23 maja 2024

Zadania z kryptografii, lista nr 8

1. Załóżmy, że dany jest generator LFSR z k-bitowym rejestrem i nie wiemy z których jego pozycji jest obliczana różnica symetryczna w trakcie działania. Ile należy wygenerować za jego pomocą bitów, żeby móc przewidzieć każdy następny.

2. *Generator pseudolosowy RSA* działa analogicznie do generatora BBS, tylko w każdej rundzie zamiast działania $x_{i+1} \leftarrow x_i^2 \bmod n$ wykonuje $x_{i+1} \leftarrow x_i^e \bmod n$. Pokaż, że nieodróżnialność generatora RSA od losowego można sprowadzić do niemożliwości ustalenia z niezaniedbywalnym prawdopodobieństwem ostatniego bitu wiadomości m, gdy znane jest $c = m^e \bmod n$.

3. Mamy n osób. Każda data urodzenia jest równie prawdopodobna (załóżmy, że nikt nie urodził się 29 lutego). Ile musi wynosić n, żeby prawdopodobieństwo istnienia dwóch osób z tą samą datą urodzenia przekraczało $1/2$

4. Niech funkcja $f : X \to Y$ nie będzie jednokierunkowa i $|X| \geq 1.1|Y|$. Pokaż, że funkcja ta nie jest silnie bezkonfliktowa.

5. Dobra funkcja haszująca to taka, której wynik działania na x zachowuje się jak liczba losowa. Dana jest funkcja haszująca h z $\{0,1\}^n$ w $\{0,1\}^k$. Dla pewnego $x_0 \in \{0,1\}^k$ wyliczamy ciąg $x_1, x_2, x_3, \ldots, x_s$ według wzoru $x_i = h(x_{i-1}, 0^{n-k})$. Jak duże powinno być s, żeby prawdopodobieństwo powtórzenia się w tym ciągu jakiejś wartości było większe niż $1/2$?

6. Konstrukcja rozszerzająca funkcje silnie bezkonfliktowe $h : \{0,1\}^n \to \{0,1\}^k$ na argumenty dowolnej długości jest określona dla $k + 2 \leq n$. Pokaż jak skonstruować taką funkcję h dla $n = k + 2$ jeśli dysponujemy funkcją silnie bezkonfliktową $f : \{0,1\}^{k+1} \to \{0,1\}^k$.

7. Niech $h_1 : \{0,1\}^{2m} \to \{0,1\}^m$ będzie silnie bezkonfliktową funkcją haszującą. Niech $h_2 : \{0,1\}^{4m} \to \{0,1\}^m$ będzie określona wzorem

$$h_2(x_1, x_2) = h_1\left(h_1(x_1), h_1(x_2)\right).$$

   Pokaż, że h_2 jest również silnie bezkonfliktową funkcją haszującą. Pokaż, że dla wszystkich i funkcja $h_i : \{0,1\}^{2^i m} \to \{0,1\}^m$ zadana wzorem

$$h_i(x_1, x_2) = h_1\left(h_{i-1}(x_1), h_{i-1}(x_2)\right)$$

   jest silnie bezkonfliktową funkcją haszującą.

8. Załóżmy, że mamy bardzo duży plik X, którego wartość $h_k(X)$ obliczona wzorem z poprzedniego zadania jest ogólnie znana. W jaki sposób przesyłając fragment pliku X od bitu i do bitu j przekonać adresata, że jest to istotnie deklarowany przez nas fragment pliku X? Można przesłać dodatkowo informację długości $O(k)$ bloków długości m.

9. Pokaż, że funkcja $f : \{0, ..., q-1\}^3 \to \mathbb{Z}_p$ dla $p = 2q + 1$ określona wzorem:

$$f(x_1, x_2, x_3) = g_1^{x_1} g_2^{x_2} g_3^{x_3},$$

   dla niezależnie wybranych g_1, g_2, g_3 rzędu $2q$ jest silnie bezkonfliktowa przy założeniu trudności znajdowania logarytmu dyskretnego.