Adatbiztonság ZH Név:
2012. május 8 Neptun kód:

1. Tekintsünk egy mini-RSA rejtjelezőt p1=101 és p2=103 prímekkel. Tegyük fel, hogy egy támadó megfigyelt egy x dokumentumot és a hozzátartozó RSA aláírást, ahol az x dokumentum egy RSA blokk hosszúságú. A támadó úgy szeretné feltörni az aláíró algoritmust (kitalálni az aláíró kulcsot), hogy arra számít, hogy az x dokumentum (természetes szám ábrázolásban) nem relatív prím a modulussal. Nagyobb-e a sikere esélye, mint egy 4 decimális számjegyből álló PIN kód véletlen eltalálásának? (7 pont)

2. Bináris üzenetfolyam bitjeit kulcsfolyamatos rejtjelezéssel rejtjelezzük: Van egy kulcsfolyam és egy üzenetfolyam; az egyes üzenetbitekhez a kulcsfolyam egyes bitjeit adjuk modulo 2: y=x+k mod 2. A üzenetfolyamon illetve a kulcsfolyamon belül a bitek függetlenek, és a két folyam független. Az üzenetbitek eloszlása P(x=0)=1/2, P(x=1)=1/2, a kulcsbitek eloszlása P(k=0)=3/4, P(k=1)=1/4.
Péter a következőt állítja: mivel az üzenetbitek pénzfeldobás-sorozatot alkotnak, továbbá a mod 2 összeadásos rejtjelezés kommutatív, a rejtjelezés tökéletes (shannon-i értelemben).
a.) Definiálja a tökéletes rejtjelezést. (2p)
a.) Pénzfeldobás-sorozatot alkot-e a rejtjelezett szöveg? (4 p)
b.) Tökéletes-e a rejtjelezés? (számítással indokoljon) (5 p)

3. Egy webszerver és egy böngésző a TLS protokollt használja a HTTP forgalom védelmére. A handshake során RSA alapú kulcscserében egyeznek meg. A szerver digitális aláírás ellenőrző kulcsot tartalmazó tanúsítvánnyal rendelkezik, és nem kéri, hogy a kliens hitelesítse magát. Adja meg, hogy ebben az esetben mely handshake üzenetek kerülnek átvitelre, és vázlatosan adja meg azok tartalmát! (8 p)

4. Egy n karakterből álló $M = (m_1, m_2, \ldots, m_n)$ üzenetet OFB módban kódolunk és az eredményül kapott $C = (c_1, c_2, \ldots, c_n)$ rejtjeles üzenetet tároljuk. Később kiderül, hogy az i. karaktert nem kell tárolnunk, ezért C-t dekódoljuk, az i. karaktert töröljük, és az így kapott $M' = (m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n)$ üzenetet újra kódoljuk. Legyen a második kódolás eredménye $C' = (c'_1, c'_2, \ldots, c'_{n-1})$. A második kódolás során ugyanazt a kezdeti értéket (IV) és kulcsot használjuk, mint az első kódolásnál. (Vegyük észre, hogy ekkor minden $0 < t < i$ esetén $c'_t = c_t$, ezért lényegében az első i-1 karaktert nem is kell újra kódolnunk.) Tegyük fel, hogy egy támadó hozzáfér C-hez és C'-höz, és megtudja a törölt m_i karakter értékét is. Fenyegeti-e veszély az M' üzenet titkosságát? Válaszát indokolja! (10 p)

5. Az Anonymous támadást próbál intézni a root DNS serverek ellen. 205 servert próbál leterhelni erősített (amplified) DNS támadás által, a sávszélesség elfoglalását célozva. Tegyük fel, hogy minden szerver szimmetrikus gigabit/s kapcsolattal rendelkezik és ez a bottleneck kapacitás. Tegyük fel, hogy 1 megabit/s szimmetrikus kapacitású támadó barátokat toboroznak, és végtelen kapacitású DNS szervereket használnak a hárított-erősített támadásra. Az erősítést úgy érik el, hogy 60 byte-os IP query csomagra a DNS hosztok 4000 byte adatot (overhead-del) küldenek a célszerverekre. A támadást teljesen, egyenletesen elosztják a célpontok között. Úgy becsli a társaság, hogy tízszeresen kell túlterhelni a DNS root szervereket a tartós siker érdekében, akár hosszabb távon is. Összesen kb. hány ilyen tag közreműködésére van szükség a sikeres támadáshoz? Válaszát indokolja! (10 p)

6. Keressen példát az alábbi tűzfal szabályhalmazban a következő inkonzisztenciatípusokra, és válaszát röviden indokolja!

a.) Shadowing (3p)
b.) Generalization (3p)
c.) Correlation (3p)

#	prot	source	destination	action
1.	tcp	10.1.1.0/25	any	deny
2.	udp	any	192.168.1.0/24	accept
3.	tcp	10.1.1.128/25	any	deny
4.	udp	172.16.1.0/24	192.168.1.0/24	deny
5.	tcp	10.1.1.0/24	any	accept
6.	udp	10.1.1.0/24	192.168.0.0/16	deny
7.	udp	172.16.1.0/24	any	accept

Pontozás: 1: 0-21, 2: 22-29, 3: 30-38, 4: 39-46, 5: 47-55

Adatbiztonság ZH megoldások
2012.május 8

1.
a.) igen nem indoklás:

2.
a.) igen nem indoklás:

b.) igen nem indoklás:

3.

4. igen nem indoklás:

5.

6.

Adatbiztonság ZH megoldások

2012.május 8

1. Igen

$$P = \frac{m - \Phi(m)}{m} = 1 - \frac{(p_1 - 1)(p_2 - 1)}{p_1 p_2} = 1 - \frac{(p_1 p_2 - p_1 - p_2 + 1)}{p_1 p_2} = \frac{1}{p_1} + \frac{1}{p_2} - \frac{1}{p_1 p_2}$$

$>> 10^{-4}$

2.

a.) Igen. A rejtjeles szöveg eloszlása ugyanaz marad mint OTP esetén: kommutatív művelet, s az egyik operandus pénzfeldobás-sorozat.

b.) Nem. A nyilt szöveg bemenet és a rejtett szöveg kimenet nem független:
P(y=0|x=0)=P(k=0)=3/4, P(y=0|x=1)=P(k=1)=1/4.

3.

A következő handshake üzenetek kerülnek átvitelre:
C → S: client-hello : kliens véletlenszáma, javasolt algoritmus-csokrok listája \\
S → C: server-hello : szerver véletlenszáma, választott algoritmus-csokor, session ID \\
S → C: server-certificate : szerver azonosító, szerver aláírás ellenőrző kulcsa, CA aláírása\\
S → C: server-key-exchange : szerver frissen generált RSA rejtjelező kulcsa, szerver aláírása \\
S → C: server-hello-done : \\
C → S: client-key-exchange : szerver RSA kulcsával rejtjelezett pre-master secret \\
C → S: (change cipher spec) \\
C → S: client-finished : eddigi handshake üzeneteken és a mester titkon számolt MAC \\
S → C: (change cipher spec) \\
S → C: server-finished : eddigi handshake üzeneteken és a mester titkon számolt MAC \\

4.

Legyen az OFB által generált kulcskarakterek sorozata k_1, k_2, …. Ekkor $c_t = m_t + k_t$ minden $t = 1, 2, \ldots, n$ esetén, valamint $c'_i = m_{i+1} + k_i$, $c'_{i+1} = m_{i+2} + k_{i+1}$, stb.
A támadó a következőket tudja kiszámolni:

$k_i = c_i + m_i$
$m_{i+1} = c'_i + k_i$
$k_{i+1} = c_{i+1} + m_{i+1}$
$m_{i+2} = c'_{i+1} + k_{i+1}$
…

A támadó tehát dekódolni tudja az m_{i+1}, m_{i+2}, …, m_n karaktereket, azaz komoly veszély fenyegeti az M' titkosságát ha $i < n$.

5.

205 site kapacitása 205 gigabit/s. Tízszeres túlterhelésük 2050 gigabit/s. 4000/60 az erősítési arány, ami kb. 66,7. Így 2050 000 Mbit/sec /66.7 = 30 745 Mbit/sec (31 472 Mbit/s, ha 1024-gyel számolunk) forgalom erősítés előtt. Egy tag 1 Mbit/s-re képes, így kb. 30 745 ember kell sikeres támadáshoz. Természetesen a való életben ez nem biztos, hogy igaz és hosszú távon (napok, hetek) kellene képesnek lennie támadniuk, miközben bűncselekményt követnek el. (A gigabit/megabit átváltásnál mind 1000 mind 1024-es váltószámot elfogadunk)

6.

a. shadowing e.g., **rule 4** is shadowed by **rule 2**; **rule 5** is shadowed by *combination* of **rule 1** and **rule 3**;
b. generalization e.g., **rule 7** is a generalization of **rule 4,…**
c. correlation pl. **rule 2** and **rule 6** are correlated