Adatbiztonság pótZH Név:
2014. május 22. Neptun kód:

1. RSA rejtjelezést tekintünk.

a) Egy *a,b* természetes számpárra milyen feltételeknek kell teljesülniük, hogy a rejtjelezésben az egyik a kódoló exponens szerepét játszhassa, miközben a másik a dekódoló exponens szerepét játsza és szerepük felcserélhető? **(3p)**
b) Nevezzen meg egy speciális esetet, amikor a hatékony rejtjelezés érdekében könnyű eldönteni, hogy a számpár melyik tagjának milyen szerepet szánunk! **(3p)**
c) Lehetséges-e, hogy a számpár egyik tagja páros szám legyen? Indokoljon! **(2p)**

2. Tegyük fel, hogy egy A számítógép egy S időszervertől a következő protokollt használva kéri le a pontos időt:

A → S : A, N
S → A : T, sig_S(A, N, T)

ahol T jelöli a pontos időt, sig_S(m) S aláírása az m adaton, és N egy sorozatszám, melyet A minden kérésnél eggyel növel. Konstruáljon támadást a protokoll ellen, ami kihasználja, hogy N predikálható! **(8p)**

3. Olyan jelszavas hitelesítő rendszerünk van, ahol a felhasználó jelszavát négy, a felhasználó által választott w_1, w_2, w_3, w_4 szó alkotja. A rendszer a felhasználó minden w_i szavához véletlen módon választ 63 ún. decoy szót, legyenek ezek $d_{i,1}$, $d_{i,2}$, …, $d_{i,63}$, és a négy decoy halmazt tárolja a jelszóval együtt. A hitelesítés négy körben történik. Az ellenőrző rendszer az *i*. körben megjeleníti w_i-t és a $d_{i,1}$, $d_{i,2}$, …, $d_{i,63}$ szavakat, de nem sorrendben, hanem valamilyen véletlen permutációban (pl. 8x8-as elrendezésben). A hitelesítés akkor sikeres, ha a felhasználó minden körben sikeresen kiválasztja a megjelenített szavak közül a saját szavát. Mekkora az on-line próbálgatást használó támadás átlagos komplexitása, ha

a) az ellenőrző egy sikertelen kör után azonnal hibát jelez és megszakítja a hitelesítést? **(3p)**
b) az ellenőrző csak a negyedik kör végén ad információt a hitelesítés eredményéről? **(3p)**
c) Hasonlítsa az a) és b) esetek erősségét egy 8 karakterből álló átlagos felhasználó által választott jelszó erősségéhez? **(2p)**

4. Egy webszerver és egy böngésző a TLS 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! **(8p)**

5. Tekintsünk egy szervert, amely 4 kbyte méretű leveleket 3 db/sec sebességgel tud feldolgozni. A szerver egy 10240(letöltés)/2048(feltöltés) kbit/sec sebességű vonal ügyfél oldali végén van. Egy támadó folyamatosan leveleket küld a szerverre DoS támadási célzattal, olyan sebességgel, hogy a szerver kapacitását pontosan 100%-ban kösse le. A levél átvitele során 20% overhead (többlet) keletkezik a TCP/IP működése miatt.

a) Hány százalékában használja ki a támadó a csatorna letöltés irányát támadás közben? **(3p)**
b) Ha a támadó inkább SYN elárasztást választ, hány packet/sec sebességgel kell támadnia, hogy a csatorna letöltés irányát 500% mértékű túlterhelés érje, feltételezve, hogy egy TCP SYN adatcsomag 66 byte méretű? **(4p)**

6. Tekintsük az alábbi példát egy tűzfalszabályra:

```
iptables -A INPUT -j REJECT -s 1.2.3.4 -p tcp --dport 80 -d 0/0 -i eth0
```

A szabály azokra a csomagokra definiál elutasítást, amelyek az 1.2.3.4 címről jöttek a gépünkre, a web portra, bármelyik általunk használt címen, de csak akkor, ha az eth0 interfészen érkeztek.

Írjon szabályt az alábbiakra:

a.) az SSH forgalom engedélyezése gépünkre bárhonnan **(2p)**
b.) az 5.6.7.8-as számú gépről tilos icmp adatot továbbítani (FORWARD) a 10.10.1.1 gép felé **(2p)**
c.) az UDP 53-as port (DNS) engedélyezett bárhonnan, de csak a szerverünk 152.66.249.135-ös IP száma irányában. **(2p)**

Pontozás: 1: 0-18, 2: 19-25, 3: 26-32, 4: 33-39, 5: 40-45

Adatbiztonság pót ZH megoldások
2014. május 22.

1. Megoldás
a) $1 \leq a < \varphi(m)$, $1 \leq b < \varphi(m)$, $(a, \varphi(m)) = 1$, $(b, \varphi(m)) = 1$, $ab = 1 \pmod{\varphi(m)}$
b) Ha az egyik kitevő 2^r+1 alakú, akkor azt érdemes publikus exponensnek választani, mert azzal gyorsan lehet titkosítani (r négyzetre emelés és 1 szorzás).
c) Nem. a és b közül egyik sem lehet páros, mert relatív prímek kell legyenek $\varphi(m)$-hez, $\varphi(m)$ pedig páros szám, így ha a vagy b páros lenne, akkor a 2 közös osztójuk lenne.

2. Megoldás:
T időpontban X lekéri a pontos időt A nevében a következő sorozatszámot használva:

X/A -> S : A, N
S -> X/A : T, sigS(A, N, T)

T' > T időpontban A szeretné lekérni a pontos időt. X elfogja A kérését és válaszol:

A -> X/S : A, N
X/S -> A : T, sigS(A, N, T)

A azt hiszi a pontos idő T, miközben az már T'.

3. Megoldás:
a) $\frac{1}{2} \times 4 \times 2^6 = 2^7$
b) $\frac{1}{2} \times (2^6)^4 = 2^{23}$
c) Átlagos felhasználó által választott jelszó erőssége: 4 + 7*2 = 18 bit, tehát erősebb mint a) és gyengébb mint b)

4. Megoldás:
client hello: kliens véletlenszáma, javasolt algoritmusok listája
server hello: szerver véletlenszáma, választott alégoritmus-csokor, Session ID
server certificate: szerver DSA publikus kulcs CA által aláírva
server key exchange: szerver Diffie-Hellman paraméterei DSA kulccsal aláírva
server hello done
client key exchange: kliens Diffie-Hellman paramétere
client finished: eddigi handshake üzeneteken és a mester titkon számolt kulcsolt hash
server finished: eddigi handshake üzeneteken és a mester titkon számolt kulcsolt hash

5. Megoldás:
a) 11520/10240 ~ 1.15%
b) 51200000/528 ~ 100000

6. Megoldás:
a) `iptables -A INPUT -j ACCEPT -p tcp --dport 22`
b) `iptables -A FORWARD -j REJECT -s 5.6.7.8 -d 10.10.1.1`
c) `iptables -A INPUT -p udp --dport 53 -d 152.66.249.135 -j ACCEPT`