# Adatbiztonság PZH

2011. május 10.

1. 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!* **(10p)**

2. Tekintsünk egy szervert és két klienset *A*-t és *B*-t. A kliensek egymást segítve próbálják anonimizálni a szervernek küldött kéréseiket oly módon, hogy mindketten a kéréseiket 1/4 valószínűséggel a másik kliensen keresztül, 3/4 valószínűséggel közvetlenül küldik a szervernek. A továbbításra kapott kéréseket mindketten közvetlenül küldik ki. *A* kliens 1/4 valószínűséggel, *B* kliens 3/4 valószínűséggel bocsát ki kéréseket.
*Melyik esetben nagyobb a szerver bizonytalansága (entrópia) az eredeti küldőre vonatkozóan: (a) ha A-tól vagy (b) ha B-től kap egy kérést? Számítással indokolja válaszát!* **(15p)**

3. RSA rejtjelezés:
a.) Fermat-prímteszt: Melyek a Carmichael számok? Mit tudunk ezen prímteszt szűrési képességéről?
b.) Mi történik, ha RSA dekódolás kapcsán, ha Fermat-álprímet használunk az RSA rejtjelezőnk generálásakor? Mi a helyzet, Carmichael szám esetén? (Formalizált levezetéssel.) **(15p)**

4. Formalizálja, majd vezesse le a CBC mód biztonságával kapcsolatos azon hiányosságot, miszerint ha egy üzenet rejtjelezésekor két rejtjeles blokk megegyezik, akkor következtetni tudunk kapcsolódó nyílt blokkok mod 2 összegére. **(8p)**

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 ..
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)*
b.) *mely felhasználóknál fut le sikeresen a cp d2/f4 d2/f6 parancs?*
c.) *ki tudja módosítani az f2 fájl jogosultságait (pl. chmod o+w d1/f2)*
d.) *ki tudja lefuttatni a rm d1/f3; cp d1/f1 d1/f3 parancsokat mind sikeresen, azaz kitörli f3-at és helyére f1-et másolja?*
e.) *g2 csoport tagjai mely fájlokat tudják olvasni d1 alkönyvtárban (mindegyikük) a fenti eredeti listából?* **(15p)**

6.

Egy rendszergazda az alábbi tűzfalszabályokat állította be a 152.66.249.128/27-es hálózat védelmében egy csomagtovábbító tűzfalon, melyet a rendszer az órán ismertetett módon kezel:

```
src=any, sport=any, dst=152.66.249.135, dport=80, prot=tcp → ALLOW
src=any, sport=any, dst=152.66.249.128/27, dport=22, prot=tcp → ALLOW
src=152.66.249.135, sport=any, dst=any, dport=53, prot=tcp,udp → ALLOW
src=152.66.249.128/27, sport=any, dst=any, dport=69, prot=udp → DROP
src=152.66.249.0/27, sport=any, dst=152.66.249.128/27, dport=161, prot=tcp,udp →
  ALLOW
src=any, sport=any, dst=152.66.149.128/27, dport=161, prot=tcp,udp → DROP
src=any, sport=any, dst=152.66.249.128/27, dport=110,143 prot=tcp → ALLOW
src=any, sport=any, dst=152.66.249.128/27, dport=8090, prot=tcp → DROP
src=152.66.249.0/24, sport=any, dst=152.66.249.128/27, dport=8090, prot=tcp → ALLOW
src=152.66.249.128/27, sport=any, dst=any, dport=any, prot=tcp,udp → ALLOW
src=any, sport=any, dst=152.66.249.128/27 dport=0-1000, prot=tcp → DROP
src=any, sport=any, dst=any dport=any, prot=any → ALLOW
```

A rendszergazda a naplófájlok alapján meglepődve észlelte, hogy a szabályokban valami hiba lehet, mert az alábbi célokat a szabályok nem jól valósították meg. Keresse meg hol van a hiba, miben hibázott a rendszergazda!
A rendszergazda célja volt:
a.) A 152.66.249.0-255 tartományból lehessen a 8090-es TCP portot elérni, máshonnan nem
b.) A védett hálózat felé az SNMP protokollt (161 UDP és TCP portok) a 152.66.249.0/27 hálózatból szabad elérni, máshonnan nem
c.) A nem használt TCP és UDP portok 1000 alatt a védett hálózat irányában tiltva legyenek, amelyekre nincs specifikus egyéb szabály
d.) A DNS szolgáltatás (53-as TCP és UDP port) kívülről elérhető legyen, de csak a DNS szerveren (152.66.249.135) **(12p)**

## Pontozás: 1: 0-29, 2: 30-39, 3: 41-51, 4: 52-63, 5: 64-75

# Adatbiztonság ZH megoldások
**2011. május 10.**

Név:

Neptun kód:

1.

2.

3. RSA:
a.)

b.)

4. CBC:

5.
a.)

b.)

c.)

d.)

e.)

6.
a.)

b.)

c.)

d.)

# Adatbiztonság ZH megoldások

2011. május 10.

**1. feladat**

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 tanusítványa 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!

**2. feladat**

Tekintsünk egy szervert és két klienset $A$-t és $B$-t. A kliensek egymást segítve próbálják anonimizálni a szervernek küldött kéréseiket oly módon, hogy mindketten a kéréseiket $\frac{1}{4}$ valószínűséggel a másik kliensen keresztül, $\frac{3}{4}$ valószínűséggel közvetlenül küldik a szervernek. $A$ kliens $\frac{1}{4}$ valószínűséggel, $B$ kliens $\frac{3}{4}$ valószínűséggel bocsát ki kéréseket. Melyik esetben nagyobb a szerver bizonytalansága (entrópia) az eredeti küldőre vonatkozóan: (a) ha $A$-tól vagy (b) ha $B$-től kap egy kérést? Számítással indokolja válaszát!

**Megoldások**

**1. feladat:** A következő handshake üzenetek kerülnek átvitelre:

| | | |
|---|---|---|
| $C \to S$: | client-hello | : kliens véletlenszáma, javasolt algoritmus-csokrok listája |
| $S \to C$: | server-hello | : szerver véletlenszáma, választott algoritmus-csokor, session ID |
| $S \to C$: | server-certificate | : szerver azonosító, szerver aláírás-ellenőrző kulcsa, CA aláírása |
| $S \to C$: | server-key-exchange | : szerver DH paraméterei: $p, g, g^x \bmod p$, szerver aláírása |
| $S \to C$: | server-hello-done | : |
| $C \to S$: | client-key-exchange | : kilens DH paramétere: $g^y \bmod p$ |
| $C \to S$: | client-finished | : eddigi handshake üzeneteken és a mester titkon számolt MAC |
| $S \to C$: | server-finished | : eddigi handshake üzeneteken és a mester titkon számolt MAC |

**2. feladat:** Jelöljük az eredeti küldőt $\alpha$-val, és azt a hosztot akitől a szerver a kérést megkapja $\omega$-val. Továbbá jelöljük $p_A$-val annak valószínűségét, hogy az eredeti küldő $A$, $p_B$-vel annak valószínűségét, hogy az eredeti küldő $B$, $p_{AB}$-vel annak valószínűségét, hogy $A$ a kérését $B$-n keresztül küldi, és $p_{BA}$-val annak valószínűségét, hogy $B$ a kérését $A$-n keresztül küldi. Tudjuk, hogy $p_A = \frac{1}{4}$, $p_B = \frac{3}{4}$, $p_{AB} = \frac{1}{4}$, $p_{BA} = \frac{1}{4}$. Ekkor:

$$\begin{aligned}
\Pr\{\alpha = A|\omega = A\} &= \frac{\Pr\{\omega = A|\alpha = A\}\Pr\{\alpha = A\}}{\sum_{X\in\{A,B\}}\Pr\{\omega = A|\alpha = X\}\Pr\{\alpha = X\}} \\
&= \frac{(1-p_{AB})p_A}{(1-p_{AB})p_A + p_{BA}p_B} \\
&= \frac{\frac{3}{4}\frac{1}{4}}{\frac{3}{4}\frac{1}{4} + \frac{1}{4}\frac{3}{4}} \\
&= \frac{1}{2}
\end{aligned}$$

Hasonlóan:

$$\begin{aligned}
\Pr\{\alpha = B|\omega = A\} &= \frac{p_{BA}p_B}{(1-p_{AB})p_A + p_{BA}p_B} = \frac{1}{2} \\
\Pr\{\alpha = B|\omega = B\} &= \frac{(1-p_{BA})p_B}{(1-p_{BA})p_B + p_{AB}p_A} = \frac{9}{10} \\
\Pr\{\alpha = A|\omega = B\} &= \frac{p_{AB}p_A}{(1-p_{BA})p_B + p_{AB}p_A} = \frac{1}{10}
\end{aligned}$$

A szerver bizonytalansága az eredeti küldőre vonatkozóan ha $A$ klienstől kapja a kérést:

$$\begin{aligned}
H &= -\sum_{X\in\{A,B\}}\Pr\{\alpha = X|\omega = A\}\log\Pr\{\alpha = X|\omega = A\} \\
&= -2\frac{1}{2}\log\frac{1}{2} = 1
\end{aligned}$$

A szerver bizonytalansága az eredeti küldőre vonatkozóan ha $B$ klienstől kapja a kérést:

$$\begin{aligned}
H &= -\sum_{X\in\{A,B\}}\Pr\{\alpha = X|\omega = B\}\log\Pr\{\alpha = X|\omega = B\} \\
&= -\frac{1}{10}\log\frac{1}{10} - \frac{9}{10}\log\frac{9}{10} \approx 0.47
\end{aligned}$$

**3.** Tk. 431.o. (13.18 feladat)

**4.** Tk. 123.oldal

**5.**

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)
e.) f2,f3

**6.**

a.) pl. Rossz a tiltás és engedélyezés sorrendje, így az engedélyezés nem aktív
b.) A rendszergazda elírta az cél IP tartományt a tiltó szabályban, 249 helyett 149-et írt.
c.) Elfelejtette letiltani az UDP protokoll portjait az 11. (utolsó előtti) szabályban
d.) A harmadik szabályban a cél helyett a forrás lett beírva, vagy más értelmezésben a teljes szabály hiányzik