**Kryptografia, maj 2002. Zadania zaliczeniowe – pierwsza seria.**

1. **Dyskretny logarytm.** Dla liczby pierwszej $p$, generatora $g$ grupy $Z_p^*$, oraz $1 \leq y < p$, niech $\mathrm{Log}_{p,g}(y)$ oznacza jedyne $x \in Z_{p-1}$ takie, że $g^x = y$.

   Należy dowieść następującej hipotezy. Przypuśćmy, że istnieje *niejednorodny* algorytm $A$ wraz z wielomianem $t(n)$, ktory, dla nieskończenie wielu par $(p, g)$, znajduje wartość logarytmu dyskretnego $\mathrm{Log}_{p,g}(y)$ w czasie wielomianowym (od $|p|$, tj. długości zapisu binarnego $p$) dla co najmniej $\frac{p}{t(|p|)}$ wartości $y$ (innymi słowy, $A$ oblicza $\mathrm{Log}_{p,g}$ z prawdopodobieństwem $\geq \frac{1}{t(|p|)}$).

   Dowieść, że wówczas istniałby także niejednorodny algorytm, ktory dla nieskończenie wielu par $(p, g)$ znajdowałby w czasie wielomianowym wartość $\mathrm{Log}_{p,g}(y)$ dla wszystkich $1 \leq y < p$.

   *Wskazówka.* Wprowadzić algorytm probabilistyczny, a następnie go zderandomizować.

2. **Obraz funkcji jednokierunkowej nie jest rzadki.** Dowieść, że funkcje jednokierunkowe nie mogą mieć obrazu wielomianowej wielkości. Dokładniej, jeśli $f$ jest funkcją jednokierunkową (powiedzmy o dziedzinie $\{0, 1\}^*$) a $p(n)$ dowolnym wielomianem, to dla dostatecznie dużych $n$, $|\{f(x) : |x| = n\}| > p(n)$.

3. **Funkcja jednokierunkowa może zachowywać długość.** Wykazać, że jeśli w ogóle istnieje jakaś funkcja jednokierunkowa, to istnieje również funkcja jednokierunkowa zachowująca dlugość, tzn. $|f(x)| = |x|$, dla każdego $x$.

4. **Generator pseudolosowy z funkcji jednokierunkowej.** Przypuśćmy, że $f : \{0, 1\}^* \to \{0, 1\}^*$ jest jednokierunkowa, a ponadto różnowartościowa i zachowuje długość. Załóżmy ponadto, że $b(x)$ jest trudnym rdzeniem (ang. *hard core bit*) funkcji $f$ i niech $\ell(n)$ będzie dowolnym wielomianem. Dowieść, że wówczas funkcja

   $$G(x) \quad = \quad b(f(x))\, b(f^2(x))\, b(f^3(x)) \ldots b(f^{\ell(|x|)}(x))$$

   jest generatorem pseudolosowym o współczynniku $\ell(n)$.

5. **Wariacje generatora.** Zakładamy, że $G$ jest generatorem pseudolosowym, a $h$ jest wielomianowo obliczalną permutacją (na słowach tej samej dlugości). Dowieść, ze funkcje $G'(x) = h(G(x))$ i $G''(x) = G(h(x))$ są również generatorami pseudolosowymi.

6. **Zdradliwy xor.** Zakładając, że funkcje jednokierunkowe istnieją, obalić następującą hipotezę:

   Dla każdej jednokierunkowej funkcji $f$ zachowującej długość, funkcja $f'(x) =_{def} f(x) \oplus x$ jest również jednokierunkowa.

   (Przyjmujemy, że $f : \{0, 1\}^* \to \{0, 1\}^*$, a $\oplus$ oznacza *xor* po współrzędnych; np. $011 \oplus 110 = 101$.)