Homework 5 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

25.11.2008

Exercise 13. 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 $|\mathcal{M}| = |\mathcal{K}| = |\mathcal{C}|$. Show that if $(\mathcal{M}, \mathcal{K}, \mathcal{C}, e, d)$ has perfect secrecy, then

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

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 14. Does the cryptosystem from Exercise 12 have perfect secrecy? If not, propose a modified system which has perfect secrecy.

Exercise 15. Consider affine ciphers on $\mathbb{Z}_{26}$, i.e. $\mathcal{M} = \mathbb{Z}_{26}$, $\mathcal{C} = \mathbb{Z}_{26}$ and $\mathcal{K} = \mathbb{Z}_{26}^* \times \mathbb{Z}_{26} = \{(a, b) \mid a, b \in \mathbb{Z}_{26},\ \gcd(a, 26) = 1\}$. Select the keys $\hat{K}$ uniformly distributed at random and independent of the messages $\hat{M}$.

Show that this system has perfect secrecy.