Homework 5 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy
24.11.2009

Exercise 13. Consider the following cryptosystem: one-letter messages are encrypted using an affine cipher. The key is chosen randomly and independent from the plaintext from a uniform distribution.

a) Show that this cryptosystem provides perfect secrecy for every distribution of $\hat{M}$.

b) Determine $H(\hat{K} \mid \hat{C})$ and $H(\hat{K} \mid \hat{M}, \hat{C})$.

Exercise 14.

Is a Hill cipher with keys in $\mathbb{Z}_m^{k\times k}$ perfectly secret when only blocks of length k are encrypted and all keys occur with the same probability?

Exercise 15. Let X, Y be random variables with support $\mathcal{X} = \{x_1, \dots, x_m\}$ and $\mathcal{Y} = \{y_1, \dots, y_m\}$, respectively, and distribution $P(X = x_i) = p_i$ and $P(Y = y_j) = q_j$, respectively. Let (X, Y) be the corresponding two-dimensional random variable with distribution $P(X = x_i, Y = y_j) = p_{ij}$. Prove the following statements from theorem 4.3:

(a) $0 \le H(X)$ with equality if and only if $P(X = x_i) = 1$ for some i.

(b) $H(X) \le \log m$ with equality if and only if $P(X = x_i) = \frac{1}{m}$ for all i.

(c) $H(X \mid Y) \le H(X)$ with equality if and only if X and Y are stochastically independent.

(d) $H(X, Y) \le H(X) + H(Y)$ with equality if and only if X and Y are stochastically independent.

Hint: $\ln z \le z - 1$ for all $z > 0$ with equality if and only if $z = 1$.