Adatbiztonság ZH Név:
2014. május 12. Neptun kód:

1. Tekintsük a következő mini-rejtjelezőt. A nyílt szövegek tere legyen az {e, f} két elemű halmaz P(e)=1/4 és P(f)=3/4 valószínűségekkel. A kulcstér legyen a {k1, k2, k3} három elemű halmaz P(k1)=1/2, P(k2)=1/4 és P(k3)=1/4 valószínűségekkel. A rejtett szövegek tere legyen az {1, 2, 3, 4}. A kódolás az alábbi táblázat szerint működik (Pl. k2 kulcs esetén az *e* szöveg rejtjelese 2)

	e	f
K1	1	2
K2	2	3
K3	3	4

a.) Mekkora annak valószínűsége, hogy a 3 rejtett szöveg kerül továbbításra? **(2p)**
b.) A lehallgatott rejtett szöveg 3. Mekkora annak valószínűsége, hogy *e* volt a nyílt szöveg? 2p
c.) Definiálja tökéletes rejtjelezőt! Tökéletes-e az adott rejtjelező? **(4p)**

2.
a.) Adja meg a Shamir-féle háromlépéses protokollt, amelynek célja, hogy A fél titkosan továbbíthasson B félnek egy m üzenetet előzetes kulcsegyeztetés nélkül. Támadni képes-e egy középen álló támadó? **(2p)**

b.) Az A fél az $E_{k1}(m) = m+k1$, a B fél az $E_{k2}(m) = m+k2$ rejtjelező transzformációt alkalmazza egyszer használatos k1, k2 kulcsokkal , ahol "+" művelet bitenkénti mod 2 összeadás a bináris blokkok között. Biztonságosan realizáljuk-e a Shamir protokollt? **(4p)**

3. Egy böngésző és egy webszerver a TLS Handshake protokollt használják. A szerver aláírás ellenőrző kulcsot tartalmazó tanusítvánnyal rendelkezik, a kliens nem rendelkezik semilyen tanusítvánnyal. Mi lesz a server-key-exchange és a client-key-exchange üzenetek tartalma, ha
a) RSA alapú kulcscserét használnak? **(4 p)**
b) egyszeri (ephemeral) Diffie-Hellman kulcscserét használnak? **(4 p)**

4. Egy n blokkból álló $M = (m_1, m_2, ..., m_n)$ üzenetet CTR módban rejtjelezünk úgy, hogy a számláló értékét 0-ról indítjuk. A rejtjelezés eredménye a $C = (c_1, c_2, ..., c_n)$ rejtjeles üzenet, amit tárolunk. Később kiderül, hogy az m_i blokkot nem kell tárolnunk, ezért C-t dekódoljuk, az i. blokkot töröljük, és az így kapott $M' = (m_1, ..., m_{i-1}, m_{i+1}, ..., m_n)$ üzenetet újra kódoljuk úgy, hogy a számlálót ismét 0-ról indítjuk és a kulcs is ugyanaz, mint az előző kódolásnál. Legyen a második kódolás eredménye $C' = (c_1, ..., c_{i-1}, c'_i, ..., c'_{n-1})$. Tegyük fel, hogy egy támadó hozzáfér C-hez és C'-höz, és megszerzi a törölt m_i nyílt blokkot is. Fenyegeti-e veszély az M' üzenet titkosságát? **(8 p)**

5. 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 ..
drwxrws---  2 u1   g1   4096 2011-04-22 10:50 d1
drwxr-xr-x  2 u2   g1   4096 2011-04-22 10:50 d2
root@gotcha:/adatbizt# ls -la d1
total 20
drwxrws--- 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---- 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-x 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 olvasni a d1/f3 fájlt és miért? **(2p)**
*b.) mely felhasználóknál fut le sikeresen a cp d1/f1 d2/f6 parancs?***(2p)**
c.) ki tudja módosítani az f3 fájl jogosultságait (pl. chmod o+w d1/f3) **(2p)**
d.) ki tudja törölni az f3 fájlt? **(2p)**

6. UDP portszkennelést végzünk egy gépen, 1000 lehetséges portra. Minden porton egy kísérletet végzünk, és max. 5 másodpercig várunk a válaszra, utána sikertelennek tekintjük a tesztet. A célgépen 100 UDP port van nyitva, ezekről a válasz kéréseinkre 1 másodperc alatt érkezik meg. A tesztelést 5 szálon végezzük el. A szkennelő gép sebességét tekintsük végtelennek.
a.) Mennyi a minimális idő, ami alatt a portszkennelés lefut és miért? **(3p)**
b.) Ha naív módon úgy implementáljuk a szkennelést, hogy előre beosztjuk melyik szál melyik portot fogja ellenőrizni, mekkora lehet a leggyorsabb és a leglassúbb szál futási ideje közötti különbség a legrosszabb esetben? **(4p)**

Pontozás: 1: 0-18, 2: 19-25, 3: 26-32, 4: 33-39, 5: 40-45

Adatbiztonság ZH megoldások
2014. május 12

1.
a.) P(3)=1/4 (=P(3|e)P(e)+P(3|f)P(f)=P(k3)P(e)+P(k2)P(f)=1/16+3/16=1/4)
b.) P(e | 3)=1/4 (=P(3 | e)P(e)/P(3) =P(k3)P(e)/P(3)=(1/4·1/4) /1/4=1/4)
c.) Nem. Pl. P(e | 1)=P(1|e)P(e)/P(1)= 1/2·1/4/(1/4·1/2)= 1 > P(e)

2. Nem biztonságos: passzív támadó is sikeres, mivel a csatornában lehallgatható három rejtett üzenet bináris összege a titok: (m+k1)+(m+k1+k2)+(m+k2)=m

3.
a) server-key-exchange: szerver által frissen generált RSA publikus kulcs, szerver aláírása
client-key-exchange: kliens által generált pre-master secret szerver RSA kulcsával kódolva

b) server-key-exchange: szerver által frissen generált DH publikus paraméterek, szerver aláírása
client-key-exchange: kliens által frissen generált DH publikus paraméter

4. Legyen a számlálóból előállított kulcsblokkok sorozata k_1, k_2, ... Ekkor $c_t = m_t \oplus k_t$ minden $1 \leq t \leq n$ esetén, valamint $c'_i = m_{i+1} \oplus k_i$, $c'_{i+1} = m_{i+2} \oplus k_{i+1}$, stb. Tudjuk továbbá, hogy a támadó ismeri C-t, C'-t, és m_i-t. Így a támadó a következőket tudja kiszámolni:
$k_i = c_i \oplus m_i$
$m_{i+1} = c'_i \oplus k_i$

5.
a.) Az u1 felhasználón és g1 csoporton kívül más nem fér hozzá az alkönyvtárhoz, a fájlhoz mindenkinek van ugyan olvasás joga, de ezért csak u1 és a g1 csoport tagjai: u1 és u2
b.) senkinél, vagy csak az u2 felhasználónál: A d2-be csak u2 írhat, de u2 nem olvashatja az f1 fájlt
c.) csak a tulajdonosa u1 és a root
d.) u1 és u2, a törléshez az alkönyvtárra kell írás jog

6.

a.) A portszkennelés összesen 100 nyitott port esetében 1-1 másodpercig tart (100 sec), 900 zárt portra 5-5 másodpercig (4500 sec), összesen 4600 sec. 5 szálon ezt optimális esetben ez 920 másodperc alatt lefut.

b.) Rossz esetben lesz olyan szál, amelyik 200 db. 5 másodperces futást fog kapni és egyetlen 1 másodperceset sem, így az a szál 200x5 = 1000 másodperc alatt fut le.

Egy szerencsés szál megkapja mind a 100 db. 1 másodperc alatt lefutó feladatot, és így 100 x 1 s + 100 x 5 s = 600 s alatt is végezhet. A különbség 400 s.