Adatbiztonság a gazdaságinformatikában ZH
2015. december 7.

Név:
Neptun kód:

1. Tekintsük a következő rejtjelező kódolást: nyílt üzenetek halmaza {a,b}, kulcsok halmaza {K1,K2,K3,K4,K5}, rejtett üzenetek halmaza {1,2,3,4,5}. A kódolást a következő mátrix írja le:

	a	b
K1	1	2
K2	2	4
K3	3	1
K4	5	3
K5	4	5

Pl. $E_{k3}(a)=3$. A kulcs valószínűségeloszlása $P_K=\{2/5, 1/5, 1/5, 1/10, 1/10\}$, az üzenet valószínűségeloszlása $P_X=\{1/3, 2/3\}$.
a.) Definiálja a tökéletes rejtjelezést **(2p)**
b.) Tökéletes rejtjelezést valósít meg a adott rejtjelezés? (**4p)**

2.
a) *Definiálja* az OFB blokk rejtjelezési módot (kódolás, dekódolás)! **(2p)**

b) Hitelesített rejtjelezést végzünk a következő módon: az üzenetet hash-eljük, majd az üzenetet és a hash-t együtt rejtjelezzük OFB módban *K* kulccsal és konstans 0 IV-t használva: Formálisan, az *m* üzenethez tartozó hitelesített és rejtjelezett üzenet a $c = E_K(m|h(m))$, ahol a rejtjelezés OFB módban történik (IV = 0).

Mutassuk meg, hogy ha a támadó hozzájut egy (*m; c*) nyílt szöveg – rejtett szöveg párhoz, akkor a K kulcsot is ki tudja számítani. **(3p)**

c) Tetszőleges *m*-mel azonos hosszúságú *m′* üzenethez *elő tudja-e állítani* a $c' = E_K(m'|h(m'))$ hitelesített rejtjelezést! **(3p)**

3.
a.) Definiálja a kriptográfiai hash függvény ütközésellenálló tulajdonságát!
b.) Tekintsük az alábbi $H(x,n) = h_1^{(n)}\left(h_2^{(n)}(x)\right)$ hash függvényt, ahol $h_1^{(n)}$ illetve $h_2^{(n)}$ a h_1 illetve h_2 hash függvények n-szeres alkalmazását jelenti. Milyen n értékekre lesz biztonságos a *H(x,n)* konstrukció, ha tudjuk, hogy
b1.) h_1 ütközés-ellenálló, de h_2 nem ütközés-ellenálló tulajdonságú? **(3p)**
b2.) h_1 nem ütközés-ellenálló, de h_2 ütközés-ellenálló tulajdonságú? **(5p)**
Válaszát, mindkét esetben Indokolja!

4. Tekintsük az alábbi /etc/passwd file részletet:

```
root /vizsga1 #: cat /etc/passwd
doris:x:1001:1001::/home/doris:/bin/bash
alex:x:1002:1002::/home/alex:/bin/bash
bob:x:1003:1004::/home/bob:/bin/bash
```

Az /etc/group fájl a fenti felhasználókra vonatkozó része:

```
root /vizsga1 #: cat /etc/group
doris:x:1001:
alex:x:1002:
teacher:x:1003:doris,alex
bob:x:1004:
works:x:1005:bob,doris
```

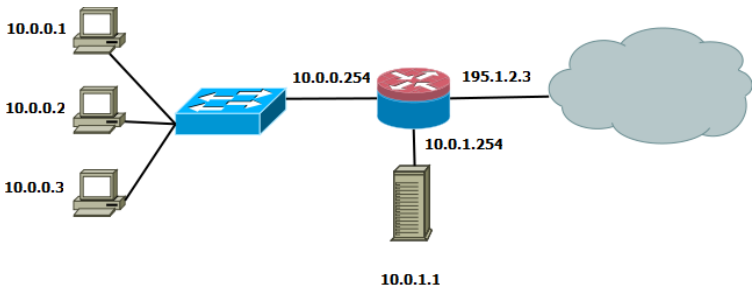
A fájl hozzáférési jogosultságok az alábbiak:

```
root /vizsga1 #: ls -al
drwxr-xr-x  4 root  root    4096 dec    3 15.58 .
drwxr-xr-x 18 root  root    4096 dec    3 15.58 ..
drwxrwsr-x  2 alex  teacher 4096 dec    3 16.13 math
drwxrwxr-x  2 doris works   4096 dec    3 16.37 test

root /vizsga1 #: ls -al math
drwxrwsr-x 2 alex  teacher 4096 dec    3 16.13 .
drwxr-xr-x 4 root  root    4096 dec    3 15.58 ..
-r--rw-r-- 1 doris teacher    9 dec    3 16.13 m1.txt
-rw-rw-r-- 1 doris teacher    9 dec    3 16.12 m2.txt

root /vizsga1 #: ls -al test
drwxrwxr-x 2 doris works 4096 dec    3 16.37 .
drwxr-xr-x 4 root  root  4096 dec    3 15.58 ..
--w-r--r-- 1 alex  doris   11 dec    3 16.30 t1.txt
-rw-r--r-- 1 doris doris   11 dec    3 16.37 t2.txt
--w-rw-rw- 1 bob   bob     11 dec    3 16.28 t3.txt
```

A felhasználók a `vizsga1` directory-ban vannak (a `math` és a `test` directory ez alatt van).

a) Ki írhatja a `math/m1.txt` fájlt? **(2 p)**
b) Melyik felhasználóknak sikeres a `cp test/t1.txt math/m2.txt` parancs **(2 p)**
c) Kik olvashatják a `test/t3.txt` fájlt? **(2 p)**
d) Doris felhasználó (doris aktív csoporttal) készít egy új fájlt a `math` directory-ba (`touch math/m4.txt`), Melyik csoport lesz a tulajdonosa a létrejövő új fájlnak? **(2 p)**

5. Tűzfal feladat



Az ábrán látható elrendezésben szeretnénk a Linux alapú tűzfalat bekonfigurálni. A belső hálózaton a gépek a 10.0.0.0/24 hálózatban vannak. A DMZ-ben (10.0.1.0/24) egy webszerver működik a 10.0.1.1-es címen. A tűzfal lábai a következők: eth0 kifelé, eth1 befelé, eth2 a DMZ irányába. Írjon iptables parancsokat a következő formátumban a részfeladatok megoldásához (a paraméterek sorrendjét lehetőleg ne változtassa meg, az alapértelmezett szabályokra ne alapozzon):

```
iptables [-t TÁBLANÉV] -A LÁNC [-p PROTOCOL] [-i INIF] [-o OUTIF] [-s SOURCE] [--sport SPORT] [-d DESTINATION] [--dport DPORT][--to ADD:PORT] -j ACTION
```

1. A belső hálózaton lévő gépek elérhetik a webszerver HTTP portját (80-as port) a DMZ-ben, és az válaszolhat is, ha az interfészek és a címek megfelelőek (állapotmentes megoldást írjon, 2 parancs) (**2 pont**).

2. A tűzfalon futó SSH szerver (22-es port) csak a belső hálózatból kaphasson csomagot, és a tűzfal mint feladó általában is csak a belső hálózatnak küldhessen csomagot (ügyeljen a megfelelő lánc választásra, az interfészeket nem kell megadni, 4 parancs) (**3 pont**).

3. A webszerver a külső hálózatból is elérhető legyen a nyilvános cím megfelelő portjain (HTTP és HTTPS (443) forgalom is lehetséges legyen, 2 parancs) (**3 pont**)

4. A tűzfalon áthaladó bármilyen LDAP-nak címzett forgalom (389-es port) logolva legyen (1 parancs). (**1 pont**)

5. Sorolja fel, hogy ingress szűrés esetén milyen szabályokra lenne szükség (elég mondatban, nem kell szabály, 2 mondat). (**1 pont**)

Pontozás: 1: 0-16, 2: 17-23, 3: 24-30, 4: 31-35, 5: 36-40

Megoldások
Adatbiztonság a gazdaságinformatikában ZH
2013. december 7.

1.
b) Nem. Pl. $P(Y=1|X=a)=2/5 \neq P(Y=1|X=b)=1/5$, igy X nyilt szöveg es és Y rejtett szöveg valószínűségi változó nem független.

2.
Lényegében kulcsfolyamos rejtjelezést végzünk, s tudjuk, hogy ekkor ismert nyílt szöveg – rejtett szöveg pár esetén kiszámolható a *k* kulcsfolyam:
$m \rightarrow h(m) \rightarrow k = c \oplus (m|h(m))$.
Ezzel a kulcsfolyammal tetszőleges más üzenet kódolható:
$m' \rightarrow h(m') \rightarrow c' = (m'|h(m')) \oplus k$.

3.
b1.) Semmilyen n-re nem lesz biztonságos, mivel a belső hash leképezésre könnyű ütközést előállítani, amit a külső leképezés helyben hagy.

b2.) Ugyan nem nehéz feladat előállítani egy ütköző x, x' h1-ősképpárt, de nehéz feladat ezekből mint h2 hash értékekből h2-ősképeket előállítani (ehhez nem egyirányúnak kellene lennie h2-nek, azonban szokásos szűkítő leképezés dimenziók esetén az ütközésmentesség implikálja az egyirányúságot)

4.

Megoldás:

- **a)** teacher csoportra van írási jog, de doris a tulajdonos!
  Csak **alex (+ root)**
- **b)** **doris (+ root)**
  (bob nem tud írni**,** alex nem tud olvasni**)**
- **c)** **doris, alex (+ root)**
- **d)** **teacher**

5.
1.

a. iptables –A FORWARD –p tcp –i eth1 –o eth2 –s 10.0.0.0/24 –d 10.0.1.1 –dport 80 –j ACCEPT

b. iptables –A FORWARD –p tcp –i eth2 –o eth1 –s 10.0.1.1 –sport 80 –d 10.0.0.0/24 –j ACCEPT

2.

a. iptables –A INPUT –p tcp –s 10.0.0.0/24 –dport 22 –J ACCEPT

b. iptables –A INPUT –p tcp –dport 22 –J DROP

c. iptables –A OUTPUT –d 10.0.0.0/24 –J ACCEPT

d. iptables –A OUTPUT –J DROP

3.

a. iptables –t NAT –A PREROUTING –p tcp –d 195.1.2.3 –dport 80 –to 10.0.1.1:80 –J DNAT

b. iptables –A PREROUTING –p tcp –d 195.1.2.3 –dport 443 –to 10.0.1.1:443 –J DNAT

4.

a. iptables –A FORWARD –dport 389 –j LOG

5.

a. Külső interfészről nem érkezhet csomag belső címes feladóval

b. Külső interfészről nem érkezhet csomag DMZ címes feladóval