

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? [7p]
- b.) Milyen valószínűséggel lehet egy jelszót megtippelni, ha háromszor tippelhetünk? [7p]
- c.) Hány jelszót kell kérni a generátortól, hogy nagy (~40%) valószínűséggel legyen két egyforma (ütköző) jelszó? (Segítség: születésnap paradoxon) [6p]

2. Hash függvények:

- a.) Adja meg az iteratív hash függvény blokksémáját (definiálja az elemeket)! [5p]
- b.) Mondja ki az MD padding tételt! [5p]
- c.) Egy H iterációs hash függvényt támadunk.
Nehéz feladat-e $H(m, H_0) = H(m^*, H_0^*)$, $m \neq m^*$ pszeudo ütközést előállítani? [5p]
Mi a válasz, ha DM paddinget is alkalmazunk? [5p]

3. Egy webszerver és egy böngésző a TLS protokollt használja a HTTP forgalom védelmére. Már létrehoztak egy session-t, és a handshake során RSA alapú kulcscsere-t használtak. A szerver digitális aláírás ellenőrző kulcsot tartalmazó tanúsítvánnyal rendelkezik, és nem kérte, hogy a kliens hitelesítse magát. Most a kliens egy új kapcsolatot szeretne nyitni a már létező session-ben, és a szerver ebbe beleegyezik. Adja meg, hogy ebben az esetben mely handshake üzenetek kerülnek átvitelre, és vázlatosan adja meg azok tartalmát! [20p]

4. Tekintse a következő on-line TTP-t használó igazságos (fair) letagadhatatlan kézbesítést biztosító protokollt:

1. $A \rightarrow TTP : E_{TTP}(A, B, m, \text{sig}_A(A, B, h(m)))$
2. $TTP \rightarrow B : A, B, h(m), \text{sig}_{TTP}(A, B, h(m))$
3. $B \rightarrow TTP : E_{TTP}(\text{sig}_B(A, B, h(m)))$
- 4a. $TTP \rightarrow A : \text{sig}_B(A, B, h(m))$
- 4b. $TTP \rightarrow B : m, \text{sig}_A(A, B, h(m))$

Mi a protokoll hibája [3p] és hogyan javítaná ki [7p]?

5. Kis kérdések:

- a.) Mi a lényegi különbség egy csomagszűrő és egy alkalmazás szintű tűzfal között? [2p]
- b.) Definiálja képletszerűen a Kockázatot (Risk)! [3p]
- c.) Jobb-e a túlélési lehetősége egy P2P botnetnek és miért? [2p]
- d.) Soroljon fel legalább 3 szerepvállalót (stakeholder) egy vállalat biztonsági folyamataiban! [3p]

6. 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?

- a) `cp friends/a3 friends/a4` [5p]
- b) `cat secrets/s3` [5p]
- c) `ls -la friends` [5p]
- d) `cd secrets` [5p]