Kodowanie i bezpieczeństwo informacji

Lista nr 2 na 5 III - 16 III 2012

Zadanie 1 Jaki jest wynik działania r-rundowej sieci Feistela na wejściu (L_0, R_0) gdy każda z funkcji rundowych jest tożsamościowa równa 0^n?

Zadanie 2 Jaki jest wynik działania r-rundowej sieci Feistela na wejściu (L_0, R_0) gdy każda z funkcji rundowych jest identycznością?

Zadanie 3 (powtórka z wykładu) Pokaż jak wydobyć klucz z dwu-rundowej sieci permutacyjno-zamieniającej mając dostęp do m par tekst jawny-kryptogram. Przyjmij, że długość bloku wynosi 64 bity, każdy z 16 S-boxów ma 4-bitowe wejście i wyjście, a ze 128-bitowego klucza pierwsze 64 bity są wykorzystane w pierwszej, a kolejne 64 w drugiej rundzie.

Zadanie 4 Zmodyfikuj parametry podane w Zadaniu 3.

- Jak zmieni się złożoność ataku dla 8 S-boxów 8-bitowych?
- Jaka będzie złożoność ataku dla bloku długości 128 i 16 S-boxów 8-bitowych?

Zadanie 5 Wyjaśnij pojęcie efektu lawinowego oraz:

- Pokaż, że losowy wybór S-boxów nie gwarantuje efektu lawinowego (możesz ograniczyć się do demonstracji na 4-bitowych S-boxach).
- Efekt lawinowy opisano jako: *zmiana pojedyńczego bitu klucza powoduje zmianę każdego bitu kryptogramu.* Jest to prawda czy fałsz? Dlaczego?
- Efekt lawinowy nie zachodzi dla *one-time pad.* Dlaczego więc stosuje się tą metodę?

Zadanie 6 Rozważ S-box $S5$ dla DES (`http://www.itl.nist.gov/fipspubs/fip46-2.htm`), dla każdego $x \in \{0,1\}^6$ i $y \in \{0,1\}^4$ oraz losowego $z \in \{0,1\}^6$ oblicz prawdopodobieństwo:

$$S_5(z) \oplus S_5(z \oplus x) = y.$$

Zadanie 7 Udowodnij, że

$$DES_{\overline{K}}(\overline{X}) = \overline{DES_K(X)},$$

gdzie $\overline{x}$ oznacza dopełnienie bitowe.

Zadanie 8 Pokaż, że blokowy schemat szyfrowania F' uzyskany z F poprzez wydłużenie długości klucza:

$$F'_{k_1,k_2}(x) := F_{k_2}(F_{k_1})(x),$$

gdzie k_1, k_2 są niezależne, nie jest bezpieczny (w szczególności istnieje szybszy atak niż brute-force). Wskazówka: rozpatrz tzw. meet in the middle attack.