# ADATBIZTONSÁG VIZSGA

2006. január 25.

1. Tekintsük egy mini RSA rejtjelezést $p_1=23$, $p_2=71$ prímekkel.

a.) Hány olyan x üzenet van ($1 \le x < m=p_1p_2$), amelynek nincs közös faktorja a titkos prímekkel? (3p)

b.) Mekkora a valószínűsége, hogy egy véletlenszerű x üzenet m faktorizációjára ad lehetőséget? (6p)

c.) Adja meg a d kódoló kitevőt, ha e=3 a publikus kitevő? (5p)

2. Véletlen m számú blokkból álló üzenetünket rejtjelezve és integritásvédelemmel szeretnénk továbbítani. Integritásvédelemül azt a gyors módszert választjuk, hogy az m darab üzenetblokkot mod 2 összegezzük, s így egy ellenőrző összeg blokkot nyerünk (azaz az ellenőrző összeg blokk i-edik bitje az üzenetblokkok i-edik bitjeinek a mod 2 összege). Ezután az m+1 darab blokkot blokkonként ECB módban rejtjelezzük AES rejtjelezőt alkalmazva

a.) Lehallgató támadó sikeres lehet-e? (5p)

b.) Aktív támadó sikeres lehet-e? (5p)

3. Egy bankkártya alkalmazásban 4 decimális karakter hosszú PIN kódot alkalmaznak. A terminál egy karakter leütése után azonnal ellenőrzi azt. A 4 karakterből összesen 1 egy karaktert téveszthet a támadó, s azt is csak egy alkalommal, utána a terminál bevonja a kártyát.
Jobb-e ez a rendszer egy kártyatolvaj ellen, mint az amelyik csak 2 decimális karakter hosszú PIN kódot alkalmaz, de amelyik a PIN kód mindkét karaktere beadása után ellenőriz és három egymás utáni hibás PIN-próbálkozás esetén nyeli csak el a kártyát.

a.) Adja meg az első rendszerben a tolvaj P1 sikervalószínűségét. (8p)

b.) Biztonságosabb-e második rendszer? (Adja meg tolvaj P2 sikervalószínűségét a második rendszerben.) (8p)

4. Bizonyítsa be, hogy egy Feistel struktúrájú rejtjelező mindig invertálható, még akkor is ha az *F* rétegfüggvény nem invertálható! (8p)

5. Egy kriptorendszer kulcshossza 100 bit. A kulcsot olyan generátorból nyerjük, amely 5 bites blokkokat állít elő. Ezen blokkokból azonos valószínűséggel olyanokat generál, amelyekben az 1 bitek darabszáma mindig kevesebb, mint a 0 bitek darabszáma. Az egymás utáni blokkok függetlenek.

a.) 20 db blokkot használunk kulcsként. Mennyi a tényleges kulcshossz, azaz mennyi az így generált kulcs entrópiája? (8p)

b.) Lehetséges-e, hogy 100 bit entrópiájú kulcsot állítsunk előállítani az adott generátorra támaszkodva? Igen válasz esetén algoritmust adjon, nem válasz esetén is részletesen indokoljon. (8p)

6. <később>

**Pontozás: 1: <=30 , 2:31 - 42, 3:43 - 55 , 4: 56 - 63, 5: 64 - 80**

# Adatbiztonság vizsga eredmények

2006. január 25.

(Ügyeljen a pontos fogalomhasználatra, pontos, formális definíciókra, részletes indoklásokra!)

Név: .....
.....

Neptun kód: .....

**1.** (3p;6p;5p)

a.)

b.)

c.)

**2.** (5p;5p)

a.) igen nem Magyarázat:

b.) igen nem Magyarázat:

**3.** (8p;8p)

a.) P1=

b.) igen nem P2=

**4.** (8p)

**5.** (8p;8p)

a.) kulcs entrópia=

b.) igen nem Magyarázat:

**6.** (8p;8p)

a.) Támadás:

b.) Javított protokoll:

# ADATBIZTONSÁG VIZSGA MEGOLDÁSOK

2006. január 25.

**1.**

a.) Φ(m)=22*70=1540

b.) 0.057

Képlet vagy indoklás:

$$P=\frac{m-\Phi(m)}{m}=1-\frac{(p_1-1)(p_2-1)}{p_1 p_2}=1-\frac{(p_1 p_2-p_1-p_2+1)}{p_1 p_2}=\frac{1}{p_1}+\frac{1}{p_2}-\frac{1}{p_1 p_2}$$

c.) 1540=513·3+1 → (-513) ·3=(-1) ·1540+1 → d=-513=1027 (mod 1540)

2.)

a.) Nem .....Még kulcskereséssel sem.

b.) Igen .....A módszer az 1....M rejtett blokk sorrend-cseréjére, páros számú ilyen blokk beszúrására érzéketlen.

**3.**

a.) $1/10^4+ 4\cdot(9/10)\cdot(1/9) \cdot(1/10^3)= 5 \cdot(1/10^4)=0.0005$

b.) 1 - (99/100)·(98/99)·(97/98)= 1- 97/100 = 0.03. Tehát az első rendszer a biztonságosabb.

**4.** Tk.29.o.

**5.** a.)

blokkfajta: db

3db 1bit 2db 0 bit → 10

4db 1bit 1db 0 bit → 5

5db 1bit 0db 0 bit → 1

Összesen: 16 –féle blokk → $\log_2 16 = 4$ bit /blokk → $100/5 \cdot 4 = 80$ bit

b.) A 16 lehetséges blokkot egyértelműen leképezzük a 0000,….,1111 16 db féljbájt egykébe. 25 db blokkot ilyen módon leképezve 100 db pénzfeldobás bitet kapunk.