Prof. Dr. Rudolf Mathar, Dr. Arash Behboodi, Markus Rothe

Exercise 6

Friday, June 1, 2018

Problem 1. (*AES encryption errors*) A sequence of message blocks is encrypted with AES in the modes ECB, CBC, OFB, CFB, and CTR. The ciphertext is sent from Alice to Bob over a channel with random transmission errors.

a) Bob wants to decrypt the ciphertext. Assume that exactly one bit in one block of the ciphertext changes during transmission. How many bits are wrongly decrypted in the worst case?

b) What happens, if one bit of the ciphertext is lost or an additional bit is inserted?

Problem 2. (*AES round key*) Consider the following AES-128 key given in hexadecimal notation:

$$K = 2D\ 61\ 72\ 69\ 65\ 00\ 76\ 61\ 6E\ 00\ 43\ 6C\ 65\ 65\ 66\ 66$$

a) What is the round key K_0?

b) What are the first 4 bytes of round key K_1?

Problem 3. (*linear feedback shift register*) 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 $m = m_1 m_2 \dots m_l$. Keys are also bit sequences $k = k_1 k_2 \dots k_n$ of fixed length $n < l$. Now, a key stream $z = z_1 z_2 \dots z_l$ is recursively generated depending on the key as following:

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

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

a) How does decryption work for this cryptosystem?

b) What happens if $k = 00 \dots 0$ 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 $p_{\max}$ of an LFSR with a key of length n?

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