Kodowanie i bezpieczeństwo informacji

Lista nr 2 na 26 II - 9 III 2012

Zadanie 1 Dany jest następujący schemat szyfrowania: $\mathcal{M} = \{a, b\}$. Algorytm generowania klucza wybiera jeden z trzech kluczy $\mathcal{K} = \{k_1, k_2, k_3\}$ z prawdopodobieństwem: $P[k_1] = 1/2, P[k_2] = 1/3, P[k_3] = 1/6$. Szyfrowanie zdefiniowane jest za pomocą równań: $e_{k_1}(a) = 1, e_{k_1}(b) = 2, e_{k_2}(a) = 2, e_{k_2}(b) = 3, e_{k_3}(a) = 3, e_{k_3}(b) = 4$, a rozkład prawdopodobieństwa występowania wiadomości jest następujący $Pr[a] = 3/5, Pr[b] = 2/5$. Oblicz:

- prawdopodobieństwo występowania poszczególnych kryptogramów $P[c]$ dla $c \in \mathcal{C}$.
- prawdopodobieństwa warunkowe $P[m|c]$ dla $m \in \mathcal{M}, c \in \mathcal{C}$.
- czy tak zdefiniowany schemat szyfrowania jest doskonale tajnym?

Zadanie 2 Dla danych z Zadania 1 oblicz:

- entropię $H(\mathcal{M}), H(\mathcal{C}), H(\mathcal{K})$.
- entropię warunkową $H(\mathcal{M}|\mathcal{C})$.

Co możesz powiedzieć o entropii szyfrów doskonałych.

Zadanie 3 Udowodnij bądź wykaż fałszywość: Jeżeli klucz w schemacie Cezara (Shift) jest wybierany z prawdopodobieństwem jednostajnym to schemat szyfrowania spełnia definicję szyfru doskonale tajnego.

Zadanie 4 Udowodnij, że schemat szyfrowania (Gen, Enc, Dec) nad $\mathcal{M}$ jest doskonale tajny wtedy i tylko wtedy gdy dla dowolnego rozkładu prawdopodobieństwa wiadomości nad $\mathcal{M}$, dla dowolnej wiadomości $m \in \mathcal{M}$ i dowolnego kryptogramu $c \in \mathcal{C}$ zachodzi:

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

Zadanie 5 Pokaż jak używać szyfru Vigenere'a do szyfrowania wiadomości o długości t tak, że doskonała tajność jest osiągnięta.