Homework 6 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Steven Corroy
01.12.2009

Exercise 16.

Suppose we use a Caesar cipher such that each key ($k \in \{0, \dots, 25\}$) is used with equal probability. We use a new key for each successible plaintext letter to encrypt. Note that this cipher is equivalent to Vernam cipher. We have f_M, f_K and f_C the probability mass functions of M, K and C. Show that this cryptosystem has perfect secrecy by following these steps:

a) Show that $\sum_{k \in K} f_M(d(k, c)) = 1$ for every ciphertext $c \in C$.

b) Compute f_C using the formula
$$f_C(c) = \sum_{k \in K} f_K(k) f_M(d(k, c)).$$

c) Compare $f_C(c)$ to $f_{C|M}(c|m)$.

Exercise 17.

Let M be a block of bits of length 64 and K be a block of bits of length 56. Let $\mathrm{DES}(M, K)$ denote the encryption of M with key K using the DES cryptosystem. Show that
$$\mathrm{DES}(M, K) = \overline{\mathrm{DES}(\overline{M}, \overline{K})},$$
where $\bar{\cdot}$ denotes the bitwise complement.

This property is called complementation property. Does this help to attack DES?

Exercise 18. In order to improve the security of DES, we could use two keys K_1 und K_2 and encrypt the plaintext M with $e(e(M, K_1), K_2)$.

a) Why should we choose $K_1 \neq K_2$?

b) Show that the expected amount of pairs of keys which encrypt plaintext blocks $M_1, \dots, M_r$ to ciphertext blocks $C_1, \dots, C_r$ is approximately $2^{112-64r}$ if we assume that

- K_1 and K_2 are independent and identically-distributed and
- K_1 and K_2 are permutations of the 64 bits plaintext blocks.

c) Show that a known-plaintext attack using a maximum of 2^{58} encryption and decryption operations has a higher probability of success when at least two pairs of plaintext and ciphertext are known.