Homework 4 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

12.11.2007

Exercise 10. Let $\mathcal{M} = \{a, b\}$ be the message space, $\mathcal{K} = \{K_1, K_2, K_3\}$ be the key space and $\mathcal{C} = \{1, 2, 3, 4\}$ be the ciphertext space. Let $\hat{M}, \hat{K}$ be stochastically independent random variables with support $\mathcal{M}$ and $\mathcal{K}$, respectively, and with probability distribution:

$$P(\hat{M} = a) = \frac{1}{4}, P(\hat{M} = b) = \frac{3}{4}, P(\hat{K} = K_1) = \frac{1}{2}, P(\hat{K} = K_2) = \frac{1}{4}, P(\hat{K} = K_3) = \frac{1}{4}.$$

The following table explains the encryption rules:

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

, e.g. $e(a, K_1) = 1$.

Compute the entropies $H(\hat{M}), H(\hat{K}), H(\hat{C})$ and $H(\hat{K} \mid \hat{C})$.

Exercise 11. Let X, Y be discrete random variables on a set Ω. Show that for any function $f : X(\Omega) \times Y(\Omega) \to \mathbb{R}$

$$H(X, Y, f(X, Y)) = H(X, Y).$$

Exercise 12. The ring $\mathbb{Z}_2$ is a field that is also named $\mathbb{F}_2$. The ring $\mathbb{Z}_4$ is not a field, but there exists a field $\mathbb{F}_4$ with 4 elements. This field can be constructed as the residue class ring of the polynomial ring $\mathbb{F}_2[x]$ modulo the ideal generated by $f := x^2 + x + 1$. Specify all elements of the field $\mathbb{F}_4$ and determine the addition und multiplication tables for $\mathbb{F}_4$.