n for root keys
- Password hashing
  - Hash (password + salt)
- SSL-protected e-commerce
  - server PKI
  - session key establishment
  - session encryption
- Software codebreaking
  - distributed key search and integer factorization

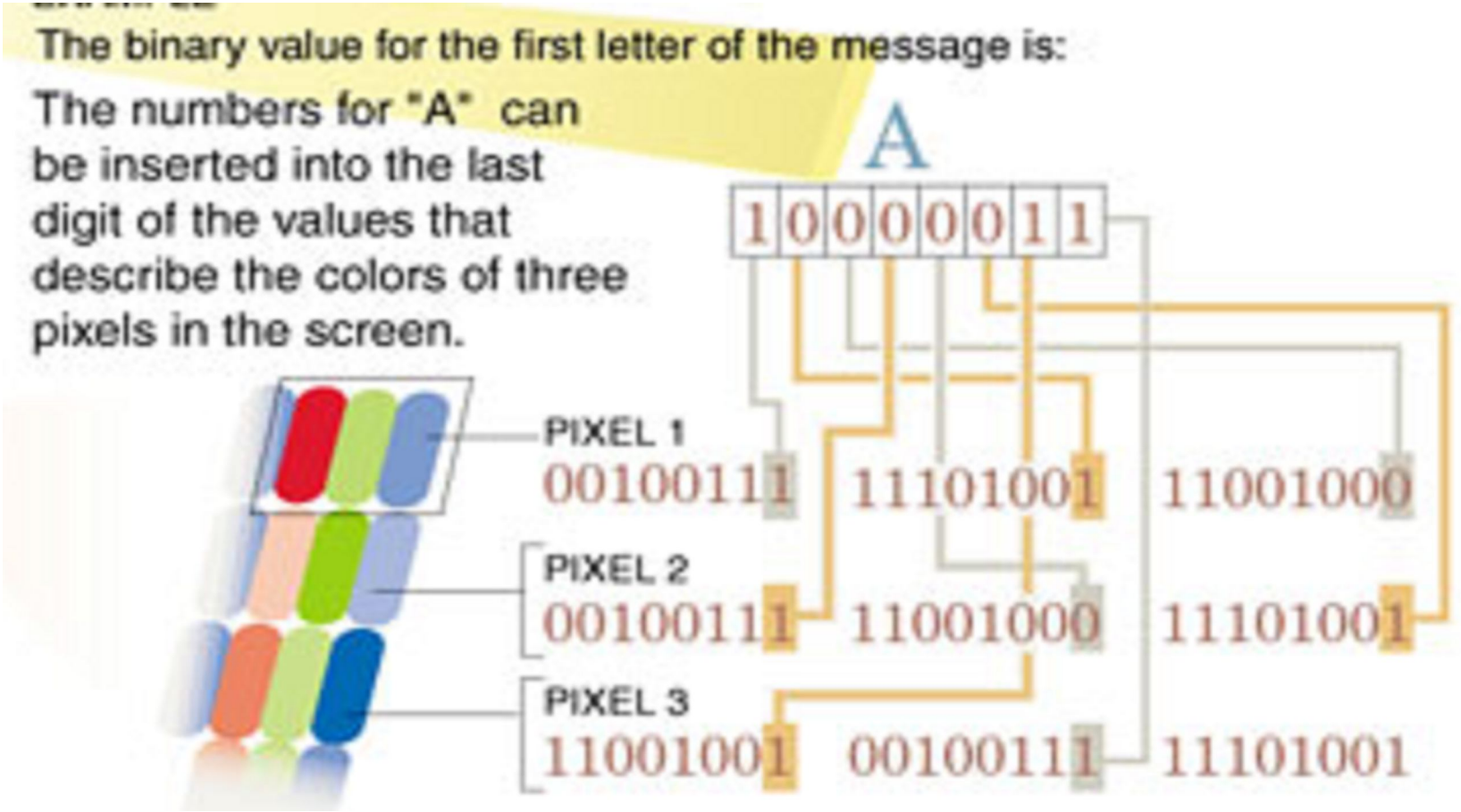
És ami nem …

- A nyilvános kulcsú alaprendszerek variánsai
  - RSA-OAEP, -PSS, -KEM
  - Cramer-Shoup schemes
    - Pedig bizonyíthatóan biztonságos …
  - Számos zéró-ismeretű verzió
- Vak aláírás
- Folyamtitkosítók (RC4 –et kivéve)
- Inkrementális MAC
- Digitális pénz
- Elektronikus aukció
- Elektronikus szavazás
- Hardware codebreaking
  - e.g., factoring circuits
  - “Deep Crack” for DES is a notable exception

A jövő?

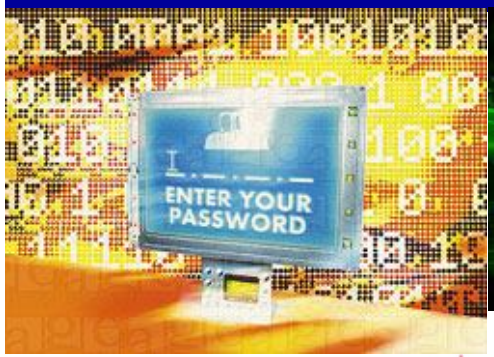
- Szteganográfia
  - Vajon mennyire nehéz detektálni?
- Quantum
  - Quantum cryptography
  - Quantum computing
- Bizonyított biztonság
  - Álom vagy valóság?

Szteganográfia



New York Times, August 3rd, 2001
http://www.nytimes.com/images/2001/10/30/science/sci_STEGO_011030_00.jpg

A 21. század internetjének biztonsági kihívásai



- Számítás
- Adattárolás
- Kommunikáció

Komponensek és tranzakciók trilliói, adatok zetta bájtja

- Skálázhatóság
- Megbízhatóság
- Rugalmasság

Személyes adatok védelme, Biztonságos szolgáltatások

Fenyegetések

- Újszerű használat => Új fenyegetések
  - Masszívan sok-felhasználós alkalmazások
  - 500 Mega számítógép, 3 Giga felhasználó, 1 tera objektum (A biztonság nem skálázható…)
  - Hatalmas mennyiségű multimedia tartalom, virtuálisan elosztott szolgáltatások (nyomon követhetőség)
  - Szenzorhálózatok
  - Kritikus infrastruktúrák
- Lényeges fenyegetések => Illetéktelen számítógép programok
  - A támadó lehetőségei :
    - Óriási számítási kapacitás
    - Lehetőség van csatlakozni és megzavarni az elosztott fizikai hálózatot (kiberterrorozmus)
    - Szervezett kiberbűnözés

Sérülékenységek

- Új architektúra => új sérülékenység
  - Számítás + adattárolás + kommunikáció
    - Személyek és objektumok azonosítása komoly kihívás
    - Erőforrás-megosztás
    - Mobilitás (nyomon követhetőség)
- Nagyobb hálózati komplexitás, nagyobb absztrakció
  - Core hálózat
    - Hogy titkosítsunk 100Gbits/s sávszélességen?
  - Access hálózat
    - Illetéktelen és kártékony programok
  - Wireless technológiák

Támadási lehetőségek

- Támadás a felhasználók kooperációja által
  - A felhasználók elvesznek a dinamikus struktúrák, elosztott alkalmazások rengetegében
  - Az egyszerű felhasználók rászedhetők
- Botnet támadás
- Illetéktelen tartalom propagálása
  - copyright visszaélés
  - Illegális tartalom szteganográfiával
- Kiberháború
  - IT infrastruktúra blokkolása
  - Dezinformáció, vélemény-manipulálás
- Kiberterrorizmus
- Személy elleni támadás
  - Azonosító-lopás, illegális bankolás, stb.