Homework 4 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy
17.11.2009

Exercise 10. The plaintext in exercise 9 is encrypted using a Vigenere cipher. Find the length of the key using the "Kasiski-Babbage"-method and decrypt the message.

```
KPJDLCGS PVHQKWRK KCKRBKPJ DLCWILKR BGSKORKO VCVCNVEW OVQDLCIL YFIRRIGB
IVSXQKRB DLCSVCXX PKRAOWYX HMXIKKRG XLGCXGWI NVEWCQYX CNKVRC
```

Exercise 11.

Suppose a cryptosystem with two keys, $\mathcal{K} = \{k_1, k_2\}$ with each probability $\frac{1}{2}$ to be used, and three plaintexts $\mathcal{M} = \{m_1, m_2, m_3\}$ that occur with probability $p(m_1) = \frac{1}{2}$, $p(m_2) = \frac{1}{4}$, $p(m_3) = \frac{1}{4}$.

a) Create an encryption function for this cipher such that there are three ciphertexts $\mathcal{C} = \{c_1, c_2, c_3\}$ and such that c_1 occurs with probability $\frac{1}{2}$.

b) Compute $H(M)$, $H(K)$, $H(C)$.

c) Compute the key evocation $H(K|C)$.

d) What is the problem of this cryptosystem?

Exercise 12.

Let $p(x)$ be a probability mass function. Prove, for all $d \geq 0$, that

$$Pr\{p(X) \leq d\} \cdot log(\frac{1}{d}) \leq H(X).$$

This inequality is called the Markov's inequality for probabilities.