

Mennyire biztonságosak a kriptográfiai protokollok?

Csirmaz László

Közép Európai Egyetem

- **Digitális aláírás – ne használjuk az MD5-t**
- **Wifi kapcsolat – mi van az RC4-gyel?**
- **Egy sor rövidítés**
- **Mit lehet mégis tenni – NESSIE**

Digitális aláírás: csak a *kivonatot*!
Kivonat készítése: MD5 (sztenderd)
2005: gyenge ütközés – kriptográfiai szenzáció



Zsebenci Klopédia

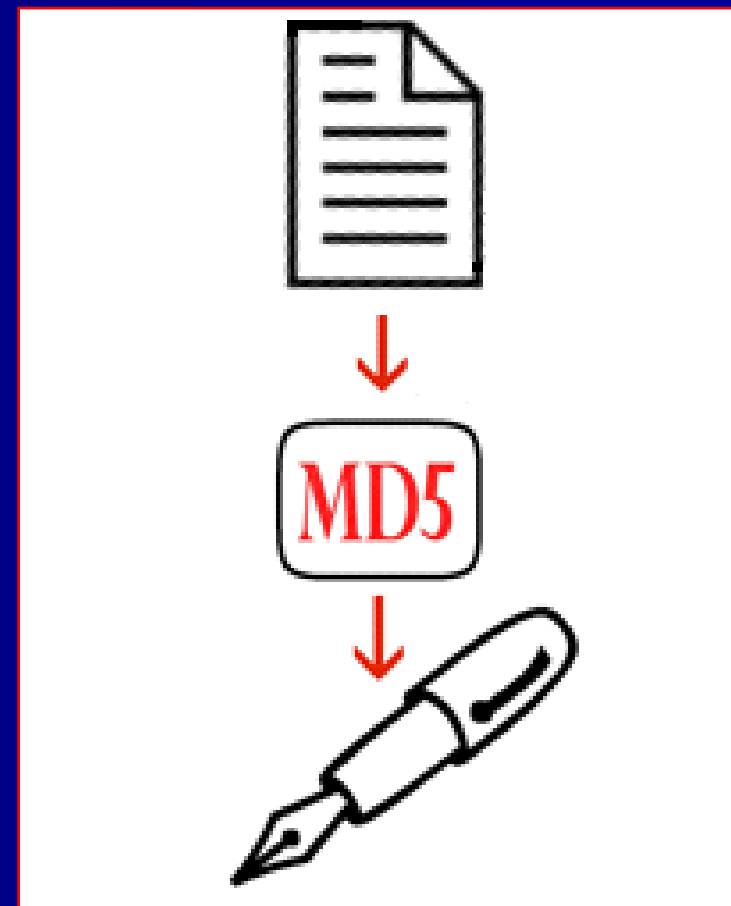


Tanár

“Tanár úr, írna nekem egy ajánlást?
Küldöm a file-t, csak alá kell írni...”

Digitális aláírás:

- **A dokumentum kivonatát írjuk alá**
- **Kivonat: MD5**
- **Aláírás: nyilvános kulcsú aláírás (akármilyen lehet)**



gv: /root/nws06/xajanlo.ps

File State Page Portrait 1.000 Letter /root/nws06/xajanlo Tue Apr 11 11:45:44

Variable Size

Open

Print All

Print Marked

Save All

Save Marked

<< >>

Reload

Ajánlólevél Zsebenci Klopédia részére

Miskolc, 2006 április 20

Az elmúlt két évben **Zsebenci Klopédia** az általam tartott kriptológiai kurzusokat látogatta. A kurzusokon nyújtott teljesítménye alapján melegen ajánlom hogy őt PhD hallgatónak ebben a szakterületen felvegyék.

Amennyiben ezzel az ajánlólevéllel kapcsolatban kérdése van, kérem forduljon hozzám bizalommal.

Barátsággal:

Csirmaz László sk

Közép Európai Egyetem

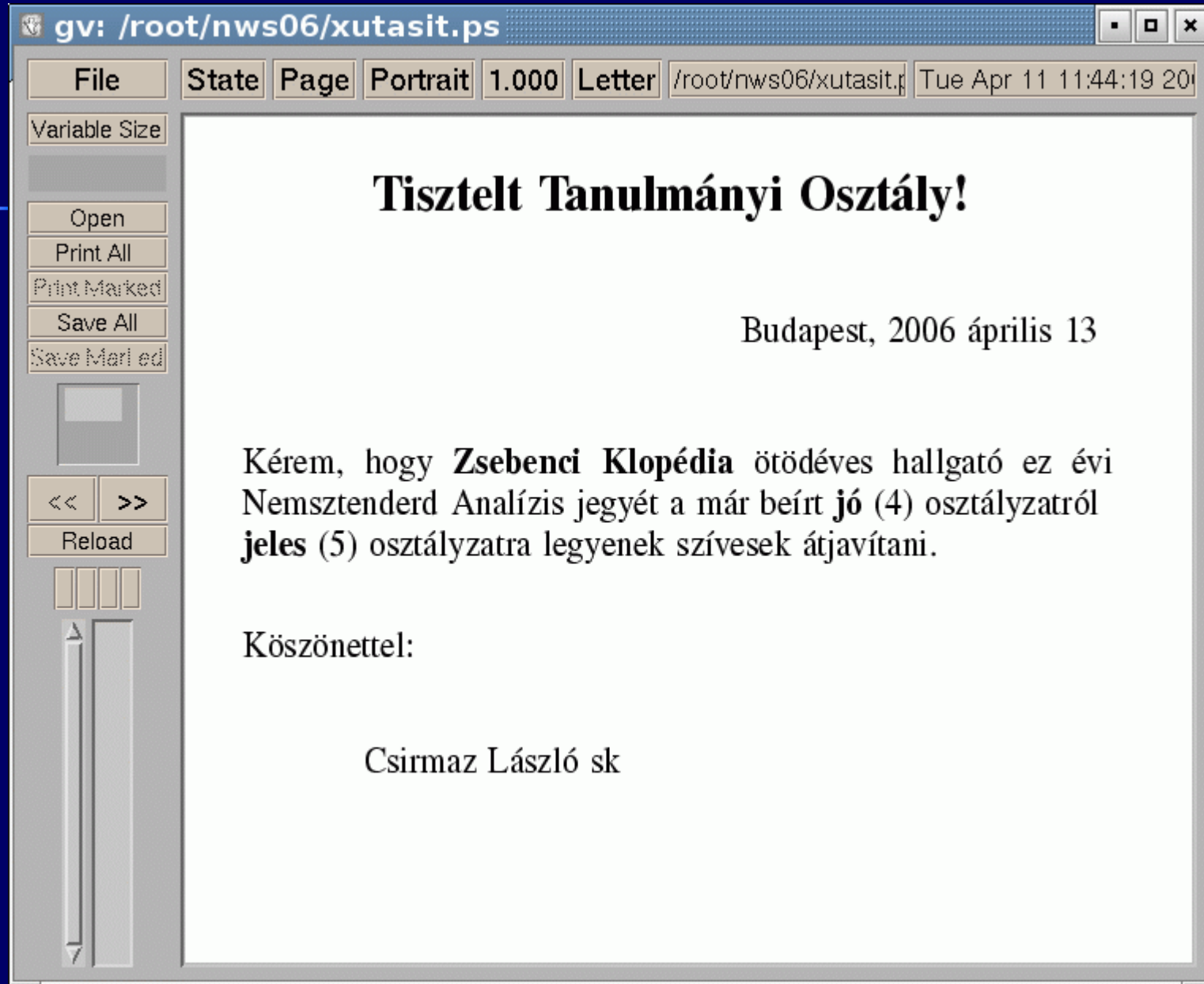
Ellenőrizzük az MD5 értéket:



“Tanár úr nyugodtan írja csak alá...”



```
> md5sum xajanlo.ps  
583bdceb34826c38ac7f1fdac3aca807 xajanlo.ps
```



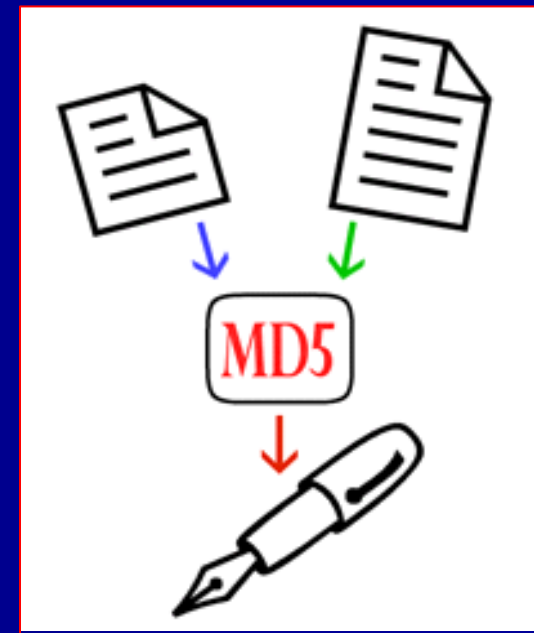
Ellenőrizzük az MD5 értéket:

583bdceb34826c38ac7f1fdac3aca807 xajanlo.ps

583bdceb34826c38ac7f1fdac3aca807 xutasit.ps

Ugyanaz a kivonat!

Ugyanaz az aláírás!



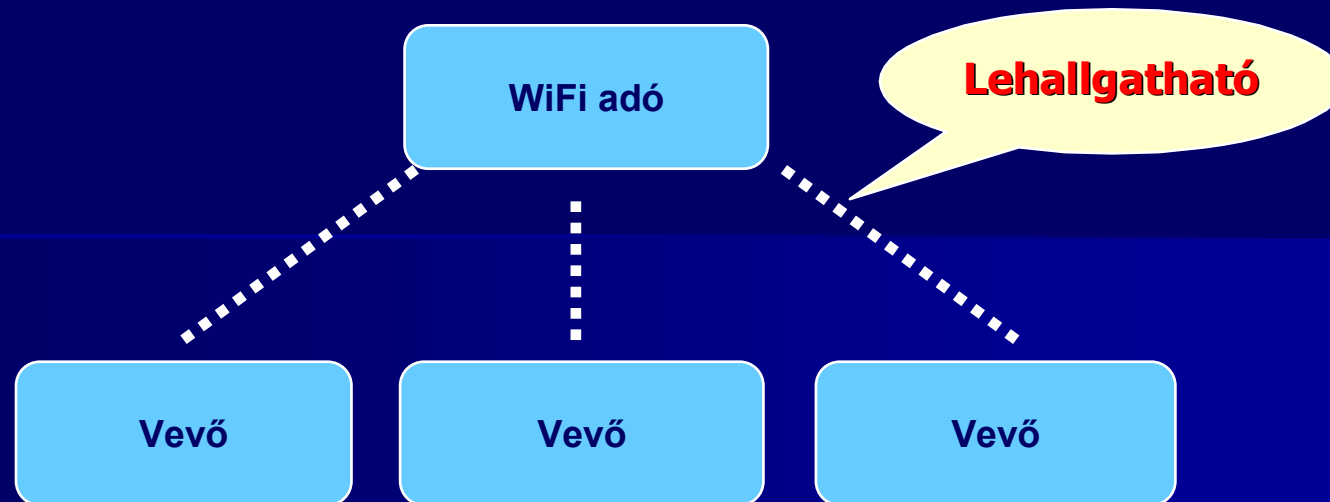
<http://renyi.hu/~csirmaz/nws06/xajanlo.ps>

<http://renyi.hu/~csirmaz/nws06/xutasit.ps>

Hogyan csinálta Klopédia?

- Magas szintű nyelv (postscript)
- `preamble; put(R1); put(R2); if(=){text1}{text2}`
- “text2”-t nyomtatja
- `preamble; put(R1); put(R1); if(=){text1}{text2}`
- “text1”-et nyomtatja
- R1 és R2 ügyesen választott véletlen sztringek
- 2005 Eurocrypt
- $\text{MD5}(\text{“preamble;put(R1);put(R2)”}) = \text{MD5}(\text{“preamble;put(R1);put(R1)”})$;
- A maradék bármi lehet, csak legyen egyforma
- Stefan Lucks, Magnus Daum konstrukciója

- **Digitális aláírás – ne használjuk az MD5-t**
- **Wifi kapcsolat – mi van az RC4-gyel?**
- **Egy sor rövidítés**
- **Mit lehet mégis tenni – NESSIE**



**Lehallgatás, jogtalan használat ellen: WEP titkosítás
(2004 óta *nem javasolt*; helyette WPA és WPA2)**

Adat:	584952454C455353
RC4(sorszám+kulcs):	1234567890ABCDEF

Összeg (továbbított):	4A7D043D6F7ABE9C
------------------------------	-------------------------

1. Probléma:

Kulcs: ugyanaz
 Sorszám: gyakran ugyanaz

 adat fejthető!

2. Probléma:

Adat első byte-ja fix (IP csomag)
 RC4 hibásan van használva

 kulcs fejthető!

3. További problémák: (CRC checksum, stb)

Adat: 584952454C455353

RC4(sorszám+kulcs): 1234567890ABCDEF

Összeg (továbbított): 4A7D043D6F7ABE9C

Tanulság...

- **protokollokat nehéz tervezni**
- **a támadások nem újak: IPSEC, SSH, Microsoft PPTP**
- **a nyilvánosság mindig segít**
- **olvassuk el a használati utasítást (RC4)**
- **érdeemes megkérdezni a szakembereket
(és hallgatni rájuk)**

- **Digitális aláírás – ne használjuk az MD5-t**
- **Wifi kapcsolat – mi van az RC4-gyel?**
- **Egy sor rövidítés**
- **Mit lehet mégis tenni – NESSIE**

Melyik a kakukktojás?

- RC4
- MD5
- RSA
- DH
- DES
- 3DES
- AES
- MAC
- IDEA
- SHA-1
- SHA-256
- RIPEMD
- ZIP
- MISTY
- KASUMI
- SAFER
- BLOWFISH
- SFLASH

Megoldás:

- RC4
- MD5
- RSA
- DH
- DES
- 3DES
- AES
- MAC
- IDEA
- SHA-1
- SHA-256
- RIPEMD
- ZIP
- MISTY
- KASUMI
- SAFER
- BLOWFISH
- SFLASH

Az összes többi kriptográfiai eljárás

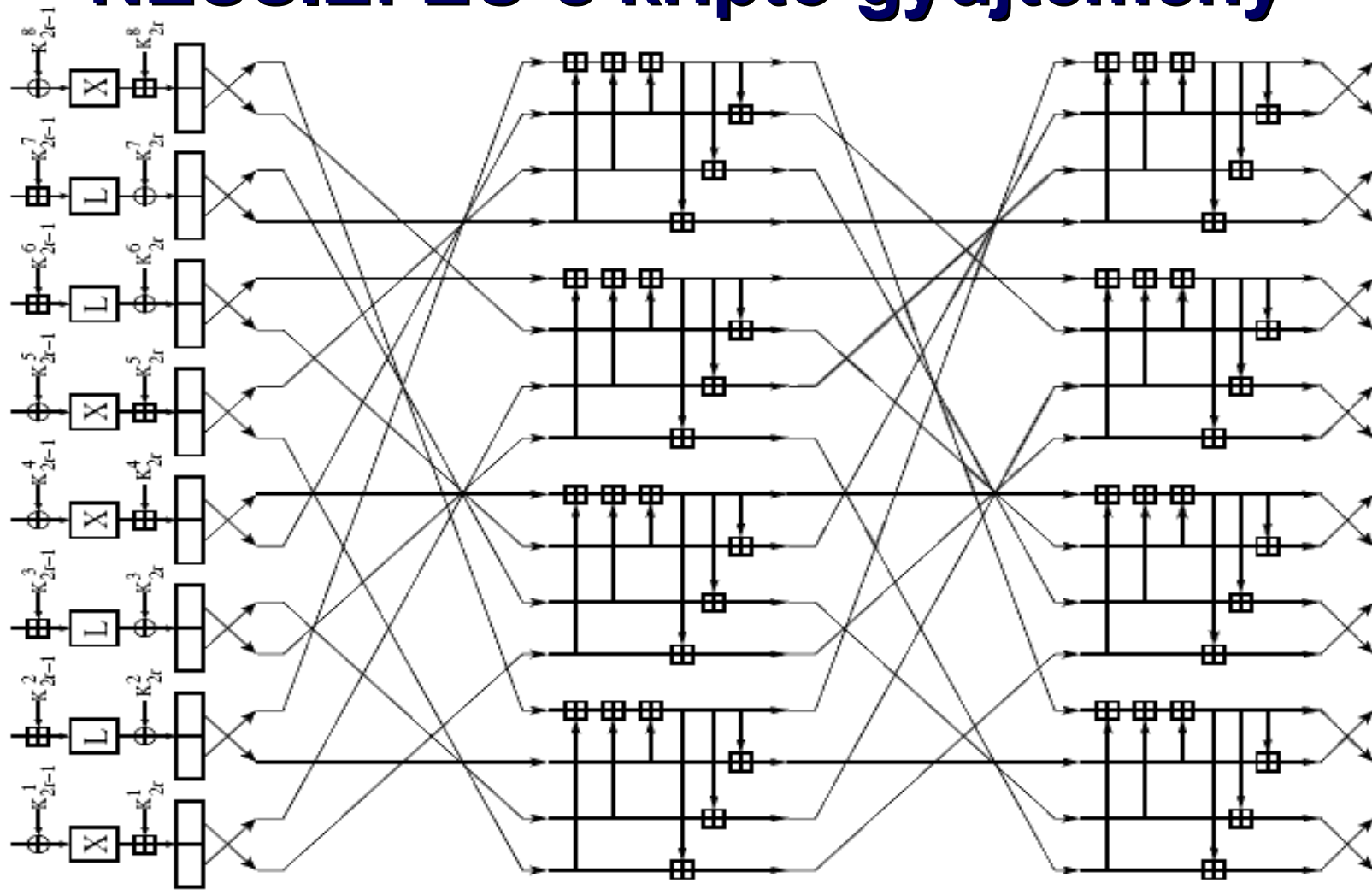
- **Digitális aláírás – ne használjuk az MD5-t**
- **Wifi kapcsolat – mi van az RC4-gyel?**
- **Egy sor rövidítés**
- **Mit lehet mégis tenni – NESSIE**

NESSIE: EU-s kriptó gyűjtemény

<http://cryptonessie.org>



NESSIE: EU-s kriptó gyűjtemény



2.10. Alternative View of Encryption Round for SAFER++ (64-bit block)



Köszönöm a figyelmet!

Csirmaz László – csirmaz@ceu.hu