Homework 6 in Cryptography I

Prof. Dr. Rudolf Mathar, Michael Naehrig

26.11.2007

Exercise 16. 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.

Exercise 17. Consider the following cryptosystem. Messages are bit sequences of arbitrary length, i.e. character sequences over the alphabet $\mathbb{F}_2 = \{0, 1\}$. Let the message be $m = m_1 m_2 \dots m_l$. Keys are also bit sequences $k = k_1 k_2 \dots k_n$ of fixed length n. Usually we have $n < l$. Now a key stream $z = z_1 z_2 \dots z_l$ is generated in a recursive manner depending on the key:

$$\begin{aligned} z_i &= k_i, \quad 1 \leq i \leq n, \\ z_i &= \sum_{j=1}^{n} s_j z_{i-j} \pmod 2, \quad n < i \leq l. \end{aligned}$$

Here $s_1, \dots, s_n$ are fixed bits which are given in advance. We encrypt $c_i := m_i \oplus z_i$ for $1 \leq i \leq l$.

(a) How does decryption work for this cryptosystem? Why should $k = 00 \dots 0$ not be chosen as the key?

(b) Encrypt the message $m = 10110001010011010100$ with $n = 4$, $s_2 = s_3 = 0$, $s_1 = s_4 = 1$ using the key $k = 0110$. The key stream is periodic. How long is its period?

This method for generating a key stream is called linear feedback shift register (LFSR).

Exercise 18. Consider the finite field $\mathbb{F}_4$ from Exercise 12. Construct an extension field $\mathbb{F}_{16}$ of $\mathbb{F}_4$ with 16 elements and describe your approach.
Hint: Start with the polynomial ring $\mathbb{F}_4[U]$.