Kryptografia

Lista 3 - 25 III 2013

Problem 1 Niech $\Pi_1 = \langle Gen_1, Enc_1, Dec_1 \rangle$, $\Pi_2 = \langle Gen_2, Enc_2, Dec_2 \rangle$ będą dwoma schematami szyfrowania. Pokaż jak skonstułować schemat szyfrowania Π (wykorzystując Π_1 i Π_2), który również będzie *CPA-secure* przy założeniu, że co najmniej jeden ze schematów Π_1 bądź Π_2 jest *CPA-secure* (nie wiesz, który ze schematów jest bezpieczny).

Problem 2 Pokaż, że szyfr blokowy F' nie jest bezpieczny.

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

gdzie F jest bezpiczenym szyfrem blokowym, a k_1, k_2 są niezależne.

Wystarczy, że pokażesz istnienie ataku na F', który jest szybszy niż atak brute-force. Jaka jest złożoność pamięciowa i czasowa ataku?

Problem 3 Pokaż, że szyfr blokowy F' nie jest bezpieczny.

$$F'_{k_1,k_2,k_3}(x) := k_1 \oplus F_{k_2}(x \oplus k_3),$$

gdzie F jest bezpiczenym szyfrem blokowym, a k_1, k_2, k_3 są niezależne.

Wystarczy, że pokażesz istnienie ataku na F', który jest szybszy niż atak brute-force. Jaka jest złożoność pamięciowa i czasowa ataku?

Problem 4 Rozważ wariant trybu szyfrowania CBC, w którym wysyłający przy każdym szyfrowaniu zwiększa IV o 1 (zamiast wybierać IV za każdym razem losowo). Pokaż, że takie postępowanie prowadzi do schematu, który nie jest odporny na atak *chosen plaintext*. (Twoim zadaniem jest skonstrułowanie adwersarza, który osiąga niepomijalną przewagę w eksperymencie $\mathsf{Priv}^{CPA}_{\mathcal{A},F-CBC}$ dla dowolnego F[1].)

Problem 5 Rozważ liniowość piątego S-boxa S_5 dla DES (`http://www.itl.nist.gov/fipspubs/fip46-2.htm`). W tym celu oblicz prawdopodobieństwo

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

dla każdego $x \in \{0,1\}^6$ i $y \in \{0,1\}^4$ oraz losowego $z \in \{0,1\}^6$.

[1] Tego rodzaju błąd występował w SSL/TLS 1.0. Porównaj z listą zadań nr 3 na pracownie.