Cryptography

Dr. Patrick Mehlitz, M.Sc. Ameen Naif

Exercise Sheet 12
Version 16.07.2020

Exercise 1.

Let $\mathcal{P} = \{a, b\}$, $\mathcal{C} = \{1, 2, 3, 4\}$ and $\mathcal{K} = \{K_1, K_2, K_3\}$ denote random variables with $\text{pr}_a^{\mathcal{P}} = 1/4$, $\text{pr}_b^{\mathcal{P}} = 3/4$ and $\text{pr}_{K_1}^{\mathcal{K}} = 1/2$, $\text{pr}_{K_2}^{\mathcal{K}} = \text{pr}_{K_3}^{\mathcal{K}} = 1/4$. Suppose that the encryption functions of the underlying cryptosystem are given by $E_{K_1}(a) = 1$, $E_{K_1}(b) = 2$; $E_{K_2}(a) = 2$, $E_{K_2}(b) = 3$ and $E_{K_3}(a) = 3$, $E_{K_3}(b) = 4$.

(a) Compute the probability distribution on $\mathcal{C}$.

(b) Compute the conditional probability distributions on the plaintext $\mathcal{P}$, given that a certain ciphertext has been observed.

(c) Is the cryptosytem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ perfectly secure? Why?

Exercise 2.

For $n \in \mathbb{N}$, let $g\colon \mathbb{Z}_2^+ \to \mathbb{Z}_2^n$ be a strongly collision resistant hash function. We define $g_1, g_2\colon \mathbb{Z}_2^+ \to \mathbb{Z}_2^{n+1}$ as well as $h\colon \mathbb{Z}_2^+ \to \mathbb{Z}_2^{2n+2}$ via

$$\forall x \in \mathbb{Z}_2^+\colon \quad g_1(x) := \begin{cases} g(x)1 & x_1 = 0, \\ 0^{n+1} & x_1 = 1, \end{cases} \qquad g_2(x) := \begin{cases} g(x)1 & x_1 = 1, \\ 0^{n+1} & x_1 = 0, \end{cases}$$
$$h(x) := g_1(x)g_2(x).$$

Show that h is a strongly collision resistant hash function. Is g_1 weakly collision resistant?