Homework 4 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier

06.11.2012

Exercise 10. Let $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ be a cryptosystem. Suppose that $P(\hat{M} = M) > 0$ for all $M \in \mathcal{M}$, $P(\hat{K} = K) > 0$ for all $K \in \mathcal{K}$, and $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$ holds. Show that if $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy, then

$$P(\hat{K} = K) = \frac{1}{|\mathcal{K}|} \text{ for all } K \in \mathcal{K}$$

and for all $M \in \mathcal{M}, C \in \mathcal{C}$ there is a unique $K \in \mathcal{K}$ such that $e(M, K) = C$.

Exercise 11. Let $\mathcal{M} = \{a, b\}$ be the message space, $\mathcal{K} = \{K_1, K_2, K_3\}$ the key space, and $\mathcal{C} = \{1, 2, 3, 4\}$ the ciphertext space. Let $\hat{M}, \hat{K}$ be stochastically independent random variables with support $\mathcal{M}$ and $\mathcal{K}$, respectively, and with probability distributions: $P(\hat{M} = a) = \frac{1}{4}, P(\hat{M} = b) = \frac{3}{4}, P(\hat{K} = K_1) = \frac{1}{2}, P(\hat{K} = K_2) = \frac{1}{4}, P(\hat{K} = K_3) = \frac{1}{4}$.

The following table explains the encryption rules:

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

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

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

(b) Why does this cryptosystem not have perfect secrecy?

(c) What could be changed to achieve perfect secrecy?