# Homework 3 in Advanced Methods of Cryptography

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

30.10.2012

**Exercise 7.** The handling of long keys for Vernam ciphers is difficult. Therefore autokey systems are proposed. For a given keyword $k = (k_0, \dots, k_{n-1})$ and message $m = (m_0, \dots, m_{l-1})$ the following two autokey systems are given.

$$c_i = \begin{cases} m_i + k_i \pmod{26} & 0 \le i \le n-1 \\ m_i + c_{i-n} \pmod{26} & n \le i \le l-1 \end{cases}$$

$$\hat{c}_i = \begin{cases} m_i + k_i \pmod{26} & 0 \le i \le n-1 \\ m_i + m_{i-n} \pmod{26} & n \le i \le l-1 \end{cases}$$

(a) Describe a ciphertext-only attack on $\mathbf{c} = (c_0, \dots, c_{l-1})$.

(b) Decrypt the cryptogram $\mathbf{c}$=DLGVTYOACOUVCEZA.

(c) Assume the keylength to be known. Describe a ciphertext-only attack on $\hat{\mathbf{c}} = (\hat{c}_0, \dots, \hat{c}_{l-1})$.

(d) Decrypt the cryptogram $\hat{\mathbf{c}}$=QEXYIRVESIUXXKQVFLHKG using keylength 2.

**Exercise 8.**

In Lemma 3.3 of the lecture notes, the expectation value of the index of coincidence was calculated for the ciphertext $(C_1, \dots, C_n)$ with random variables $C_1, \dots C_n$ i.i.d.

(a) Derive the variance of the index of coincidence $\mathrm{Var}(I_C)$ for the model of Lemma 3.3.

**Exercise 9.**

Let $X, Y$ be random variables with support $\mathcal{X} = \{x_1, \ldots, x_m\}$ and $\mathcal{Y} = \{y_1, \ldots, y_d\}$. Assume that $X, Y$ are distributed by $P(X = x_i) = p_i$ and $P(Y = y_j) = q_j$.

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

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

(c) $H(X \mid Y) \leq H(X)$ with equality if and only if $X$ and $Y$ are stochastically independent (conditioning reduces entropy).

(d) $H(X, Y) = H(X) + H(Y \mid X)$ (chainrule of entropies).

(e) $H(X, Y) \leq H(X) + H(Y)$ with equality iff $X$ and $Y$ are stochastically independent.

**Hint** (a): $\ln z \leq z - 1$ for all $z > 0$ with equality if and only if $z = 1$.

**Hint** (b),(c): If $f$ is a convex function, the Jensen inequality $f(E(X)) \leq E(f(X))$ holds.