Kryptografia dla informatyków I, 2017/18 8.2.2018

Egzamin - zadania

Stefan Dziembowski MIM UW

Zadanie 1:

Podaj ile rozwiązań ma równanie

$$x^8 = 25 \pmod{43 \cdot 47}.$$

Odpowiedź uzasadnij.

Zadanie 2:

Niech $f : \{0,1\}^* \to \{0,1\}^*$ będzie funkcją jednokierunkową, a $G : \{0,1\}^* \to \{0,1\}^*$ generatorem pseudolosowym. Zdefiniujmy $h : \{0,1\}^* \to \{0,1\}^*$ jako $h(x) := f(G(x))$.

1. Czy zawsze h jest funkcją jednokierunkową?
2. Czy zawsze h jest generatorem pseudolosowym?

W przypadku odpowiedzi "tak" podaj dowód tego faktu, w przypadku odpowiedzi "nie" załóż, ze fukcje jednokierunkowe istnieją i skonstruuj przykład odpowiednich f i G.