Hálózatbiztonsági protokollok

pótzárthelyi feladatok
2003 december 11.

1. feladat

Bizonyítsa be, hogy egy Feistel struktúrájú rejtjelező mindig invertálható, még akkor is ha az F réteg-függvény nem invertálható.

2. feladat

Mutassa meg, hogy a csupa 0 bitből álló kulcs egy gyenge DES kulcs.

3. feladat

Legyen $P = P_1|P_2|\ldots|P_N$ egy N blokkból álló nyíltszöveg. P-t CBC módban rejtjelezzük egy K kulccsal és egy IV kezdeti változóval. Az eredmény legyen az N blokkból álló $C = C_1|C_2|\ldots|C_N$ rejtettszöveg. Tegyük fel, hogy egy támadó megszerzi P-t és C-t, valamint megfigyel egy másik, M blokkból álló $C' = C'_1|C'_2|\ldots|C'_M$ rejtettszöveget, melyről azt is tudja, hogy szintén CBC módot használva ugyanazzal a K kulccsal de különböző kezdeti változóval állították elő, mint C-t. Tegyük fel továbbá, hogy C_i megegyezik C'_j-vel valamely i-re és j-re, ahol $1 < i \leq N$ és $1 < j \leq M$.

- Mutassa meg, hogy ekkor a támadó meg tudja fejteni P'_j-t (azaz a C' rejtettszöveghez tartozó nyíltszöveg j. blokkját). [0.4 pont]
- Mekkora annak a valószínűsége, hogy a támadó által megfigyelt M blokkból álló C' legalább egy blokkja megegyezik a támadó által ismert, N blokkból álló C valamely blokkjával, ha a blokkméret n bit és C minden blokkja különböző? [0.6 pont]

4. feladat

Tegyük fel, hogy egy h iterált hash-függvény kimenetének mérete 64 bit és így a hash-függvény nem ütközésmentes (collision resistant)[1]. Valaki úgy próbálja h kimenetének méretét megnövelni, hogy kimenetként nemcsak az utolsó, hanem az utolsó két láncváltozó (chaining variable – CV) értékét használja. Az így nyert h' hash-függvényre tehát:

$$h'(x) = CV_{L-1}|CV_L$$

Bizonyítsa be, hogy h' nem lesz ütközésmentes!

5. feladat

Tekintsük az X9.17 véletlenszám generátort. Adja meg a backtracking támadás algoritmusát (azaz hogyan lehet K, $seed_{i+1}$, és $output_i$ valamely ismert, de nem invertálható f függvénye ismeretében meghatározni $output_i$ és $seed_i$ értékét).

6. feladat

Javítsa ki a nyílvános-kulcsú Needham-Schröder protokollt, hogy az ellenálljon a Lowe-féle támadásnak.

[1] 2^{32}, azaz kb. 4 milliárd üzenet közül nagy valószínűséggel lesz kettő melyeknek ugyanaz a hash-értéke.