Kryptografia

Lista 1 - na 11 III 2013

Definition 1. Schemat szyfrowania $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ nad przestrzenią wiadomości $\mathcal{M}$ jest **doskonale tajny** gdy dla dowolnego rozkładu prawdopodobieństwa nad $\mathcal{M}$, dla każdego $m \in \mathcal{M}$, dla każdego kryptogramu $c \in \mathcal{C}$ dla którego $P[C = c] > 0$ zachodzi:

$$P[M = m|C = c] = P[M = m].$$

Definition 2. Schemat szyfrowania $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ nad przestrzenią wiadomości $\mathcal{M}$ jest **doskonale tajny** gdy dla dowolnego rozkładu prawdopodobieństwa nad $\mathcal{M}$, dla każdego $m \in \mathcal{M}$, dla każdego kryptogramu $c \in \mathcal{C}$ zachodzi:

$$P[C = c|M = m] = P[C = c].$$

Definition 3. Schemat szyfrowania $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ nad przestrzenią wiadomości $\mathcal{M}$ jest **doskonale tajny** gdy dla dowolnego rozkładu prawdopodobieństwa nad $\mathcal{M}$, dla każdej pary wiadomości $m_0, m_1 \in \mathcal{M}$, i dowolnego kryptogramu $c \in \mathcal{C}$ zachodzi:

$$P[C = c|M = m_0] = P[C = c|M = m_1].$$

Problem 1 Udowodnij (bądź znajdź kontrprzykład), że definicje 1 i 2 są sobie równoważne.

Problem 2 Udowodnij (bądź znajdź kontrprzykład), że definicje 2 i 3 są sobie równoważne.

Problem 3 Udowodnij (bądź znajdź kontrprzykład), że definicje 1 i 3 są sobie równoważne.

Problem 4 Udowodnij bądź obal: Dla każdego schematu szyfrowania, który jest doskonale tajny, zachodzi: dla dowolnego rozkładu prawdopodobieństwa na przestrzeni wiadomości $\mathcal{M}$, dla dowolnych $m, m' \in \mathcal{M}$ i dla dowolnego $c \in \mathcal{C}$:

$$P[M = m|C = c] = P[M = m'|C = c].$$

Problem 5

1. Udowodnij, że *shift cipher* jest doskonale tajny wtedy i tylko wtedy, gdy szyfrowany jest pojedyńczy znak.
2. Udowodnij, że One Time Pad jest doskonale tajny.

Definition 4. Powiemy, że funkcja f jest **pomijalna** (negligible) jeżeli dla każdego wielomioanu $p(\cdot)$ istnieje takie N, że dla wszystkich $n > N$ zachodzi: $f(n) < \frac{1}{p(n)}$.

Definition 5. Mówimy, że generator $G_\lambda : K_\lambda \to \{0,1\}^n(\lambda)$ jest **przewidywalny** na pozycji i gdy istnieje algorytm A o wielomianowym czasie działania (względem λ) taki, że:

$$Pr_{k \leftarrow K_\lambda}\left[A\left(G_\lambda(k)|_{1,\ldots,i}\right) = G_\lambda(k)|_{i+1}\right] > \frac{1}{2} + \epsilon(\lambda)$$

dla pewnej niepomijalnej funckji $\epsilon(\lambda)$.

Definition 6. Mówimy, że $G : K \to \{0,1\}^n$ jest **bezpiecznym generatorem pseudolosowym** (secure PRG) jeżeli dla każdego efektywnego testu statystycznego A:

$$Adv_{PRG[A,G]} := \left|P_{k \leftarrow K}\left[A\left(G(k)\right) = 1\right] - P_{r \leftarrow \{0,1\}^n}\left[A(r) = 1\right]\right| < \epsilon(n),$$

dla pewnej pomijalnej funckji $\epsilon(n)$.

Problem 6 Udowodnij, że bezpieczny generator bitów losowych jest nieprzewidywalny.

Problem 7 Udowodnij, że nieprzewidywalny generator bitów losowych jest bezpiecznym