Adatbiztonság PZH Név:
2013. május 23 Neptun kód:

1. Tegyük fel, hogy DES rejtjelezést használtunk (DES kulcsméret 56 bit) 64 bites véletlen üzenet blokkok rejtjelezésére, ahol az üzenet blokkok utolsó bitje paritásbit. Rejtett szövegeket figyelhet meg a támadó, majd kimerítő kulcskeresést végez. 50 rejtjeles blokk megfigyelése elegendő-e a feladat sikeres végrehajtásához, azaz várhatóan sikerül-e kiválasztani a keresett kulcsot? (A DES kódolást és dekódolást véletlen függvényként modellezheti.) **(7p)**

2. Tekintsünk egy mini RSA rejtjelezést p_1=23, p_2=71 prímekkel.
a.) Hány olyan x üzenet van ($1 \leq x < m=p_1p_2$), amelynek nincs közös faktorja a titkos prímekkel? **(2p)**
b.) Mekkora a valószínűsége, hogy egy véletlenszerű x üzenet m faktorizációjára ad lehetőséget? **(2p)**
c.) Adja meg a d kódoló kitevőt, ha e=3 a publikus kitevő? **(3p)**

3. Egy webszerver és egy böngésző az SSL protokollt használja a HTTP forgalom védelmére. A handshake során Diffie-Hellman alapú kulcscserét használnak, és a szervernek egy DSA digitális aláírás ellenőrző kulcsot tartalmazó tanúsítványa van. A szerver nem kéri, hogy a kliens hitelesítse magát.

Adja meg, hogy ebben az esetben mely handshake üzenetek kerülnek átvitelre, és vázlatosan adja meg azok tartalmát! **(8 pont)**

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? **(2p)**
b) Eléri-e a protokoll a célját? Indokoljon! **(6p)**

5. Adott az alábbi tűzfal szabályhalmaz:
Keressen példát a következő inkonzisztenciatípusokra, és válaszát röviden indokolja!

No.	Proto	Src	Dst	Decision
1	tcp	10.1.1.0/25	any	deny
2	udp	10.1.1.0/24	192.168.0.0/16	accept
3	tcp	10.1.1.0/24	any	accept
4	udp	192.168.1.0/24	10.1.1.0/24	deny
5	tcp	10.1.1.128/25	any	deny
6	udp	10.1.1.0/24	any	deny
7	udp	192.168.1.0/25	10.1.0.0/16	accept

a.) Shadowing **(2p)**
b.) Generalization **(2p)**
c.) Correlation **(2p)**

6. Unix/Linux hozzáférésvédelem

```
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   root    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 d1/f1 fájlt és miért? (rm d1/f1)* **(2p)**
b.) mely felhasználóknál fut le sikeresen a cp d2/f4 d1/f6 parancs? **(2p)**
c.) az u1 felhasználó (u1 aktív csoporttal) készít egy új fájlt d1-ben (touch d1/fu1), milyen csoport lesz a tulajdonosa a létrejövő fájlnak **(2p)**
d.) A root felasználó mely fájlokat tudja törölni az f1 alkönyvtárban **(1p)**
e.) Ki tudja végrehajtani sikeresen az f2 fájl olvasási jogának teljes törlését? (chmod a-r d1/f2) **(1p)**

Pontozás: 1: 0-16, 2: 17-23, 3: 24-30, 4: 31-37, 5: 38-44

(A feladatlapon jelölje bekarikázással azon feladatokat, amikkel érdemben foglalkozott.)

Adatbiztonság PZH megoldások

2013.május 23

1. Nem.
P(egy téves kulccsal helyes paritásúra dekódolunk egy rejtett szöveg blokkot) = 2^{-1}
P(50 rejtjeles blokk mindegyikét helyes paritásúra dekódoljuk egy téves kulcs mellett) = 2^{-50}
A szűrésen átment kulcsok átlagos száma a kulcstér teljes végigkeresése után $2^{56} \cdot 2^{-50} = 64 >> 1$

2. a.) $\Phi(m) = 22 * 70 = 1540$

b.) P=0.057, ahol

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

c.) $1540 = 513 \cdot 3 + 1 \rightarrow (-513) \cdot 3 = (-1) \cdot 1540 + 1 \rightarrow d = -513 = 1027 \pmod{1540}$

3.
client hello: kliens véletlenszáma, javasolt algoritmusok listája
server hell: szerver véletlenszáma, választott algoritmus-csokor, Session ID
server certificate: szerver DSA publikus kulcs CA által aláírva
server key exchange: szerver Diffie-Hellman paraméterei DSA kulccsal aláírva
server hello done
client key exchange: kliens Diffie-Hellman paramétere
client finished: eddigi handshake üzeneteken és a mester titkon számolt kulcsolt hash
server finished: eddigi handshake üzeneteken és a mester titkon számolt kulcsolt hash

4.

a) unlinkability of sender and receiver (globális lehallgató ellen), sender anonymity (fogadóval szemben) (1 p – 1 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.

a.) pl. 5-ös szabályt árnyékolja a 3-as
b.) pl. 6-os a 2-essel
c.) pl. 7-es a 4-essel

6.

a.) u1 és u2, mert u1 és a g1 csoport tagjai írhatják az alkönyvtárat
b.) d1-be u1 és a g1 írhat, tehát csak u1 és u2 jön szóba, ők mindketten hozzáférnek a f4 fájlhoz, tehát u1 és u2.
c.) g1 lesz, mert csoport setgid jel van az alkönyvtáron
d.) Az összeset, mert a root felhasználó speciális jogú
e.) u1, ő a tulajdonosa (és a root)