# Homework 5 in Cryptography I

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

12.05.2011

**Exercise 14.**

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

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

**Exercise 15.** Let $X, Y$ be discrete random variables on a set $\Omega$.

(a) Show that for any function $f : X(\Omega) \times Y(\Omega) \to \mathbb{R}$, the relationship

$$H(X, Y, f(X, Y)) = H(X, Y)$$

holds.

**Exercise 16.**

Let $X, Y$ be random variables with support $\mathcal{X} = \{x_1, \ldots, x_m\}$ and $\mathcal{Y} = \{y_1, \ldots, y_m\}$. 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 if and only if $X$ 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.