

1.

a.) Definiálja az RSA algoritmust! 5p

b.) RSA algoritmus esetén a kulcsok előállításához $p=101$, $q=113$ prímekből indultunk ki.

b1.) Adja meg a lehető legkisebb kódoló kulcsként használható exponenst! 2p

b2.) Határozza meg a dekódoló kulcsot! 5p

c.) Milyen alakú számok között keresné egy RSA rejtjelező publikus kulcsát, ha minimalizálnia kellene a rejtjelezés számításigényét? (Indokoljon) 3p

2.

a.) Definiálja a CBC-MAC algoritmust (képlet vagy blokkséma), s nevezze meg annak biztonsági feladatát! 5p

b.) Mutasson be egy adaptívan választott üzenet alapú támadást CBC-MAC ellen! 10p

3.

Egy webszerver és egy böngésző az TLS protokollt használja a HTTP forgalom védelmére. A handshake során Diffie-Hellman kulcscserét szeretnének használni. A szervernek fix DH paramétereket 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! 15p

4.

Tekintsünk egy szervert és két klienset A-t és B-t. A kliensek azonos valószínűséggel bocsátanak ki kéréseket a szerver felé. A kliensek egymást segítve próbálják anonimizálni a szervernek küldött kéréseiket a következő módon:

- A a kéréseit p_A valószínűséggel B-n keresztül, $1-p_A$ valószínűséggel közvetlenül küldi a szervernek,
- B a kéréseit p_B valószínűséggel A-n keresztül, $1-p_B$ valószínűséggel közvetlenül küldi a szervernek.

Mi a feltétele annak, hogy a fenti rendszer elérje a “gyanún felüli” (beyond suspicion) küldő anonimitási szintet a szerverrel szemben? 10p

Mekkora a szerverrel szembeni küldő anonimitás szintje bitekben mérve (entrópia) ha $p_A = p_B = 1/4$? 10p

5. 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
```

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

- a) cp friends/a1 friends/a4 5p
- b) cat secrets/s3 5p
- c) ls -la friends 5p
- d) cd friends 5p

6.

a.) Adjon meg legalább négyet az IBSZ műszaki-technikai, szakmai védelmi intézkedései fő fejezetének neveiből. 2p

b.) Mi a portscannelés lényege, írja le milyen főbb lépésekből áll ez egyszerű TCP portscan (-sT) esetén! 5p

c.) Miért fontos, hogy digitális aláírás esetén magát az aláírást az üzenet hash értékén végezzük el, és nem magán az üzeneten? 3p

d.) Mondjon legalább három indokot, melyek megalapozzák azt, hogy a Stuxnet malware-t ipari létesítmények ellen, professzionális csoport hozta létre! 5p

Pontozás: 1: < 40 p 2: 40-54 3: 55-69 4: 70 – 84 5: 85-100

Eredmények:

1.a) RSA algoritmus:

1.b1) $e=.....$

1.b2) $d=.....$

1.c)

2a) CBC-MAC:

2b) CBC-MAC támadás:

3) TLS handshake üzenetek és tartalmuk:

4) feltétel:

entrópia:

5) a) `cp friends/a1 friends/a4`

b) `cat secrets/s3`

c) `ls -la friends`

d) `cd friends`

6a) IBSZ:

6a) TCP portscan:

6a) hash:

6a) Stuxnet:

Adatbiztonság ZH, GaIn
Megoldások
November 30, 2010

1.

b1.) $p_1=101$, $p_2=113$

$m = p_1 * p_2 = 101 * 113 = 11413$

$\phi(m) = (p_1-1) * (p_2-1) = 100 * 120 = 11200$

Az exponenssel kapcsolatos feltétel, hogy relatív prím legyen $\phi(m)=2^6 5^2 7$ -hez. A legkisebb ilyen szám a 3.

Tehát $e = 3$.

b2.) euklideszi algoritmussal (egy lépésben): $11200=3733*3+1$, ezért $d= -3733= 7467$.

c.) $e = 2^t + 1$, t pozitív egész.

Indoklás: minimális számú, $t+1$ szorzás művelettel megoldható a rejtjelezés

2. Lásd előadás fóliák, vagy tk. 6.1. pontja

3.

A következő handshake üzenetek kerülnek átvitelre:

$C \rightarrow S$: & client-hello & : kliens véletlenszáma, javasolt algoritmus-csokrok listája \\\

$S \rightarrow C$: & server-hello & : szerver véletlenszáma, választott algoritmus-csokor,
session ID \\\

$S \rightarrow C$: & server-certificate & : szerver azonosító, szerver publikus DH paraméterei,
CA aláírása \\\

$S \rightarrow C$: & server-hello-done & : \\\

$C \rightarrow S$: & client-key-exchange & : kliens DH paraméterei \\\

$C \rightarrow S$: & (change cipher spec) \\\

$C \rightarrow S$: & client-finished & : eddigi handshake üzeneteken és a mester titkon számolt
MAC \\\

$S \rightarrow C$: & (change cipher spec) \\\

$S \rightarrow C$: & server-finished & : eddigi handshake üzeneteken és a mester titkon számolt
MAC \\\

4.

Jelöljük az eredeti küldőt α -val, és azt a hosztot akitől a szerver a kérést megkapja ω -val.

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= \frac{\Pr\{\omega = A|\alpha = A\} \Pr\{\alpha = A\}}{\sum_{X \in \{A,B\}} \Pr\{\omega = A|\alpha = X\} \Pr\{\alpha = X\}} \\ &= \frac{\Pr\{\omega = A|\alpha = A\}}{\sum_{X \in \{A,B\}} \Pr\{\omega = A|\alpha = X\}} \\ &= \frac{1 - p_A}{1 - p_A + p_B}\end{aligned}$$

Hasonlóan:

$$\begin{aligned}\Pr\{\alpha = B|\omega = A\} &= \frac{p_B}{1 - p_A + p_B} \\ \Pr\{\alpha = B|\omega = B\} &= \frac{1 - p_B}{1 - p_B + p_A} \\ \Pr\{\alpha = A|\omega = B\} &= \frac{p_A}{1 - p_B + p_A}\end{aligned}$$

A gyanún felüli anonimitási szint elérésének feltétele a következő:

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= \Pr\{\alpha = B|\omega = A\} \\ \Pr\{\alpha = B|\omega = B\} &= \Pr\{\alpha = A|\omega = B\}\end{aligned}$$

Ez akkor és csak akkor teljesül, ha $p_A + p_B = 1$.

Ha $p_A = p_B = \frac{1}{4}$, akkor

$$\begin{aligned}\Pr\{\alpha = A|\omega = A\} &= 1 - p_A = \frac{3}{4} \\ \Pr\{\alpha = B|\omega = A\} &= p_B = \frac{1}{4}\end{aligned}$$

Ebből az entrópia a következő módon számolható:

$$\begin{aligned}H &= - \sum_{X \in \{A,B\}} \Pr\{\alpha = X|\omega = A\} \log \Pr\{\alpha = X|\omega = A\} \\ &= -\frac{1}{4} \log \frac{1}{4} - \frac{3}{4} \log \frac{3}{4} \\ &= 0.25 * 2 + 0.75 * 0.415 \\ &= 0.81125\end{aligned}$$

5.

- a.) alice,bob,mallory
- b.) alice,tiger,piglet
- c.) alice,bob,mallory
- d.) alice,bob,tiger,piglet,mallory

6.

- a.) Infrastruktúrához kapcsolódó védelmi intézkedések; Hardverekhez kapcsolódó védelmi intézkedések; Adathordozókhoz kapcsolódó védelmi intézkedések; Dokumentumokhoz kapcsolódó védelmi intézkedések; Szoftverekhez kapcsolódó védelmi intézkedések; Adatokhoz kapcsolódó védelmi intézkedések; Kommunikációhoz kapcsolódó védelmi intézkedések; Személyekhez kapcsolódó védelmi intézkedések;
- b.) A rendszeren rendelkezésre álló szolgáltatások (nyitott portok) feltérképezése. TCP scan esetén a kliens oldal egy TCP Syn csomagot küld, nyitott port esetén a kapott Ack csomag után a kapcsolatot rendesen lezárja (Ack-t küld, majd RST csomagot).
- c.) Az elsődleges ok, hogy a digitális aláírás kiszámítása erőforrás-igényes, a hash számítás gyors. A jelzett kombináció kevesebb erőforrást emészt fel.
- d.) Több nem ismert (0-day) sérülékenységet tartalmazott, amelyhez felfedezése nehéz.
 - PLC-t is tartalmazó rendszerbe próbált kódot injektálni.
 - USB kulcsra is fertőz, hogy internettel nem rendelkező helyeken, pl. ipari létesítményben is terjedhessen.
 - A PLC rendszerben azonosítókat keres, egy konkrét célpontra lett megírva.
 - A Realtek, JMicron aláírásával rendelkező drivert használt fel, amelyet megszerezni nehéz.