Homework 7 in Cryptography I
Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
26.05.2011
Note: This exercise will be held in lecture room AH III.

Exercise 20.

(a) Which of the functions IP, E, ⊕K_i, S, P in the encryption procedure of the Data Encryption Standard (DES) are linear?

Note: Linearity: \( f(a \oplus b) = f(a) \oplus f(b) \)

Exercise 21.

Let \( M \) be a block of bits of length 64 and let \( K \) be a block of bits of length 56. Let \( \text{DES}(M, K) \) denote the encryption of \( M \) with key \( K \) using the DES cryptosystem. \( \overline{x} \) denotes the bitwise complement of a block \( x \).

(a) Show that the complementation property holds:
\[
\text{DES}(M, K) = \overline{\text{DES}(\overline{M}, \overline{K})}
\]

(b) How does the complementation property help to attack DES?

Exercise 22.

Consider the following Linear Feedback Shift Register (LFSR) based stream cipher. Messages are bit sequences of arbitrary length, i.e., character sequences over the alphabet \( \mathbb{F}_2 = \{0, 1\} \). Let the message be \( m = m_1 m_2 \ldots m_l \). Keys are also bit sequences \( k = k_1 k_2 \ldots k_n \) of fixed length \( n < l \). Now, a key stream \( z = z_1 z_2 \ldots z_l \) is recursively generated depending on the key as following:
\[
\begin{align*}
z_i &= k_i, \quad 1 \leq i \leq n, \\
z_i &= \sum_{j=1}^{n} s_j z_{i-j} \pmod{2}, \quad n < i \leq l.
\end{align*}
\]

The bits \( s_1, \ldots, s_n \) are fixed and 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?

(b) What happens if \( k = 00 \ldots 0 \) is chosen as the key?

(c) Encrypt the message \( m = 10110001010011010100 \) with \( n = 4 \), \( s_2 = s_3 = 0 \), \( s_1 = s_4 = 1 \) using the key \( k = 0110 \).

(d) How long is the period\(^1\) of the key stream in (c)? What is the maximal period \( p_{\text{max}} \) of an LFSR with a key of length \( n \)?

\(^1\)The period of an LFSR is defined as \( p = \min\{k \in \mathbb{N} | \exists i_0 \in \mathbb{N}, i \in \mathbb{N}, \forall i \geq i_0 : z_{i+k} = z_i \} \).