Lista zadań. Nr 9. 9 maja 2005

Kryptografia

IIUWr.

1. Niech $h : X$ Y
   będzie funkcją skrótu. Dla każdego $y \in Y$ niech
   $$h^{-1}(y) = \{x : x(x) = y\}$$
   i niech
   $$s_y = |h^{-1}(y)|.$$
   Zdefiniujmy
   $$N = |\{\{x_1, x_2\} : h(x_1) = h(x_2)\}|.$$
   (a) Wykaż, że
   $$\sum_{y \in Y} s_y = |X|,$$
   zatem średnią wszystkich s_y jst $\bar{s} = |X|/|Y|$.

   (b) Wykaż, że
   $$N = \sum_{y \in Y} \binom{s_y}{2} = \frac{1}{2} \sum_{y \in Y} s_y^2 - \frac{|X|}{2}$$
   (c) Wykaż, że
   $$\sum_{y \in Y} (s_y - \bar{s})^2 = 2N + |X| - \frac{|X|^2}{Y}.$$
   (d) Korzystając z wyniku udowodnionego w (c), wykaż, że
   $$N \geq \frac{1}{2} \left(\frac{|X|^2}{|Y|} - |X| \right),$$
   a równość zachodzi wtedy i tylko wtedy, gdy
   $$s_y = \frac{|X|}{|Y|},$$
   dla każdego $y \in Y$.

2. Niech ϵ oznacza prawdopodobienstwo tego, że $h(x_1) = h(x_2)$, gdzie x_1 i x_2 są losowymi (niekoniecznie różnymi) elementami X. Udowodnij, że
   $$\epsilon \geq \frac{1}{|Y|},$$
   przy czym równość zachodzi wtedy i tylko wtedy, gdy
   $$|h^{-1}(y)| = \frac{|X|}{|Y|},$$
   dla każdego $y \in Y$.

3. Rozważmy funkcję Chauma-van Heijsta-Pfitzmann z wartościami $p = 15083$, $\alpha = 154$ i $\beta = 2307$. Mając konflikt

$$\alpha^{7431}\beta^{5564} \equiv \alpha^{1459}\beta^{954} \bmod p,$$

oblicz $\log_\alpha \beta$.

4. Niech p_1 i q_1 będą dwiema różnymi (dużymi) liczbami pierwszymi, $p = 2p_1 + 1$, $q = 2q_1 + 1$ oraz $n = pq$. Niech ponadto α będzie elementem rzędu $2p_1q_1$ w Z_n^*. Określmy funkcję skrótu h : $\{1, \ldots, n^2\}$ Z_n^*
za pomocą wzoru

$$h(x) = \alpha^x \bmod n.$$

Przyjmijmy, że do zdefiniwania takiej funkcji h wybrano wartości $n = 603241$ oraz $\alpha = 11$ i załóżmy, że mamy trzy konflikty funkcji h: $h(1294755) = h(80115359) = h(52738737)$. Wykorzystaj te informacje do rozłożenia na czynniki pierwsze liczby n.

5. Niech $h_1 : (Z_2)^{2m} \to (Z_2)^m$ będzie silnie bezkonfliktową funkcją skrótu.

   (a) Wykaż, że poniżej określona funkcja $h_2 : (Z_2)^{4m} \to (Z_2)^m$ jest silnie bezkonfliktowa

(1)	zapisz $x \in (Z_2)^{4m}$ jako $x = x_1 \parallel x_2$, gdzie $x_1, x_2 \in (Z_2)^{2m}$
(2)	jako $h_2(x)$ przyjmij $h_1(h_1(x_1) \parallel h_1(x_2))$,

   gdzie $\parallel$ oznacza konkatenację.

   (b) Wykaż, że zdefiniowane poniżej funkcje $h_i : (Z_2)^{2^i m} \to (Z_2)^m$ są silnie bezkonfliktowe.

(1)	zapisz $x \in (Z_2)^{2^i m}$ jako $x = x_1 \parallel x_2$, gdzie $x_1, x_2 \in (Z_2)^{2^{i-1} m}$
(2)	jako $h_i(x)$ przyjmij $h_1(h_{i-1}(x_1) \parallel h_{i-1}(x_2))$,