Kryptografia dla informatyków I, 2016/17 7.2.2017

Egzamin - zadania

Stefan Dziembowski MIM UW

Zadanie 1:

Rozwiąż równanie

$$x^{322} = 9 \pmod{187}$$

dla $x \in Z^*_{187}$.

Zadanie 2:

Niech $f : \{0,1\}^* \to \{0,1\}^*$ będzie funkcją jednokierunkową. Niech $\{H_s\}_{s\in\{0,1\}^*}$ będzie rodziną funkcji haszujących odpornych na kolizje. Zdefiniujmy rodzinę funkcji $\{G_s\}_{s\in\{0,1\}^*}$ w następujący sposób: dla każdych $x, s \in \{0,1\}^*$ niech

$$G_s(x) := f(H_s(x)).$$

Czy $\{G_s\}_{s\in\{0,1\}^*}$ musi również być rodziną funkcji haszujących odpornych na kolizje? W przypadku odpowiedzi "tak" podaj dowód tego faktu, w przypadku odpowiedzi "nie" załóż, ze rodziny funkcji haszujących odpornych na kolizje istnieją i skonstruuj przykład takich f i $\{H_s\}_{s\in\{0,1\}^*}$, że $\{G_s\}_{s\in\{0,1\}^*}$ nie jest taką rodziną.