Informatikai biztonság alapjai

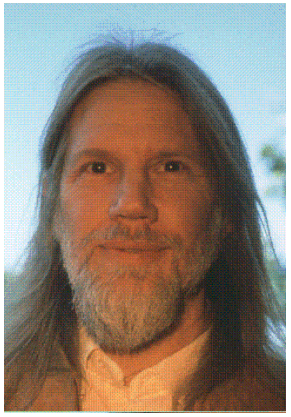
4. Algoritmikus adatvédelem

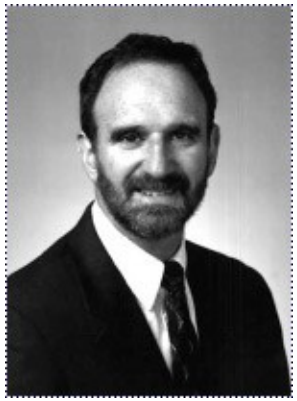
Pethő Attila

2008/9 II. félév

A digitális aláírás felfedezői

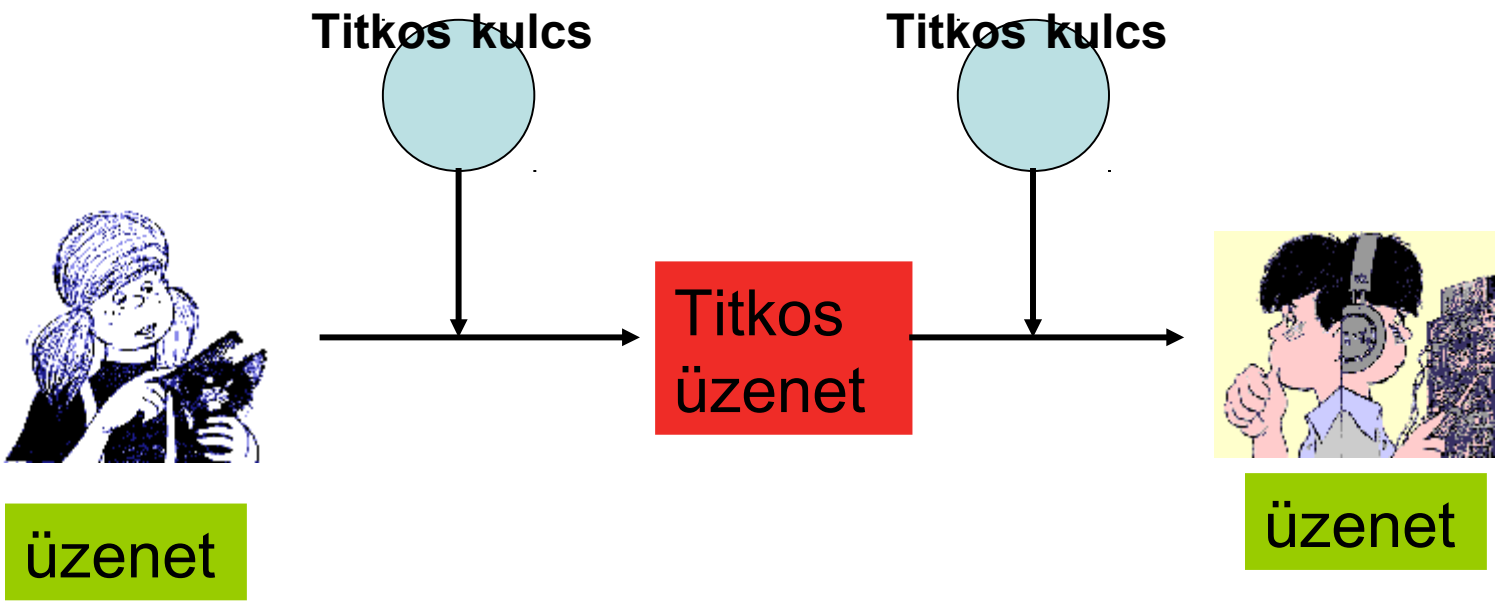
Dr. Whitfield Diffie és Martin E. Hellman (1976) a nyilvános kulcsú titkosítás elvének megfogalmazói.





Ralph C. Merkle (1979)

Titkos kulcsú vagy szimmetrikus titkosítás

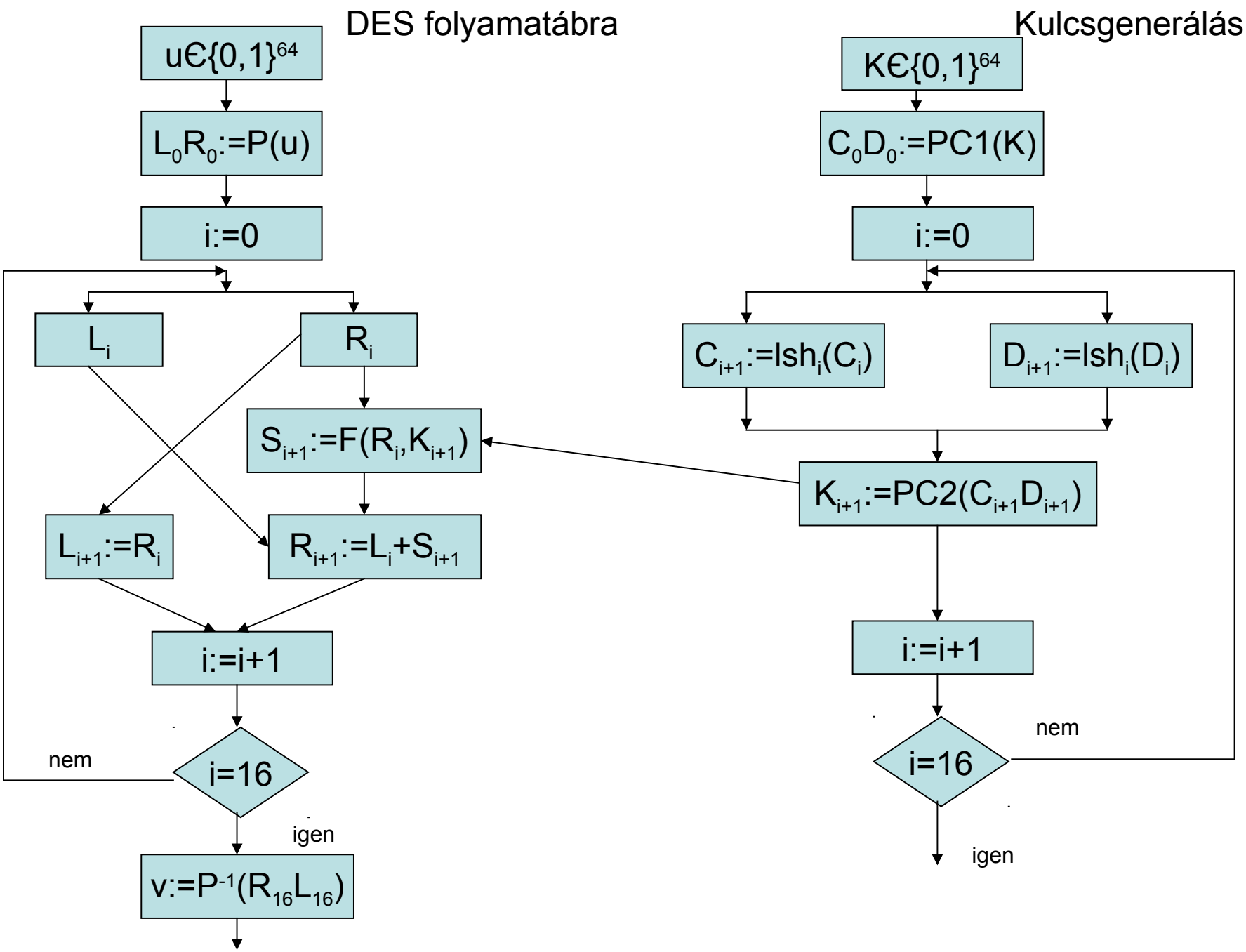


- Egy közös kulcs a titkosításhoz és a megfejtéshez.
- A kulcs
  - közös generálása vagy
  - kicserélése
  - tárolása

  gondot jelent.
- Nagyon gyors és elterjedt.
- DES (1976), TDES, AES (2000)

DES

- Data Encryption Standard
- 1973-ban tervezte Horst Feinstel az IBM mérnöke.
- 1976-óta USA szabvány.
- Legtöbbet használt titkosító algoritmus.
- 64 bites bináris szavakat kódol formailag 64 bites kulccsal.
- A kulcs effektív része 56 bites, mert minden 8. bit paritásellenőrzésre szolgál.


DES folyamatábra
Kulcsgenerálás
u∈{0,1}64
L0R0:=P(u)
i:=0
Li
Ri
Si+1:=F(Ri,Ki+1)
Li+1:=Ri
Ri+1:=Li+Si+1
i:=i+1
i=16
nem
igen
v:=P-1(R16L16)
K∈{0,1}64
C0D0:=PC1(K)
i:=0
Ci+1:=lshi(Ci)
Di+1:=lshi(Di)
Ki+1:=PC2(Ci+1Di+1)
i:=i+1
i=16
nem
igen

DES algoritmus paraméterei

- P bitenkénti permutáció, P^{-1} a P inverze,
- F egy 32 és egy 48 bites szóból S-boxok felhasználásával 32 bites szót képez,
- + bitenkénti xor művelet,
- PC1 eltávolítja a paritásbiteket és összekeveri a maradékot,
- lsh_i balshift 1 vagy 2 pozícióval, i-től függően,
- PC2 megadja a 48 bites aktuális kulcsot.

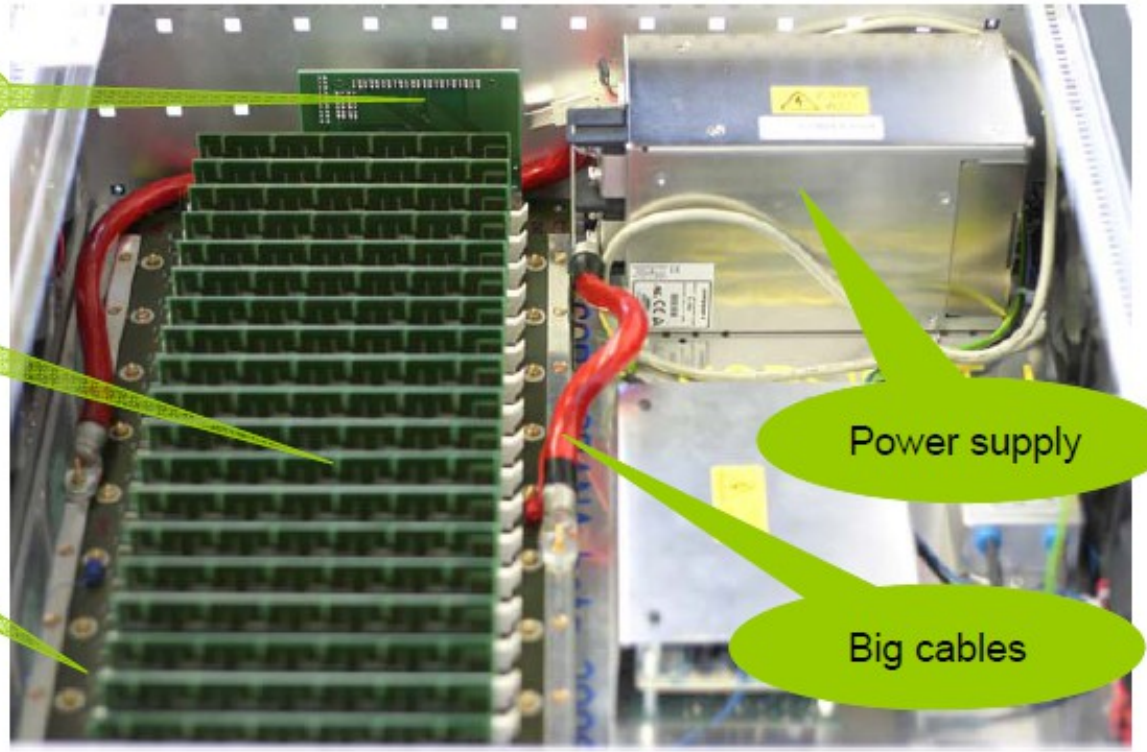
DES feltörése

- COPACOBANA: Now, the average search time for a single DES key is **less than a week**, precisely 6.4 days. The worst case for the search has been reduced to 12.8 days now.

  (Horst Görtz Institute for IT Security)

COPACOBANA: What's inside?

hg
Horst-Görtz Institu
für IT Sicherhe



Scales easily:

- 20 FPGA modules/machine (120 FPGAs/ machine)
- multiple machines via USB/ Ethernet

TDES

- A DES 56 bites kulcsa ma már nem elég biztonságos.
- Három DES-t alkalmaz egymás után az input szóra.
- A kulcshossz 168 bit.

AES

- Advanced Encryption Standard
- A NIST (National Institute of Standard and Technology) 1997-ben felhívás új szimmetrikus titkosító szabványra.
- 2000-ben eredmény: győztes Rijndael, alkotói Vincent Rijmen és Joan Daemen.
- 128/192/256 bites blokkokat 128/192/256 bites kulccsal titkosít, minden párosításban.

AES 128 kódolása

- A 128 bites input szót 16 bájtra bontja és ezeket egy 4x4-es táblázatba rendezi, amelyet állapotnak (state) nevez.
- Az állapotra 9 teljes és egy részleges fordulóban 4 függvényt alkalmaz.
- 11 menetkulcsot generál a mesterkulcsból.

AES függvényei

- ByteSub(State): az állapot minden bájtját kicseréli egy S-box által meghatározott bájtra. Az S-boxot matematikai függvényként is ki lehet számítani.
- ShiftRow(State): az állapot i-dik sorát i-1 pozícióval balra tolja.
- MixColumn(State): az állapot oszlopait, mint vektorokat megszorozza egy mátrixszal.
- AddRoundKey(State, RoundKey): bitenkénti xor az aktuális állapot és a menetkulcs között.

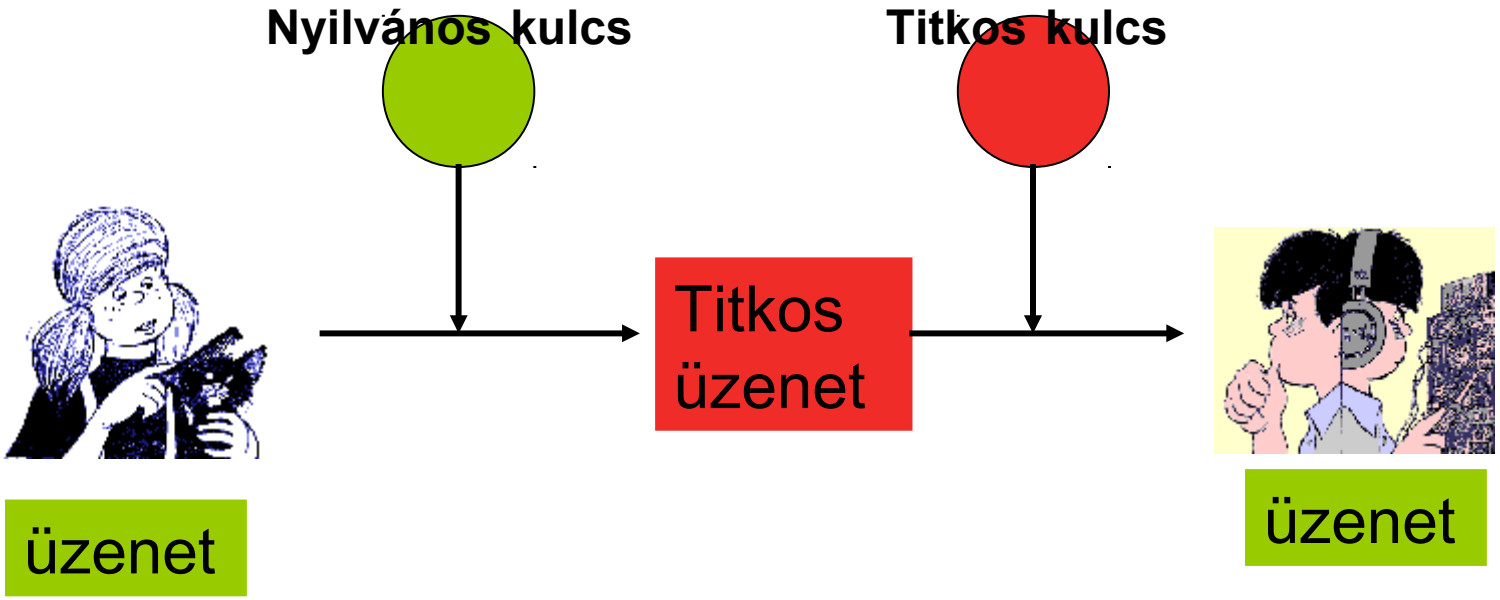
Az AES vérehajtása

- Jelölés: ByteSub=B, ShiftRow=S, MixColumn=M, AddRoundKey=A.
- Az algoritmus folyamata:

A BSMA BSMA BSMA BSMA BSMA

BSMA BSMA BSMA BSMA BSA

Nyilvános kulcsú vagy asszimmetrikus titkosítás



A megfejtő kulcsot csak az üzenet címzettje ismerheti,
de a hozzá tartozó kódoló kulcsot bárki tudhatja.

Egyirányú és egyirányú csapóajtó függvény

- **Egyirányú függvény:** Olyan, amelyet „könnyű” kiszámítani, de csak a függvényt kiszámító algoritmust és a függvényértéket ismerve „nehéz” invertálni.
- **Egyirányú csapóajtó függvény:** Olyan egyirányú függvény, amely „könnyen” invertálható külön ismeret birtokában.
- Példa egyirányú függvényre: telefonkönyv

Vannak-e egyirányú csapóajtó függvények?

- Nem tudjuk a létezésüket matematikai eszközökkel bizonyítani.
- Igen, vannak a gyakorlatban megbízhatónak bizonyuló egyirányú csapóajtó függvények.
  - **RSA:** melynek biztonsága azon alapul, hogy ha $m=pq$, ahol p és q prímszámok, e és y adottak, akkor az

    $$y \equiv x^e \pmod m$$

    kongruenciából az x „nehezen” határozható meg.
  - **ElGamal**: legyen p prímszám, $0<g<p-1$ olyan, hogy $\{g^0, g^1, \ldots, g^{p-2}\} = \{1,2,\ldots,p-1\}$. Ha y adott, akkor meghatározandó x, amelyre $g^x \bmod p = y$.

RSA

- Ronald Rivest, Adi Shamir és Leonard Adleman publikálta 1977-ben.
- Leggyakrabban használt aszimmetrikus vagy nyílt kulcsú titkosító algoritmus.
- A biztonsága azon alapul, hogy nagy számokat nagyon nehéz prímszámok szorzatára bontani.

RSA paraméterek

Legyenek:

- p,q prímszámok, $n=pq$, $\varphi(n)=(p-1)(q-1)$,
- $1<e,d<\varphi(n)$ olyanok, hogy $ed \bmod \varphi(n)=1$.

- n és e a nyilvános kulcsok,
- d a titkos kulcs.

RSA kódolás és dekódolás

- Legyen $0 \leq x < n$, akkor a kódolás
- $y = RSA(x) := x^e \bmod n$.
- Ezt a nyilvános kulcs (n,e) ismeretében bárki ki tudja számítani.

Ha x és n legnagyobb közös osztója 1, ami nagyon valószínű, akkor a dekódolás:

- $RSA^{-1}(y) := y^d \bmod n$.
- Ezt csak az tudja kiszámítani, aki d-t ismeri.

RSA paraméterek választása

- p,q legalább 512 bit nagyságú prímszámok, amelyek különbsége legalább 500 bites.
- n és φ(n) kiszámítása kézenfekvő.
- e-t véletlenszerűen választhatjuk vagy legyen 17,
- e és φ(n) ismeretében d-t kibővített euklideszi algoritmussal lehet meghatározni.

Összehasonlítás

	Kulcsméret	Sebesség(kulcs-méret)	Haté-konysá g	Kulcs tárolás
Szimmetrikus: DES, TDES, AES, …	64(56), 112, 128/192/256	~kulcshossz	1	nincs
Aszimmetrikus : RSA, ElGamal, …	1024/2048, 512/1024	~kulcshossz^3	1000	Amíg nem kompromit-tálódik.

Összehasonlítás

	Előny	Hátrány
Szimmetrikus: DES, TDES, AES, …	Közérthető, Egyszerű programozni, Rövid kulcshossz, Gyors	Legalább két személy a titokgazda, A kulcsot rövid ideig lehet tárolni, Kulcscsere.
Aszimmetrikus: RSA, ElGamal, …	Matematikai eszközökkel elemezhető, Egy személy a titokgazda! A kulcs tárolható. Nyilvános/titkos kulcs	Lassú, Komplikált, Nehéz programozni.

Mit is jelent az aláírás?

- **Új Magyar Lexikon** (1961): nincs ilyen címszó
- **Magyar Nagylexikon** (1993): magán-, ill. közokirat hitelességének a bizonyítéka. Magánokiraton tanúsítja, hogy az aláíró a nyilatkozatot megtette, elfogadta, magára nézve kötelezőnek ismerte el.

Szent István aláírása

Törvényi szabályozás

- 2001. szeptember 1-én hatályba lépett a 2001. évi XXXV. törvény az elektronikus aláírásról.
- ***Elektronikus aláírás****:* elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

- Hagyományos aláírás
  - fizikai dokumentum részét képezi
  - több oldalas dokumentum minden oldalát alá kell írni
  - ellenőrzése egy hiteles aláírási minta alapján történik
  - aláírt dokumentum fénymásolata megkülönböztethető az eredetitől
- Digitális aláírás
  - hozzácsatolódik az elektronikus dokumentumhoz
  - hosszabb dokumentumnál elég egyszer aláírni
  - nyilvános ellenőrző algoritmus
  - az aláírt üzenet könnyen másolható

Elektronikus aláírások

- **Elektronikus aláírás**:
  elektronikus formájú aláírás, legtágabb kör (pl. begépelt név, digitális toll)

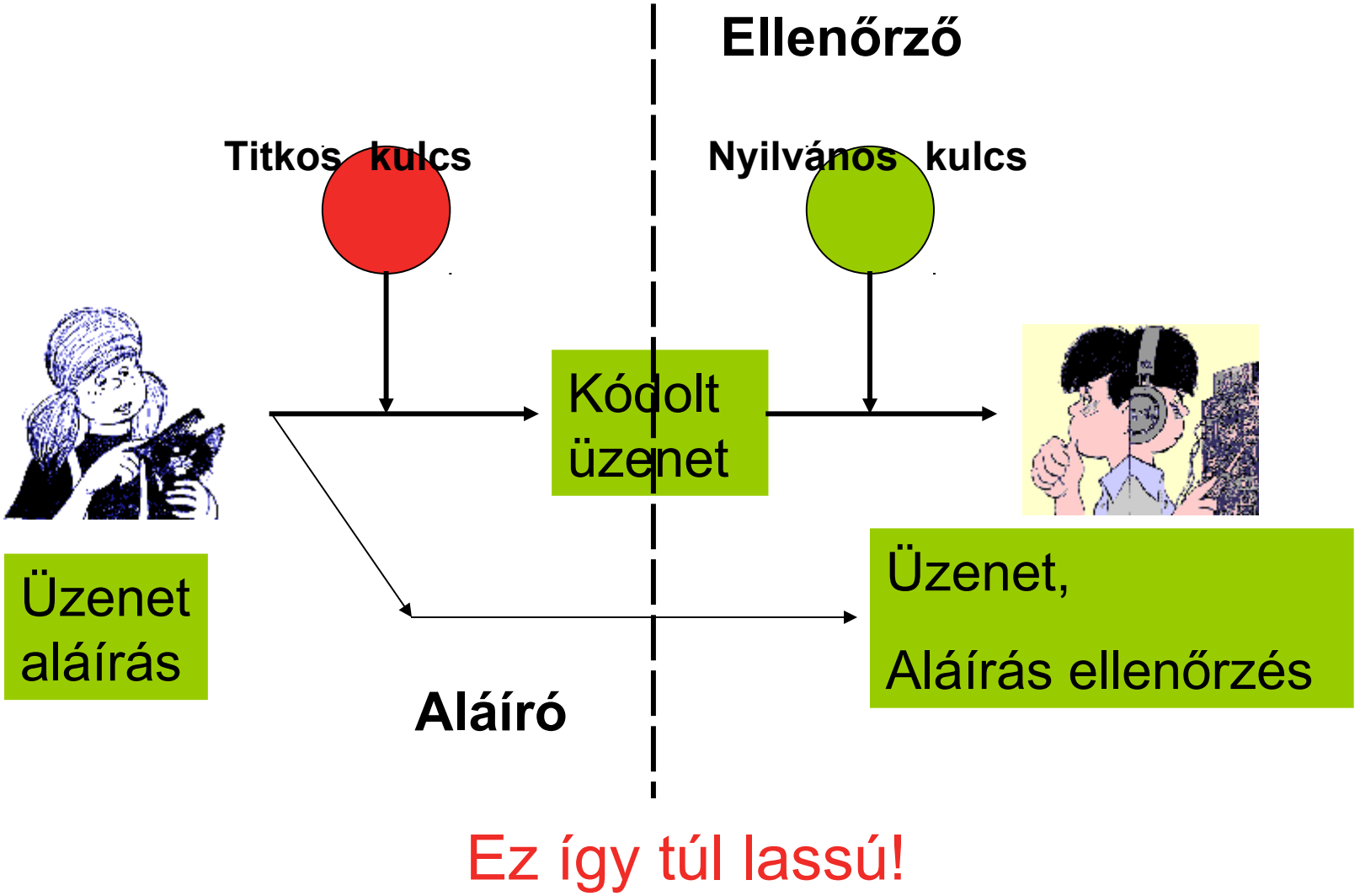
- **Fokozott biztonságú elektronikus aláírás**:
  "elektronikus aláírás, amely megfelel a következő követelményeknek:
  - Alkalmas az aláíró azonosítására, és egyedülállóan hozzá köthető,
  - Olyan eszközzel hozták létre, mely kizárólag az aláíró befolyása alatt áll,
  - A dokumentum tartalmához olyan módon kapcsolódik, hogy minden - az aláírás elhelyezését követően az iraton, illetve dokumentumon tett - módosítás érzékelhető

- **Minősített elektronikus aláírás**: "olyan - fokozott biztonságú - elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából *minősített tanúsítványt* bocsátottak ki"

Digitális aláírás jellemzői

- Üzenet eredetének letagadhatatlansága
- Üzenet adatintegritása
- Hitelesség
- Hamisíthatatlan
- Az aláírt üzenet kivonat nem használható fel újra

A digitális aláírás elve

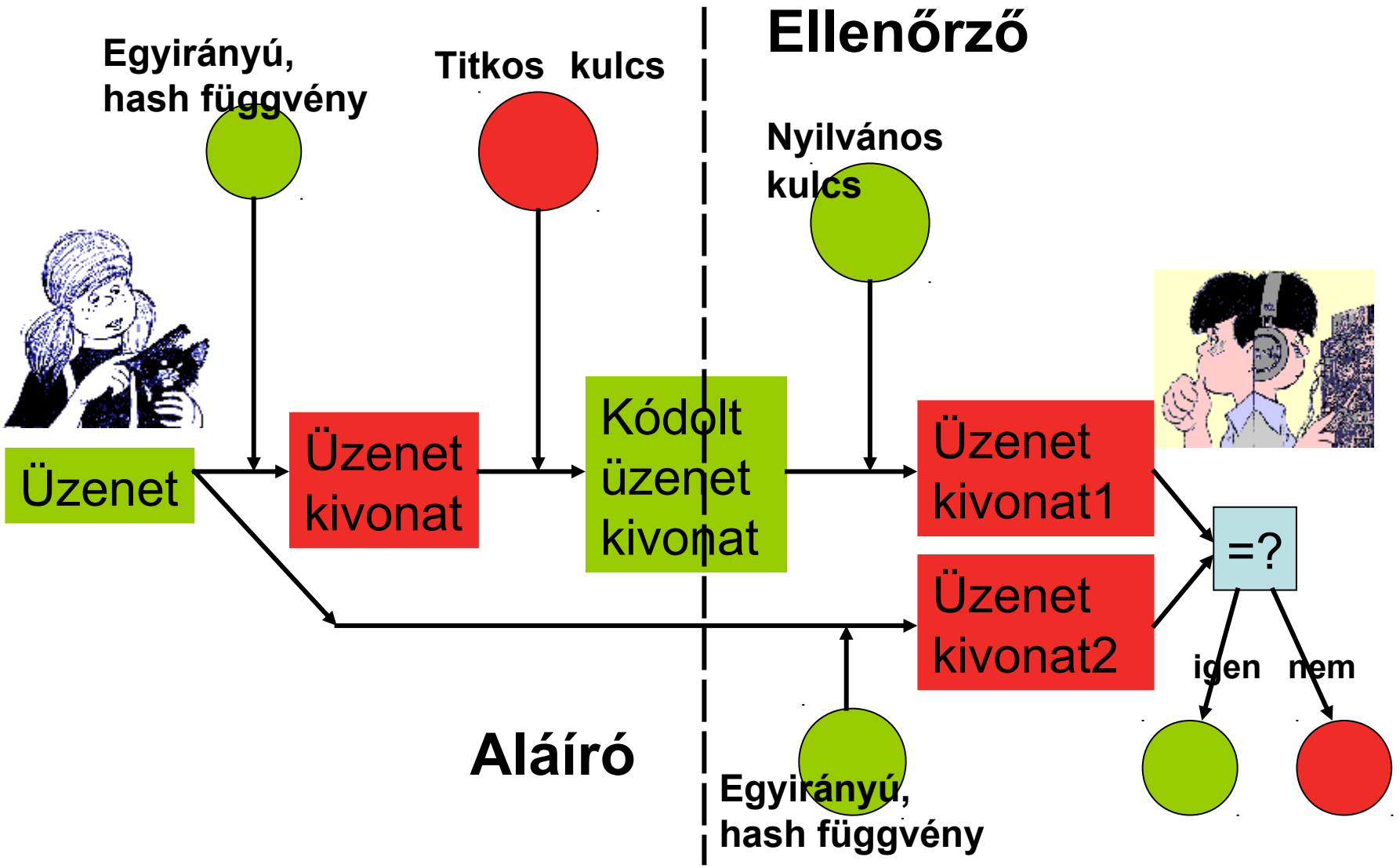


Ez így túl lassú!

Digitális aláírás aszimmetrikus titkosítással

- Az aszimmetrikus titkosítás használható digitális aláírásra, mert
  - a titkos kulcs azonosítja a tulajdonosát,
  - a dokumentum módosítása a kódolt változat dekódolásakor kiderül,
  - a titkosított dokumentum nem módosítható
  - Különböző dokumentumoknak, különböző az aláírt változata is.

A digitális aláírás labormodellje



- Ez így már elfogadhatóan gyors, de…
- Aladár nem lehet biztos abban, hogy Kriszta nyilvános kulcsa tényleg hozzá tartozik.
- Kell tehát erre egy igazolás, amelyet egy hitelesítő szervezet (Certification Authority, CA) ad ki.
- Erre Krisztának is szüksége van, hogy hamisítás esetén bizonyítani tudja az igazát.

A digitális aláírás a gyakorlatban 1.

CA, adatbázis

Kriszta1, nyilvános kulcs, lejárat,…

Aladár1, nyilvános kulcs, lejárat,…
Kriszta2, nyilvános kulcs, lejárat,…
Aladár2, nyilvános kulcs, lejárat,…
Kriszta3, nyilvános kulcs, lejárat,…
Aladár3, nyilvános kulcs, lejárat,…
.
.

A digitális aláírás a gyakorlatban 2.

Aláírt dokumentum

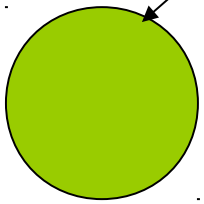
Nyilvános kulcs lekérdezése

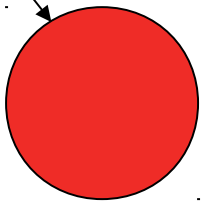
CA

Aláírás ellenőrzés

Igen

Nem





Mivel és hol írjuk alá a dokumentumokat?

- Nem tollal! Vagy ha igen, akkor a tollnak legalább annyit kell változnia, mint a lúdtollnak a mai írószerszámokhoz képest.
- A ***digitális tollnak*** elég nagy számítási teljesítménnyel kell rendelkeznie, de ne legyen mások számára elérhető és vihessük mindig magunkkal.
- *Megoldási javaslat* (nem az enyém): a privát kulcsot az aláíró algoritmussal helyezzük el egy aktív memória kártyán vagy egy penn-drive-on.

RSA aláírás I.

Kulcsgenerálás

- p és q két nagy prím
- $n := p \cdot q$
- $1 < e < \varphi(n)$, $(e, \varphi(n)) = 1$ választása,
- $e \cdot d \equiv 1 \pmod{\varphi(n)} \rightarrow d$ meghatározása

Titkos információk: p,q,d

d: aláíró kulcs

Nyilvános kulcs: n,e

e: ellenőrző exponens

RSA aláírás II.

m üzenet, *H* ütközésmentes hash függvény

Aláírás folyamata

- lenyomat készítése: $H(m)$
- aláírás generálás: $[H(m)]^d \equiv s \pmod{n}$

Ellenőrzés

- (m,s) elküldése
- $H(m)$ kiszámítása
- $s^e \bmod n$ kiszámítása

} Ha megegyeznek, akkor az aláírás érvényes

Gyakorlati alkalmazások

- hivatalos okiratok aláírása (adóbevallás, cégeljárás, ügyvédi ellenjegyzés, közigazgatási hatósági eljárás, elektronikus számlázás, vizsgalejelentések)
- időbélyegzés
- vak aláírás (elektronikus szavazások, elektronikus pénz)
- online nyereményjátékok (Puttó)
- kód aláírás
- partner-azonosítás

Időbélyegzés 1.

Bizonyítja, hogy

- elektronikus dokumentum egy adott időpontban már létezett
- adott időpont után nem változott meg

Alkalmazhatóság:

- elektronikus aláírások
- elektronikus dokumentumok adott időben való létezésének és annak sértetlenségének igazolása

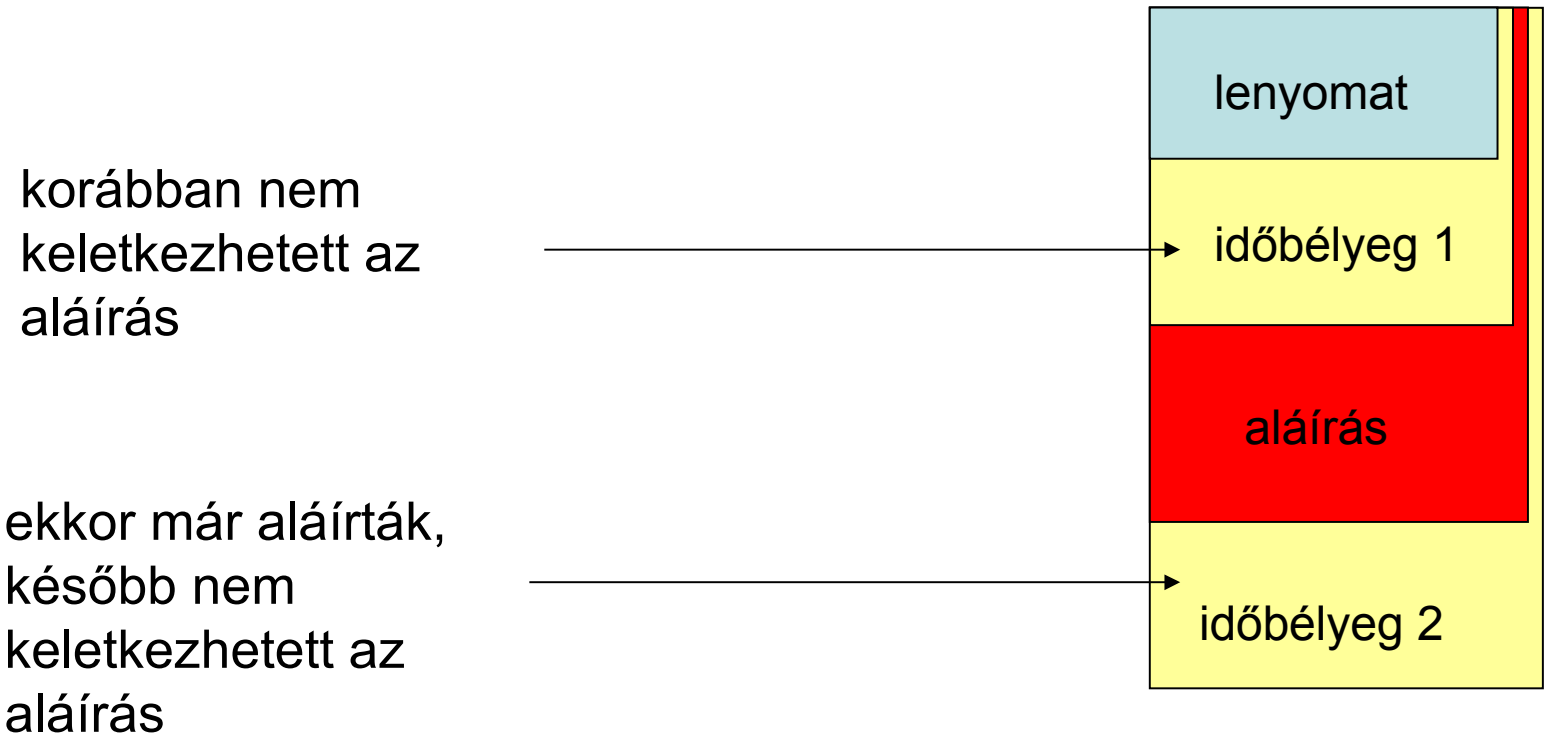
Időbélyegzés 2.

Az időbélyegzés folyamata:

- Véglegesítjük az adott dokumentumot
- Megfelelő program segítségével elkészül az adott dokumentum lenyomata
- A lenyomatot a program elküldi az Időbélyegző Szolgáltatónak
- Az Időbélyegző Szolgáltató elkészíti az időbélyeget, aláírásával hitelesíti azt, és visszaküldi a programnak
- A program csatolja a dokumentumhoz az időbélyeget

Elektronikus aláírás időbélyegzése

Amennyiben pontos időpontot, vagy időintervallumot kívánunk megadni, akkor összesen két időbélyegre van szükség.



Vak aláírások

Aladár

Hitelesítő Szervezet

- véglegesíti a dokumentumot
- belehelyezi egy átlátszatlan, indigós borítékba
- lezárja a borítékot és elküldi aláírásra

- aláírja a lezárt borítékot és visszaküldi a feladónak

- kiveszi a borítékból a dokumentumot
- az aláírás ellenőrizhető

Nem tudja mit írt alá!!

A Hitelesítő Szervezet hitelesen aláírja a dokumentumot anélkül, hogy ismerné annak tartalmát.

RSA vak aláírás I.

Kulcsgenerálás

- p és q két nagy prím
- $n:=p \cdot q$
- $1< e <\varphi(n)$ választása
- $e \cdot d \equiv 1 \pmod{\varphi(n)} \rightarrow d$ meghatározása

Titkos információk: p,q,d

d: aláíró kulcs

Nyilvános információk: n,e

e: ellenőrző kulcs

RSA vak aláírás II.

A „vakított” üzenet létrehozása

- *m’* eredeti üzenet
- Alice választ egy b$\in Z_n$ „vakító” értéket
- $m \equiv b^e \cdot H(m') \pmod n$
- *m* elküldése

Aláírás folyamata

- $s \equiv m^d \pmod n$
- *s* visszaküldése

Aláírt eredeti üzenet kiszámítása

- $s' \equiv s \cdot b^{-1} \pmod n$
- *s’* az eredeti üzenet hiteles aláírása

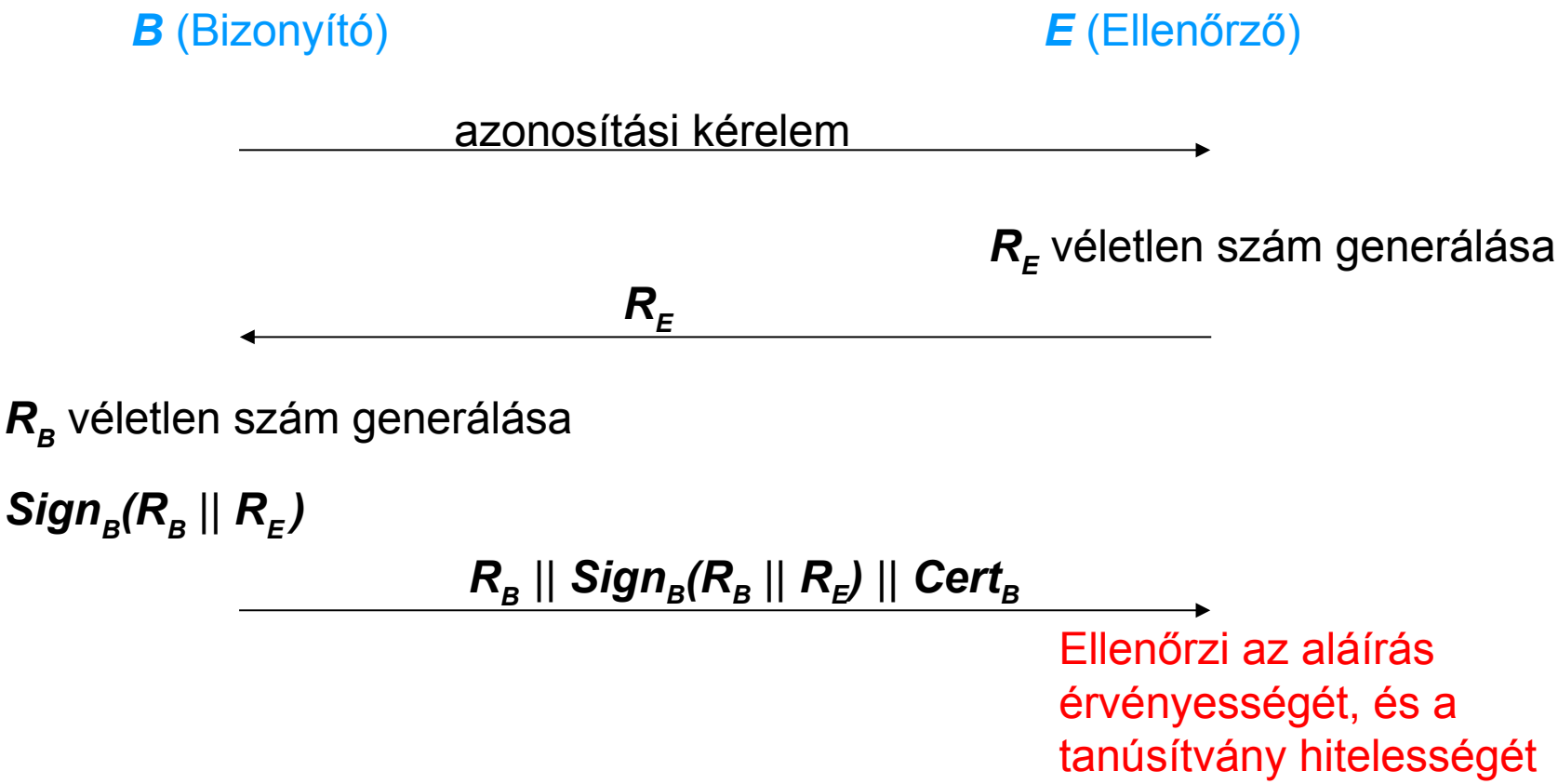
RSA vak aláírás III.

Aláírás ellenőrzése:

$$(s')^e \equiv ((sb)^{-1})^e$$
$$\equiv ((m^d b)^{-1})^e$$
$$\equiv m^{de} b^{-e}$$
$$\equiv m b^{-e}$$
$$\equiv b^e H(m') b^{-e}$$
$$\equiv H(m') \pmod{n}$$

Partner-azonosítás

Egy véletlen érték titkos kulccsal történő digitális aláírása



Nyilvános kulcs infrastruktúra, hitelesítő szervezetek.

Nyilvános kulcs infrastruktúra

- Alkalmazásai
- Jogi háttér
- Tanúsítványok
  - Típusai
  - Felépítése

A nyilvános kulcs infrastruktúra alkalmazásai

- Elektronikus ügyintézés
- Elektronikus számlázás
- Elektronikus levelezés
- Elektronikus közzététel
- Elektronikus bizonylatmegőrzés
- Partnerazonosítás az interneten:
  - Banki ügyintézés
  - Vásárlás

Jogi háttér

- Törvény az elektronikus aláírásról.
- Törvény az elektronikus számlázásról.
- Elektronikus bizonylatmegőrzés.
- Hírközlési hatóság irányelvei.

A tanúsítvány felépítése

```
Certificate:
   Data:
       Version: 3 (0x2)
       Serial Number: 1 (0x1)
       Signature Algorithm: md5WithRSAEncryption
       Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
               OU=Certification Services Division,
               CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Validity
           Not Before: Aug  1 00:00:00 1996 GMT
           Not After : Dec 31 23:59:59 2020 GMT
       Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/emailAddress=server-certs@thawte.com
       Subject Public Key Info:
           Public Key Algorithm: rsaEncryption
           RSA Public Key: (1024 bit)
               Modulus (1024 bit):
                   00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:
                   68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:
                   85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:
                   6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:
                   6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:
                   29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:
                   6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:
                   5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:
                   3a:c2:b5:66:22:12:d6:87:0d
               Exponent: 65537 (0x10001)
       X509v3 extensions:
           X509v3 Basic Constraints: critical
               CA:TRUE
   Signature Algorithm: md5WithRSAEncryption
       07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:
       a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:
       3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:
       4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:
       8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:
       e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:
       b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:
       70:47
```

Aláírások típusai

- Egyszerű elektronikus aláírás
- Fokozott biztonságú elektronikus aláírás
- Minősített elektronikus aláírás

A PKI szolgáltatók felépítése

- Hitelesítő hivatal
- Regisztrációs hivatal
- Tanúsítványtár

Tanúsítványok életciklusa

- A tanúsítvány kiadása
- A tanúsítvány használata
- A tanúsítvány visszavonása