

# Pótzh Megoldások

2010. május 14.

## 1. feladat

1. **Nem.** Annak a valószínűsége, hogy egy téves kulccsal helyes paritásúra dekódolunk egy rejtett szöveg blokkot,  $2^{-4}$ . Annak a valószínűsége, hogy például 12 rejtjeles blokk mindegyikét helyes paritásúra dekódoljuk téves kulcs mellett  $2^{-48}$ , tehát a nem kiszűrt téves kulcsok átlagos száma a kulctér teljes végigkeresése után  $2^{56} \times 2^{-48} = 2^8 = 256$  lenne.

## 2. feladat

a) **Nem.**

1. C megfigyel egy előző, A és B közötti lefutását a protokollnak, s tárolja a 3. lépésbeli  $z_1$  ( illetve  $z_2$  ) - et. Mivel nem változik lefutásonként  $z_1$  ( $z_2$ ), ezért triviálisan meg tudja személyesíteni A vagy B felet a másik előtt (visszajátszásos támadás). Ezen időpecséttel segíthetnénk.
2. Sőt a jelszavakat is meg tudja állapítani: A helyére lép, és az első lépést

$$1'. A(C) \rightarrow B : ID_A, k_C^p$$

lépésre cseréli. Sikeresen végigjut az összes lépésen, s az 5. lépésben megkapja a  $P_B$  jelszót. Ezen már időpecséttel sem segíthetnénk.

b) **Nem.** Ekkor az a1.) támadás még működik, de  $z_1$  illetve  $z_2$ -ben alkalmazott időpecséttel (sorszámozással) megakadályozható. Ha mégis szükség van a nyilvános kulcsok cseréjére, akkor 1. illetve 2. lépésben küldjük át a kulcsátvitványt is

## 3. feladat

- $(M|CRC(M)) \oplus K$ , ahol M az üzenet és K az aktuális IV-ből és a WEP kulcsból generált kulcsfolyam (az RC4 kiemelte)

- A támadó tetszőleges  $\Delta M$ -hez kiszámolja  $(\Delta M|CRC(\Delta M))$ -et, majd ezt XOR-olja az eredeti üzenethez:

$$\begin{aligned} ((M|CRC(M)) \oplus K) \oplus (\Delta M|CRC(\Delta M)) &= \\ ((M \oplus \Delta M)|(CRC(M) \oplus CRC(\Delta M))) \oplus K &= \\ ((M \oplus \Delta M)|CRC(M \oplus \Delta M)) \oplus K & \end{aligned}$$

ahol kihasználtuk, hogy a CRC függvény lineáris az XOR-ra nézve, azaz:  
 $CRC(X \oplus Y) = CRC(X) \oplus CRC(Y)$

- Schogyan.
- Az IV-t üzenetsorszámként használhatnánk: a küldő minden üzenet elküldésekor növelné a sorszámot, a vevő csak olyan üzenetet fogadna el, melynek sorszáma nagyobb az eddig vett legnagyobb sorszámnál.

#### 4. feladat

- Shadowing: pl. 2-es szabály leárnyékolja 4-es szabályt; 1-es és 3-as szabály közösen leárnyékolja az 5-ös szabályt.
- Generalization: pl. 7-es szabály a 4-esnek az "általánosítása".
- Correlation: pl. 2-es és a 6-os szabály korrelál.

#### 5. feladat

- Az egyedi szavak előfordulási valószínűségeit a spam és ham üzenetek tekintetében
- Nehezebb tervezés, nagyobb késleltetés a parncsoknál.
- A csomagszűrő nem tud belenézni a csomagok belsejébe.