Adatbiztonság PPZH Név:
2012. május 21 Neptun kód:

1. Egy fonetikus jelszó generátor működése a következő: kiválaszt kettő 3 betűs jelszó töredéket, hogy egy 6 betűs jelszót generáljon. A töredékek a következő módon épülnek fel: Magánhangzó – Mássalhangzó – Magánhangzó. Az ABC legyen a 26 betűs angol ABC (Magánhangzó: a,e,i,o,u,y).

a.) Hány különböző jelszó képzelhető el? (2p)
b.) Milyen valószínűséggel lehet egy jelszót megtippelni, ha háromszor tippelhetünk? (2p)
c.) Hány jelszót kell kérni a generátortól, hogy nagy (~40%) valószínűséggel legyen két egyforma (ütköző) jelszó? (4p)

2. Tekintsük az alábbi H: $\{0,1\}^* \rightarrow \{0,1\}^n$ hash függvényt: $H(x)=h_1(x_1 \mid h_2(x_2))$, ahol x_1 és x_2 az x bitsorozat első és második fele, valamint | a bitsorozatok összefűzését jelenti.
a.) Definiálja az ütközésellenálló hash függvényt (1p)
b.) Biztonságos-e a $H(x)$ konstrukció, ha tudjuk, hogy h_1: $\{0,1\}^* \rightarrow \{0,1\}^n$ ütközés-ellenálló, de h_2: $\{0,1\}^* \rightarrow \{0,1\}^n$ nem ütközés-ellenálló tulajdonságú. Indokoljon! (9p)

3. Egy kliens és egy szerver közötti biztonsági protokoll a következő részekből áll:

- kölcsönös partnerhitelesítés a kapcsolat elején (C – kliens, S – szerver):
  C → S: N_C
  S → C: N_S, $MAC_K(N_C)$
  C → S: $MAC_K(N_S)$

ahol N_X egy 128 bites véletlen szám (nonce), K egy korábban létrehozott hosszú élettartamú közös AES kulcs C és S között, $MAC_K()$ pedig a CBC-MAC függvény az AES blokkrejtjelezővel, K kulccsal és IV = 0 beállítással;

- kapcsolat során küldött üzenetek rejtjelezése az AES blokkrejtjelezővel CTR módban a fent említett K kulccsal;
- rejtjelezett üzenetek integritásvédelme CBC-MAC módszerrel az AES blokkrejtjelezővel, K kulccsal, és IV = 0 beállítással.

Mutasson támadást, melyben a támadó tetszőleges, a fenti módszerrel rejtjelezett üzenetet dekódolni tud! (12 p)

4. Tekintsünk egy MIX alapú anonim kommunikációs rendszert! Tegyük fel, hogy a MIX-nek van egy RSA kulcspárja, és minden felhasználó ismeri a MIX (e, n) publikus kulcsát. A rendszer úgy működik, hogy a felhasználó az m üzenetét a MIX publikus kulcsával kódolja, azaz a tankönyvi RSA segítségével előállítja a $c = m^e \bmod n$ rejtjeles üzenetet, és c-t küldi a MIX-nek. A MIX dekódolja c-t, és m-et nyíltan küldi tovább az m-ben található eredeti címzettnek. Vissza irányú kommunikáció nincs, ezért m nem tartalmaz információt a küldőről. A MIX kötegelve dolgozik: 100 bejövő üzenetet mindig megvár (tfh. ezek 100 különböző felhasználótól érkeznek), s csak utána kezdi kiküldeni az ezekhez tartozó nyílt üzeneteket az eredeti címzetteknek megkevert sorrendben.
a) Milyen privacy-vel kapcsolatos célt próbál elérni ez a protokoll? (1p)
b) Eléri-e a protokoll a célját? Indokoljon! (6p)

5. Egy spamszűrő az órán ismertetett Bayes szűrést használja. Feltételezi, hogy Pr(S)=Pr(W)=0,5. Adatbázisa a következő adatokat tanulta meg:
Pr(olcsón|S)=0,01 Pr(eladó|S)=0,01 Pr(telek|S)=0,05
Pr(olcsón|H)=0,001 Pr(eladó|H)=0,005 Pr(telek|H)=0,1

Adott egy levél: „Telek olcsón eladó" tartalommal. Mekkora az esélye, hogy a levél spam? Számolja ki az órán tanult módon a levél kombinált spam-valószínűségét (három tizedes jegy precizitású részszámítások elegendőek)! (10p)

6. Unix/Linux hozzáférésvédelem az órán előadott módon

Tekintsük az alábbi `/etc/passwd` file részletet:

```
u1:x:1003:1004:,,,:/home/u1:/bin/bash
u2:x:1004:1005:,,,:/home/u2:/bin/bash
u3:x:1005:1006:,,,:/home/u3:/bin/bash
u4:x:1006:1007:,,,:/home/u4:/bin/bash
```

Az `/etc/group` file releváns része:

```
u1:x:1004:
u2:x:1005:
u3:x:1006:
u4:x:1007:
g1:x:1008:u1,u2
g2:x:1009:u2,u3,u4
g3:x:1010:u2,u3
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@gotcha:/adatbizt# ls -la
total 16
drwxr-xr-x  4 root root 4096 2011-04-22 10:49 .
drwxr-xr-x 25 root root 4096 2011-04-22 10:51 ..
drwxrwsr-x  2 u1   g1   4096 2011-04-22 10:50 d1
drwxr-xr--  2 u2   g1   4096 2011-04-22 10:50 d2
root@gotcha:/adatbizt# ls -la d1
total 20
drwxrwsr-x 2 u1   g1   4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw------- 1 u1   u4      4 2011-04-22 10:50 f1
-rw-rw-r-- 1 u1   g1     16 2011-04-22 10:50 f2
-rwxrwxrwx 1 u1   g2      8 2011-04-22 10:50 f3
root@gotcha:/adatbizt# ls -la d2
total 16
drwxr-xr-- 2 u2   g1   4096 2011-04-22 10:50 .
drwxr-xr-x 4 root root 4096 2011-04-22 10:49 ..
-rw-r--r-- 1 root g1      7 2011-04-22 10:50 f4
--w------- 1 root g1      6 2011-04-22 10:50 f5
```

a.) Mely felhasználók tudják kitörölni a `d2/f4` fájlt és miért? (`rm d2/f4`) (2p)
b.) Mely felhasználóknál fut le sikeresen a `cp d2/f4 d2/f6` parancs? (2p)
c.) Ki tudja módosítani az `f2` fájl jogosultságait (pl. `chmod o+w d1/f2`) (2p)
d.) Ki tudja lefuttatni a `rm d1/f3; cp d1/f1 d1/f3` parancsokat mind sikeresen, azaz kitörlni `f3`-at és helyére `f1`-et másolni? (2p)

Pontozás: 1: 0-21, 2: 22-29, 3: 30-38, 4: 39-46, 5: 47-55

Adatbiztonság PPZH megoldások

2012.május 21.

1.

a.) 26 = 6 + 20 N = $(6 * 20 * 6)^2$ = 720^2≈ 2^{19}

b.) ~3/720^2= 5.8 E-6

c.) Születésnapi paradoxon: ~√720^2= 720

2.

b.) Nem. Legyen $m_{i,1}$ az m_i üzenet első fele, ugyanígy $m_{i,2}$ a második fele (i=1,2). Keressünk olyan $m_1 \neq m_2$ üzenetpárt, amire $m_{1,1}= m_{2,1}$, $m_{1,2} \neq m_{2,2}$, $h_2(m_{1,2})=h_2(m_{2,2})$. Ekkor $h_1(m_{1,1} \mid h_2(m_{1,2}))= h_1(m_{2,1} \mid h_2(m_{2,2}))$.

3. (lásd 2011-es ppzh feladatsorban is!)

Bármely fél rejtjelező-orákulumként használható a partnerhitelesítés protokollt felhasználva:

A → S: X

S → A: Y, $MAC_K(X) = AES_K(X+0) = AES_K(X)$

A rejtjelezett üzenet i. blokkja így áll elő: M_i XOR $AES_K(C_i)$ ahol M_i az i. nyílt blokk, C_i az i. számláló érték. Tehát tetszőleges rejtjeles blokk dekódolható úgy hogy megszerezzük $AES_K(C_i)$ – t az orákulumtól.

4.

a) unlinkability of sender and receiver (globális lehallgató ellen), sender anonymity (fogadóval szemben) (½ p – ½ p)

b) unlinkability: Nem. Bárki megfigyelheti a MIX-ből kimenő nyílt üzeneteket, azokat kódolhatja a MIX publikus kulcsával, és így megállapíthatja, hogy melyik kimenő üzenet melyik bemenő üzenethez tartozik. (4p)

Sender anonymity: igen, mert az üzenetek nem tartalmaznak információt a küldőre vonatkozóan. (2p)

5.

Egyedi valószínűségek:

Pr(S|olcsón)=Pr(olcsón|S)/(Pr(olcsón|S)+Pr(olcsón|H)) = 0,01 / (0,01+0,001)=0,909

Pr(S|eladó)= 0,01/ (0,01+0,005)=0,667

Pr(S|telek)= 0,05/(0,05+0,1)=0,333

p= Pr(S|olcsón)* Pr(S|telek)* Pr(S|eladó) /

(Pr(S|olcsón)* Pr(S|telek)* Pr(S|eladó) + (1-Pr(S|olcsón))* (1-Pr(S|telek))*(1-Pr(S|eladó))

azaz p= 0,202/ (0,202 + 0,02) = 0,202/0,222=90,991%

6.

a.) csak u2, más nem írhat az alkönyvtárba (+root)

b.) csak u2, mert ő írhat d2-be, és tudja olvasni f4-et is.. (+root)

c.) csak a tulajdonos, u1 (és a root)

d.) a törlést csak u1,u2 tudja elvégezni f1-et viszont ebből csak u1 olvashatja, ő írni is tud az alkönyvtárba, tehát csak u1. (+root)