Adatbiztonság ZH Név:
2013. május 16 Neptun kód:

1. Tekintsen egy ElGamal rejtjelezőt mod 11 szorzócsoport felett g=2 primitív elemmel. Legyen a titkos kulcs x = 7. Tegyük fel, hogy a véletlen generátorán a következő output 6.

a.) Definiálja az ElGamal rejtjelezést (kódolás, dekódolás)! **(3p)**
b) Adja meg a nyilvános kulcsot! **(2p)**
c.) Kódolja az m=5 nyílt szöveget! **(2p)**
d.) Dekódolja a (9,8) rejtett szöveget! **(3p)**

2. a.) CBC-MAC definiciója (folyamatábra, formula, a jelölések magyarázatával) **(3p)**

b.) Definiáljuk egy üzenethitelesítő (MAC) konstrukciót az alábbi módon. Adott egy CBC-MAC eljárás, amely *n* bithosszú blokkokra osztja a bemenetét. Mielőtt egy *m* üzenet CBC-MAC értékét kiszámolnánk a hagyományos módon, kiegészítjük az üzenetet vagy egy 1^n blokkal (*n* hosszú csupa 1), ha *m* páratlan számú blokkra osztható fel, vagy egy 0^n blokkal (*n* hosszú csupa 0), ha *m* páros számú blokkra osztható fel. Az ilyen módon kiegészített adat CBC-MAC értéke lesz az *m* üzenet hitelesítő kódja.

Biztonságos-e a konstrukció? Miért? **(7p)**

3. Az AWP (Another Weak Protocol) célja két távoli fél között átküldött üzenetek titkosítása, integritásvédelme, és a visszajátszás elleni védelem. Feltesszük, hogy a felek között már van egy megosztott 128 bites K szimmetrikus kapcsolatkulcs. Egy M üzenet integritásvédő ellenőrző-összegét úgy számoljuk ki, hogy M-et 128 bites M_i (i = 1, 2, …) blokkokra osztjuk, ha az utolsó blokk, M_{last} rövidebb 128 bitnél, akkor 0 bitekkel 128 bitre egészítjük ki, majd az így kapott blokkok (bitenkénti) XOR összegét számolva kapjuk az ellenőrző-összeget: $ICV = M_1 + M_2 + ... + M_{last}$ (ahol + jelöli az XOR-t). Ezután az ICV-t az eredeti üzenet végére csatoljuk, és az (M | ICV) bitsorozatot rejtjelezzük AES rejtjelezővel CTR módban. A rejtjelezésnél használt számláló kezdeti értéke C, és a számlálót minden blokk rejtjelezése után eggyel növeljük. A kezdő C értéket a csomag fejlécében küldjük át a vevőnek, így az átküldött csomag formátuma a következő: C | $AES\text{-}CTR_{K,C}$(M | ICV), ahol $AES\text{-}CTR_{K,C}$() jelöli az AES-sel történő CTR módú rejtjelezést K kulccsal és C kezdeti számláló értékkel. A kapcsolat kezdetén (az első üzenet küldésekor) C-t 0-ról indítjuk, majd minden üzenet küldésekor eggyel növeljük. Így C üzenetsorszámként is funkcionál, s ez biztosítja a visszajátszás elleni védelmet. Új kapcsolat esetén új K kapcsolatkulcsot használunk, s C-t ismét 0-ról indítjuk.

Konstruáljon támadást az AWP protokoll integritásvédelmi mechanizmusa ellen **(4p)** *és titkosítási eljárása ellen* **(6p)***!*

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

5. Egy spamszűrő az órán ismertetett Bayes szűrést használja. Feltételezi, hogy Pr(S)=Pr(W)=0,5. Adatbázisa a következő adatokat tanulta meg:
Pr(gyors|S)=0,01 Pr(hatékony|S)=0,01 Pr(defektjavítás|S)=0,05
Pr(gyors|H)=0,001 Pr(hatékony|H)=0,005 Pr(defektjavítás|H)=0,1

Adott egy levél: „Gyors, hatékony defektjavítás" tartalommal.
Mekkora az esélye, hogy a levél spam? Számolja ki az órán tanult módon a levél kombinált spam-valószínűségét (három tizedes jegy precizitású részszámítások elegendőek)! **(10p)**

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

No.	Proto	Src	Dst	Decision
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

a.) Shadowing **(2p)**

b.) Generalization **(2p)**

c.) Correlation **(2p)**

Pontozás: 1: 0-19, 2: 20-27, 3: 28-35, 4: 36-43, 5: 44-52

Adatbiztonság ZH megoldások

2013.május 16

1. a.) Tk.371.o

b.) $b=2^7=7 \pmod{11}$

c.) rejtett szöveg=$(2^6, 2^{6\cdot 7} \cdot 5)=(9, 2^2 \cdot 5)=(9,9) \pmod{11}$

d.) nyílt szöveg=$8 \cdot 9^{-7}=8\cdot(9^{-1})^7=8\cdot(5)^7=8\cdot5\cdot5^2\cdot5^2\cdot5^2=8\cdot5\cdot3\cdot3\cdot3=2$

2. b. Nem biztonságos.
MAC orákulum kérések: m_1 üzenet MAC-je $MAC_k(m_1)$, m_2 üzenet MAC-je $MAC_k(m_2)$, ahol m_1 és m_2 egy blokk méretű.
Támadás:Legyen $m_3=m_1 | 1^n | MAC_k(m_1) + m_2$, ahol + mod 2 bitekénti összeadás.
$MAC_k(m_3)= MAC_k(m_2)$.

3. Páros számú blokk azonos módosítását nem detektálja az integritásvédelmi mechanizmus ($M_1+X+M_2+X+M_3+\ldots+M_{last} = M_1+M_2+M_3+\ldots+M_{last}$).
Továbbá a blokkokon könnyű célzott módosítást végezni a kulcsfolyam-rejtjelezés miatt (M+Q+M' = (M+M')+Q, ahol Q az AES-CTR által generált kulcsfolyam).

Két egymást követő üzenet kódolásához használt két kulcsfolyam nagy mértékben átfed (azonos). Pl. a C. üzenethez használt kulcsfolyam: $AES_K(C)$, $AES_K(C+1)$, $AES_K(C+2)$, ... és a C+1. üzenethez használt kulcsfolyam: $AES_K(C+1)$, $AES_K(C+2)$, ... Ezért az első kódolt üzenet i+1. és a második kódolt üzenet i. blokkját XOR-olva, a nyílt üzenetek megfelelő blokkjainak XOR összegét kapjuk: $Y_{i+1} + Y'_i = (M_{i+1}+AES_K(C+i)) + (M'_i+AES_K(C+i)) = M_{i+1}+ M'_i$. Ha ismerjük az egyik üzenetet, akkor ebből ki tudjuk számítani a másikat.

4.
a) ½ x 4 x $2^6 = 2^7$
b) ½ x $(2^6)^4 = 2^{23}$
c) Átlagos felhasználó által választott jelszó erőssége: 4 + 7*2 = 18 bit, tehát erősebb mint a) és gyengébb mint b)

5. Egyedi valószínűségek:
Pr(S|gyors)=Pr(gyors|S)/(Pr(gyors|S)+Pr(gyors|H)) = 0,01 / (0,01+0,001)=0,909
Pr(S|hatékony)= 0,01/ (0,01+0,005)=0,667
Pr(S|defektjavítás)= 0,05/(0,05+0,1)=0,333

p= Pr(S|gyors)* Pr(S|hatékony)* Pr(S|defektjavítás) /
(Pr(S|gyors)* Pr(S|hatékony)* Pr(S|defektjavítás) + (1-Pr(S|gyors))* (1-Pr(S|hatékony))*(1-Pr(S|defektjavítás))

azaz p= 0,202/ (0,202 + 0,02) = 0,202/0,222=90,991%

6.

a.) pl. 4-es szabályt árnyékolja a 2-es
b.) pl. 7-es a 4-est
c.) pl. 2-es a 6-ossal