Homework 4 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

18.11.2008

Exercise 10. The handling of long keys for Vernam ciphers is difficult. Therefore autokey systems are proposed: choose a keyword $k = (k_0, \dots, k_{n-1})$ and encode the message $m = (m_0, \dots, m_{l-1})$ as follows.

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

Why should this methode not be used? Describe a ciphertext-only attack where the keylength n is unknown.

A better but still not advisable suggestion is given as follows.

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

Describe a ciphertext-only attack on the second method. You may assume the keylength n to be known.

Exercise 11. Let X, Y be discrete random variables on a set Ω. Show that for any function $f : X(\Omega) \times Y(\Omega) \to \mathbb{R}$

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

Exercise 12. Let $\mathcal{M} = \{a, b\}$ be the message space, $\mathcal{K} = \{K_1, K_2, K_3\}$ be the key space and $\mathcal{C} = \{1, 2, 3, 4\}$ be the ciphertext space. Let $\hat{M}$, $\hat{K}$ be stochastically independent random variables with support $\mathcal{M}$ and $\mathcal{K}$, respectively, and with probability distribution

$$P(\hat{M} = a) = \frac{1}{4}, P(\hat{M} = b) = \frac{3}{4}, P(\hat{K} = K_1) = \frac{1}{2}, P(\hat{K} = K_2) = \frac{1}{4}, P(\hat{K} = K_3) = \frac{1}{4}.$$

The following table explains the encryption rules:

	K_1	K_2	K_3
a	1	2	3
b	2	3	4

, e.g. $e(a, K_1) = 1$.

Compute the entropies $H(\hat{M}), H(\hat{K}), H(\hat{C})$ and $H(\hat{K} \mid \hat{C})$.