Homework 5 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

19.11.2007

Exercise 13.

(a) Does the cryptosystem from Exercise 4 have perfect secrecy?

(b) Consider the following modification of this cryptosystem: The matrices A and B are now of the form

$$A = \begin{pmatrix} 1 & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \; B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}.$$

How many possible keys does this system have? Does this system have perfect secrecy, assuming that the message space is $\mathcal{M} = \{0,1\}^4$ and that each key is chosen with the same probability?

Exercise 14. Does the cryptosystem from Exercise 10 have perfect secrecy? If not, propose a modification of the 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 $\hat{K}$ evenly distributed at random and independent of the message distribution $\hat{M}$.

Show that this system has perfect secrecy.