Exercise 4 in Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Jose Angel Leon Calvo

2015-05-07

Problem 10. *(weak permutations)* The permutation $\pi = (1)(2, 11, 5, 8)(3, 6, 7, 4)(9, 10)$ defines a permutation cipher with block length $k = 11$.

(a) Determine the number of character sequences of length 11 over the usual alphabet with 26 letters whose ciphertext is equal to the plaintext.

Hint: $(2, 11, 5, 8)$ means that position 2 is moved to position 11, 11 to 5, 5 to 8 and 8 to 2.

Problem 11. *(properties of entropy)*

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.

Problem 12. *(entropy of function)* Let X, Y be discrete random variables on a set Ω. Show that for any function $f : X(\Omega) \times Y(\Omega) \to \mathbb{R}$, it holds:

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