

1. Feladat (20p)

a.) Definiálja a publikus kulcsú kulcs-tanúsítványt?

b.) Mi a tanúsítvány lánc és mi a feladata? Vázoljon fel egy példát!

c.) Mi a root CA?

e.) Sorolja fel az X.509 szabványú tanúsítvány elemeit (legalább 4 elemet)!

2. Feladat (20p)

a.) Definiálja a kriptográfiai hash függvények ütközésellenálló tulajdonságát.

b.) Tekintsük a $H: \{0,1\}^* \rightarrow \{0,1\}^n$ 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 \mid a bitsorozatok összefűzését jelenti.

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!

3. feladat. (20p)

Egy webszerver és egy böngésző az TLS protokollt használja a HTTP forgalom védelmére. A handshake során RSA alapú kulcscserét szeretnének használni. A szervernek egy RSA publikus rejtjelező kulcsot tartalmazó tanúsítványa van, a kliensnek nincsen tanúsítványa. 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!

4. feladat. (20p)

a) Hogyan működik a duális aláírás a SET protokollban? Rajzolja fel a sémát, és magyarázza el a séma motivációját!

b) Hogyan működik a DigiCash elektronikus készpénz séma? Írja fel a protokoll lépéseit!

c) Sorolja fel az elektronikus fizetési protokollokkal kapcsolatos biztonsági követelményeket (legalább 3 követelményt)!

5. feladat. (20p)

Unix hozzáférésvédelem

Tekintsük az alábbi /etc/passwd file részletet:

```
alice:x:1003:1003:,,,:/home/alice:/bin/bash
bob:x:1004:1004:,,,:/home/bob:/bin/bash
tiger:x:1005:1005:,,,:/home/tiger:/bin/bash
piglet:x:1006:1006:,,,:/home/piglet:/bin/bash
mallory:x:1007:1007:,,,:/home/mallory:/bin/bash
```

Az /etc/group file releváns része:

```
alice:x:1003:
bob:x:1004:alice
tiger:x:1005:
piglet:x:1006:
mallory:x:1007:
winnie:x:1008:tiger,piglet
cryptoland:x:1009:alice,bob,mallory,root
```

A fájl hozzáférési jogosultságok az alábbiak:

```
root@hbgyak:/thewood# ls -la
total 16
drwxrwsr-x 4 root winnie      4096 2010-04-08 11:23 .
drwxr-xr-x 23 root root      4096 2010-04-08 11:30 ..
drwxrwx--x 2 root cryptoland  4096 2010-04-08 11:24 friends
drwxr-x--- 2 alice winnie    4096 2010-04-08 11:25 secrets
```

```
root@hbgyak:/thewood# ls -la friends/
total 20
drwxrwx--x 2 root cryptoland  4096 2010-04-08 11:24 .
drwxrwsr-x 4 root winnie     4096 2010-04-08 11:23 ..
-rwxr--r-- 1 alice winnie     10 2010-04-08 11:26 a1
-rw-r--r-- 1 bob cryptoland   10 2010-04-08 11:26 a2
-rw----- 1 bob cryptoland   10 2010-04-08 11:26 a3
```

```
root@hbgyak:/thewood# ls -la secrets/
total 20
drwxr-x--- 2 alice winnie     4096 2010-04-08 11:25 .
drwxrwsr-x 4 root winnie     4096 2010-04-08 11:23 ..
-rw-rw-r-- 1 alice winnie     10 2010-04-08 11:25 s1
-rw-r----- 1 tiger cryptoland 10 2010-04-08 11:26 s2
-rw-rw-r-- 1 alice winnie     10 2010-04-08 11:39 s3
```

A felhasználók (alice, bob, tiger, piglet, mallory) közül ki tudja végrehajtani sikeresen az alábbi parancsokat, miközben a thewood alkönyvtárban dolgozik:

- cp friends/a1 friends/a4
- cat secrets/s3
- ls -la friends
- cd friends