# Kriptográfia

## Tizenegyedik előadás
## Digitális aláírások,
## kölcsönös és egyirányú hitelesítés, a DSA

Dr. Németh L. Zoltán
SZTE, Számítástudomány Alapjai Tanszék
2008 ősz

# Elektronikus aláírás vagy digitális aláírás?

Az Elektronikus aláírás tv. indoklása tartalmazza, hogy az elektronikus aláírás fogalomba beletartozik az a mindenfajta technológiai biztonságot nélkülöző eljárás is, amikor az aláíró egy elektronikus szöveg végére odaírja a nevét vagy más azonosítóját. Ezek nem minősülnek fokozott biztonságú elektronikus aláírásnak. Ezt a kört nevezik "egyszerű elektronikus aláírásnak" is. Az elektronikus aláírás fogalmába a fentieken túl természetesen beletartoznak a fokozott biztonságú és a minősített elektronikus aláírások is.

A nyílt kulcsú infrastruktúrán alapuló elektronikus aláírást digitális aláírásnak is szokták nevezni.

(Fogalomtár)

# Digitális aláírások (Digital Signatures)

- eddig foglalkoztunk a hitelesítéssel
  - ami biztosítja a feleket egy harmadik támadótól
  - de **nem védi meg őket egymástól,** a kommunikáció a kölcsönös bizalomra épült
- a digitális aláírás a hagyományos aláíráshoz hasonlóan erre is képes, sőt a hanyományos aláírástól eltérően nem az üzenet hordozójához (a papírhoz), hanem magához az üzenethez kötődik, pl. másolható, több példányban létezhet.
- a nyilvános kulcsú kriptográfia az alapja, nélküle igen nehezen megvalósítható biztonsági feladatokat (pl. letagadhatatlanság) lát el.

# A digitális aláírás feladatai

1. azonosítsa a dokumentum szerzőjét, és ellenőrizhető legyen az aláírás ideje
2. hitelesítse az üzenet tartalmát (az aláírás pillanatában)
3. harmadik fél által ellenőrizhető legyen a felek közti viták igazságos eldöntése végett

Tehát a hitelesítés funkcióján túl további szolgáltatásokat tartalmaz

# A digitális aláírás tulajdonságai

Ezek alapján a digitális aláírás olyan bitsorozat legyen, mely

1. függjön az aláírt üzenettől
2. a szerzőre jellemző egyedi információra épüljön
   - hogy védjen a hamisítástól és a letagadástól is
3. egyszerűen elkészíthető legyen
4. egyszerűen felismerhető és ellenőrizhető legyen
5. reménytelenül sok számításba tartson hamisítani
   - új üzenetet készíteni meglévő aláírásoz
   - vagy hamis aláírást készíteni adott üzenethez
6. praktikusan tárolható legyen hosszú távra is

# Direkt digitális aláírások I (Direct Digital Signatures)

- csak a küldő és a címzett közötti, megbízható harmadik fél nincs
- feltételezi, hogy a címzett ismeri a küldő nyilvános kulcsát
- az aláírást az üzenetnek vagy annak hash kódjának a küldő magánkulcsával való kódolása („titkosítása”) jelenti
- ha azt is szeretnénk hogy az üzenet titkos legyen persze szükség van a címzett nyilvános kulcsával való titkosításra is
- ami fontos, hogy **az aláírás után** történjen
- mert viták esetén a megbízható harmadik félnek az aláírás mellett az üzenetet is látnia kell

# Direkt digitális aláírások II (Direct Digital Signatures)

- az aláírás biztonsága a küldő magánkulcsának titokban tartásán múlik
- ez  gondod jelenthet: elhagyás, eltulajdonítás esetén ->
  - hitelesített(!) időbélyegzés és
  - időben történő kulcsvisszahívás kell,
  - célszerű a külön aláíró kulcspár használata, mely csak aláírásra (a magánkulcs) és annak ellenőrzésére (a nyilvános kulcs) szolgál nem pedig titkosításra - megfejtésre

# Digitális aláírás döntőbiróval
# Arbitrated Digital Signatures

- *A döntőbíró (arbitrator) olyan választott vagy kijelölt személy vagy szervezet, akinek egy aláíró, illetve ellenőrző közötti vita eldöntése a feladata, ha köztük nincs megegyezés egy digitális aláírás érvényességét illetően. (Fogalomtár)*
- A döntőbíró a vitákon túl
  - ellenőrzi (validates) az aláírást a hozzá eljuttatott üzeneten
  - dátummal látja el, majd elküldi a címzettnek
- a döntőbíróban mindkét félnek meg kell bízni
- a megvalósítás történhet mind a nyilvános, mind a szimmetrikus kriptográfia algoritmusaival
- a döntőbíró vagy elolvashatja az üzenethez, **vagy nem** (elég a titkosított tartalmat és annak aláírását látnia)

# Hitelesítési protokollok
# Authentication Protocols

- a feleknek meg kell győzniük partnerüket személyük hitelességéről, és szükséges a kulcscseréhez is
- lehet egyirányú vagy kölcsönös
- alapvetően fontos
  - a bizalmasság – a kapcsolatkulcsok védelméhez
  - ezért egy előzetesen eljutatott, megbízható közös titkos vagy nyilvános kulcs kell hozzá
  - időbeni pontosság (timeliness) – a visszajátszásos támadások (replay attacks) kivédésére
- a biztonságos protokollok tervezése nagy körültekintést igényel
- **számos publikált protokollban fedeztek fel hibákat, melyeket később korrigálni kellett.**

# Visszajátszásos támadások (Replay Attacks)

- amikor a támadó egy valós (aláírt/titkosított/stb.) üzenetet lemásol és később újra elküld
  - egyszerű visszajátszás
  - ismétlés, mely naplózható (can be logged)
  - észrevehetetlen visszajátszás (cannot be detected)
  - visszajátszás a küldőnek módosítás nélkül (backward replay)
- lehetséges ellen intézkedések
  - üzenet sorszámok (sequence numbers) használata (általában nem praktikus, mert emlékezni kell a legutóbbi sorszámra)
  - időbélyegek (timestamps, az órák szinkronizálása kell)
  - kérdés/felelet (challenge/response) egyszeri nonce-okkal

# Kölcsönös hitelesítés szimmetrikus titkosítással

- a kulcsok két szintű (**főkulcs - kapcsolatkulcs**) hierachiájával
- általában egy **kulcselosztó központon**

  (Key Distribution Center, KDC) keresztül, amiben mindenki megbízik
  - minden fél a központtal egy-egy főkulcson osztozik
  - a központ generálja a feleknek kapcsolatkulcsokat
  - és a főkulcs segítségével osztja ki őket

# A Needham-Schroeder protokoll szimmetrikus kriptográfiával

- az eredeti alap kulcscsere protokoll
- kulcselosztás harmadik fél segítségével
- egy KDC közvetít A és B között
- nekik a Ka és Kb szimmetrikus kulcsokkal titkosítva
- ő generálja és osztja ki a Ks kapcsolatkulcsot
- ezért benne abszolút meg kell bízni
- a protokoll:
  1. A->KDC: $ID_A \| ID_B \| N_1$
  2. KDC -> A: $E_{Ka}[Ks \| ID_B \| N_1 \| E_{Kb}[Ks \| ID_A]]$
  3. A -> B: $E_{Kb}[Ks \| ID_A]$
  4. B -> A: $E_{Ks}[N_2]$
  5. A -> B: $E_{Ks}[f(N_2)]$

# Needham-Schroeder Protocol

- arra szolgál, hogy biztonságosan szétosszon A és B közt egy új Ks kapcsolatkulcsot
- de sérülékeny a visszajátszásra,
  - ha egy korábbi Ks kapcsolatkulcs kompromittálódott
  - a támadó visszajátszthatja a 3. üzenetet
  - meggyőzve B-t, hogy A-val kommunikál és

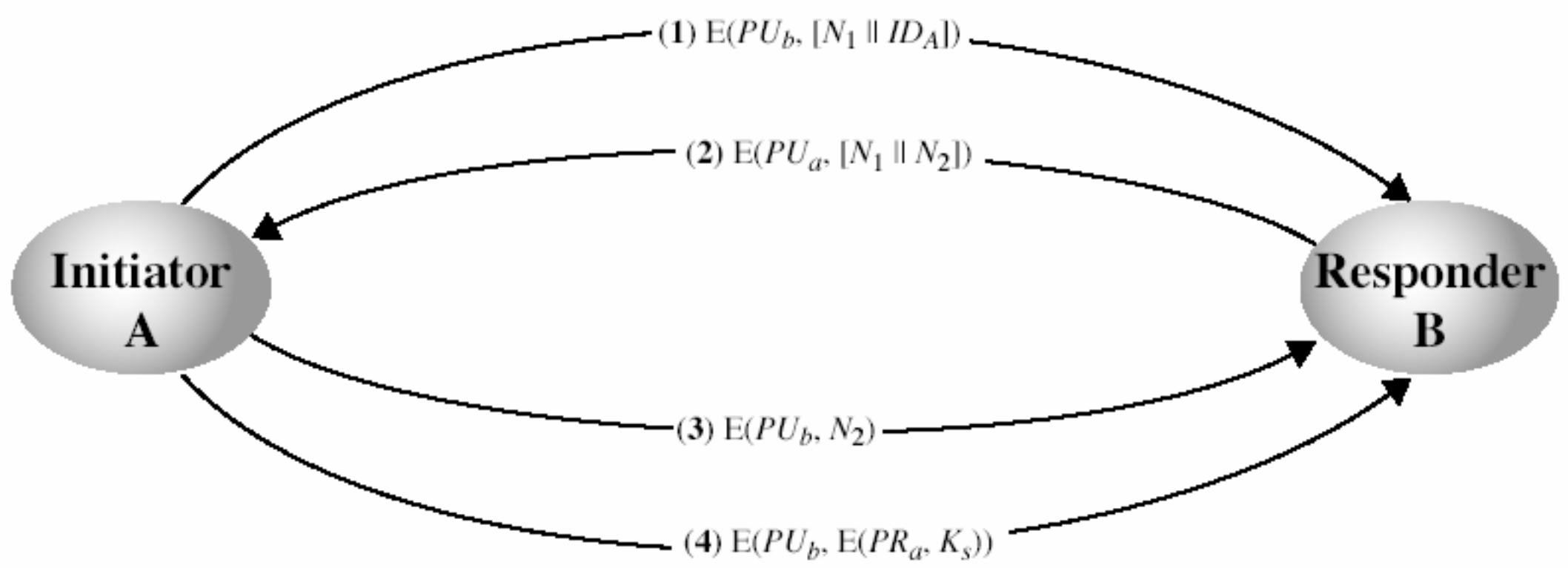
  rávéve, hogy eztán a régi Ks-t használja
- a hiba kijavítása történhet:
  - időbélyegekkel (Denning 81)
  - még egy nonce használatával (Neuman 93)

# Kölcsönös hitelesítés nyilvános kulcsú titkosítással

- a nyilvános kulcsú titkosítás számos megközelítési módot kínál
- egy példát már láttunk a kulcselosztásnál
- de ehhez a feleknek biztosnak kell lenniük, hogy valóban a partner nyilvános kulcsát birtokolják
- ez a feltétel nem mindig praktikus
- helyette elég egy hitelesítő szerver (Authentication Server, AS) nyilvános kulcsát ismerni
- számos protokoll van időbélyegekkel vagy nonce-okkal

# Titkos kulcs szétosztás nyilvános kulcsú kriptográfiával

Ha már $\mathbf{PU_A}$ és $\mathbf{PU_B}$ cseréje megtörtént:




$\mathbf{N_1}$ és $\mathbf{N_2}$ „nonce” = véletlen bitsorozat, a kapcsolat egyedi azonosítója

# Denning AS protokoll

- Denning 81 protokollja a következő:
  1. A -> AS: $ID_A$ || $ID_B$
  2. AS -> A: $E_{PRas}[ID_A||PU_a||T]$ || $E_{PRas}[ID_B||PU_b||T]$
  3. A -> B: $E_{PRas}[ID_A||PU_a||T]$ || $E_{PRas}[ID_B||PU_b||T]$ || $E_{PUb}[E_{PRA}[K_s||T]]$
- észrevétel: a $K_s$ kapcsolatkulcsot A választja, így nem kell AS-ben megbíznia a megőrzéséhez
- az időbélyegek megóvnak a visszajátszástól, de az órák szinkronizálása kell hozzájuk

# Egyirányú hitelesítés (One-Way Authentication)

- akkor szükséges, ha a feladó és a címzett **nem egyidőben** érintkezik,
  pl. e-mailezés esetén
- a ,,boríték” = az e-mail fejléce szabadon olvasható kell, hogy legyen a postázáshoz
- de az üzenet külön-külön lehet
  - titkos **és/vagy**
  - hiteles (vagyis a feladó által aláírt)

# Szimmetrikus titkosítással

- A címzettnek (B) nem kell online lennie:

  **1.** A->KDC: $ID_A \| ID_B \| N_1$

  **2**. KDC -> A: $E_{Ka}[Ks \| ID_B \| N_1 \| E_{Kb}[Ks \| ID_A]]$

  **3.** A -> B: $E_{Kb}[Ks \| ID_A] \| E_{Ks}[M]$

- *ez nem véd a visszajátszástól*
  - alkalmazhatnánk időbélyegeket, de az e-mailek átjutásának időnként nagyobb várakozási ideje ezt problematikussá teszik.

# Nyilvános kulcsú titkosítással

- már láttunk néhány megközelítést
- ha a bizalmasság a fő szempont, akkor pl:

  A->B: $E_{PUb}[Ks] \,||\, E_{Ks}[M]$

  - vagyis titksosított kapcsolatkulcs, majd az üzenetet vele titkosítva
- ha csak hitelesítésre van szükség pl:

  A->B: $M \,||\, E_{PRa}[H(M)] \,||\, E_{PRas}[T||ID_A||PU_a]$

  - vagyis üzenet, aláírás, tanúsítvány (AS-től)

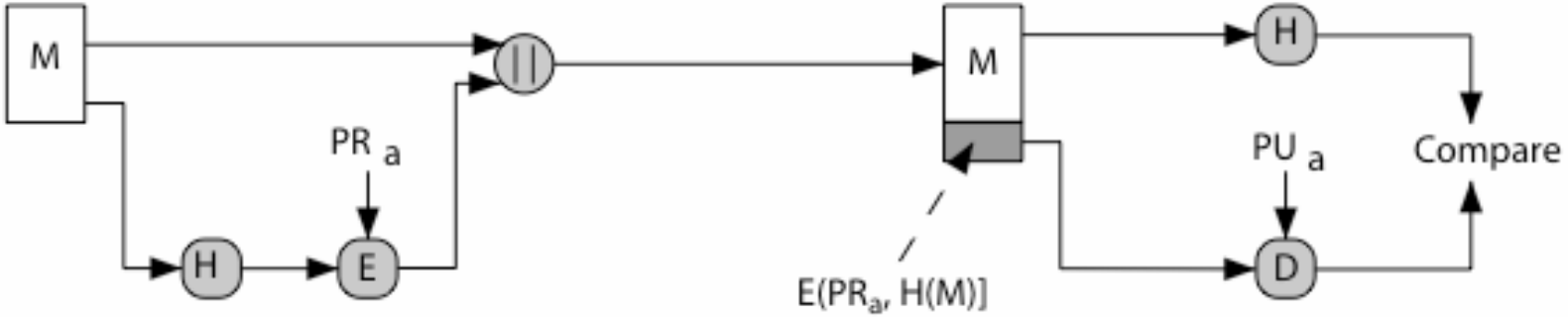
# A digitális aláírási szabvány
# Digital Signature Standard (DSS)

- az USA kormányzata által elfogadott aláírási séma
- tervezői: NIST & NSA
- szabvány: FIPS-186 (1991)
- felülvizsgálva: 1993, 1996, 2000
- az SHA hash algoritmusra épül
- a DSS a szabvány neve, DSA az algoritmusé
- a FIPS 186-2 (2000) más alternatívákat is kínál az RSA-ra vagy az elliptikus görbékre alapozva

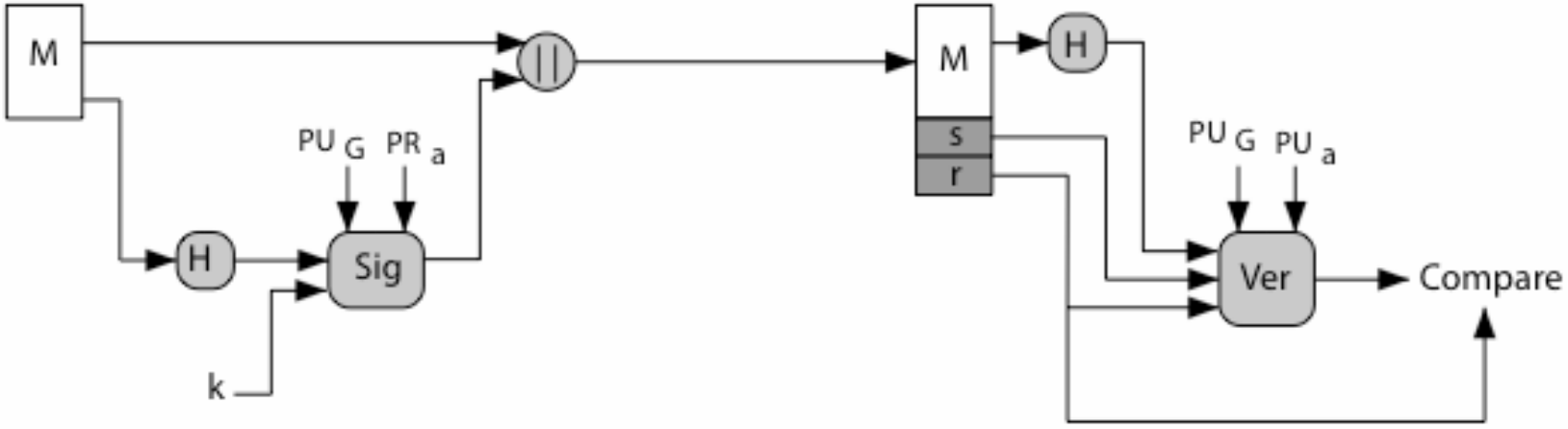
# A digitális aláírási szabvány

- 320 bites aláírást készít
- 512-1024 bites biztonsággal
- kisebb és **gyorsabb** mint az RSA
- csak digitális aláírási séma, titkosításra nem jó
- a biztonság a diszkrét logaritmus probléma nehézségén alapszik
- az ElGamal & Schnorr sémák variációja

# Az RSA-ra alapozott aláírás és a DSA különbsége




(a) RSA Approach




(b) DSS Approach

# A DSA paraméterei: p, q, g, x és y

- megosztott globális nyilvános kulcs értékek: **p,q,g**
  - **q** legyen egy 160 bites prímszám
  - **p** legyen egy nagy prímszám, melyre
    - $2^{L-1} < p < 2^{L}$
    - ahol L= 512 - 1024 bit és 64-gyel osztható
    - 2001-ben módosítás: csak L=1024
    - és **q** a **(p-1)** egyik nagy osztója
  - legyen $g = h^{(p-1)/q} \mod p$
    - ahol $h < p-1$, $h^{(p-1)/q} \mod p > 1$ véletlen
    - így **g** rendje nagy (pontosan **q**) lesz $Z_p$-ben, mert $g^q = (h^{(p-1)/q})^q = h^{(p-1)} = 1 \pmod p$
- a felhasználók (azaz az aláírók)
  - választanak egy $x < q$ magánkulcsot és
  - kiszámítják az $y = g^x \mod p$ nyilvános kulcsot

# DSA aláírás készítés

- az **M** üzenet aláírása két 160 bites szám lesz: **r** és **s**
- egy **M** üzenet aláírásához a küldő:
  - generál egy véletlen **k számot, ahol k<q**
  - fontos:
    - **k**-nak véletlennek kell lennie
    - használat után meg kell semmisíteni,és
    - újrahasználni tilos
- ezután így számítjuk az aláírást:

$$r = (g^k \bmod p) \bmod q$$

$$s = k^{-1} \cdot (H(M) + x \cdot r) \bmod q$$

- az **M** üzenet **aláírása**: **(r,s)**
- melyet az üzenettel együtt elküldhetünk

# A DSA aláírás ellenőrzése

- miután az M-et és az `(r,s)` aláírást megkapta a címzett vagy bárki más kiszámíthatja:

$$w = s^{-1} \bmod q$$
$$u1 = H(M) \cdot w \bmod q$$
$$u2 = r \cdot w \bmod q$$
$$v = (g^{u1} \cdot y^{u2} \bmod p) \bmod q$$

- ha **v=r** akkor az aláírást elfogadja
- a DSA helyességének bizonyítását lásd a szabványban FIPS 186-2 (11-12. oldal):

http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

# Az újabb szabványtervezet

- A faktorizációt és így a diszkrét logaritmus problémát megoldó algoritmusok fejlődése miatt indokolt a nagyobb prímszámokra való áttérés
- Javaslat p és q hosszára bitekben

  **L = 1024, N = 160**

  **L = 2048, N = 224**

  **L = 2048, N = 256**

  **L = 3072, N = 256**

- 2008 novemberében még csak tervezet a szabvány új verziója: FIPS-186-3: http://csrc.nist.gov/publications/drafts/fips_186-3/Draft_FIPS-186-_November200.pdf
- Elliptikus görbék feletti csoportokban is

# Felhasznált irodalom


- William Stallings: Cryptography and Network Security, 4th Edition, Prentice Hall, 2006. (Chapter 13)
- Lawrie Brown előadás fóliái (Chapter 13)
- **KIKERES Fogalomtár** 3.0 www.fogalomtar.hu