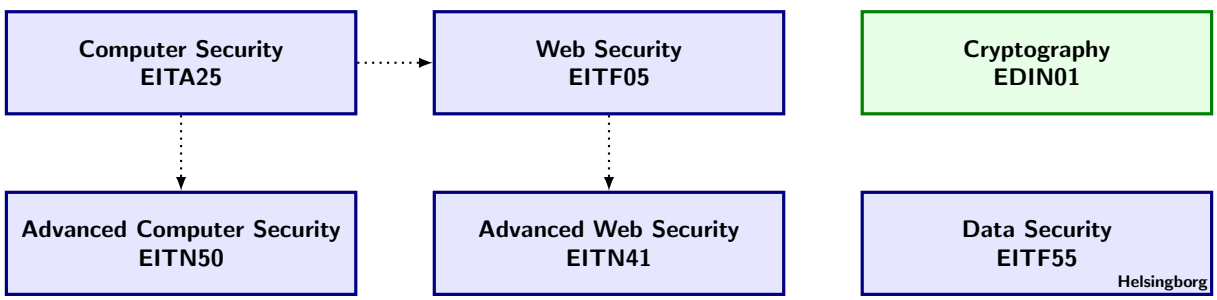
EDIN01 Cryptography 2017

Project 3: Correlation Attack

- This project will be done in groups of 1-2 people.
- Estimated effort: 10 man-hours

Learning goals:

- Learn about stream ciphers.
- Learn about correlation attacks.
- Implementing a correlation attack.
- Improving presentation skills.



1 Introduction

One important family of encryption methods is stream ciphers. The principle behind stream ciphers is to consider the message to encrypt as a stream of message symbols and encrypt each symbol individually.

Let $m = m_1, m_2, \ldots$ be the plaintext to encrypt. The stream cipher takes a secret key K and produces a keystream $z = z_1, z_2, \ldots$. The encryption is then given as $c_i = e(z_i, m_i)$. Often, the message, the ciphertext, and the keystream are sequences of binary digits. A binary synchronous stream cipher where the encryption function is XOR, i.e., $c_i = m_i + z_i \mod 2$, is called *binary additive stream cipher*, see Figure 1.

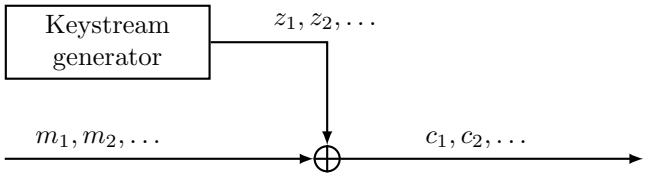


Figure 1: Principle of binary additive stream ciphers.

A common method to build a keystream generator is to combine several linear feedback shift registers to get a keystream with desired statistical properties. Futhermore, the secret key K is the initial states of the LFSRs.

The most important class of attacks on LFSR-based stream ciphers is *correlation attacks*. Basically, if one can in some way detect a correlation between the known output sequence and the output of one individual LFSR, this can be used in a "divide-and-conquer" attack on the individual LFSR.

In this project a correlation attack on a given keystream generator will be implemented.

2 The Keystream Generator

In the keystream generator that we consider there are three LFSRs. Let L_i and $C_i(D)$ denote the length and the feedback polynomial of the ith LFSR. The values of L_i and $C_i(D)$ for the different LFSRs are,

$$\begin{aligned} L_1 &= 13, \quad C_1(D) = 1 + D + D^2 + D^4 + D^6 + D^7 + D^{10} + D^{11} + D^{13}, \\ L_2 &= 15, \quad C_2(D) = 1 + D^2 + D^4 + D^6 + D^7 + D^{10} + D^{11} + D^{13} + D^{15}, \\ L_3 &= 17, \quad C_3(D) = 1 + D^2 + D^4 + D^5 + D^8 + D^{10} + D^{13} + D^{16} + D^{17}. \end{aligned}$$

The keystream symbol is determined from the output of the LFSRs in the following way. If two or three output symbols from the LFSRs are one, the keystream symbol will be one, otherwise it will be zero. The keystream generator is depicted in Figure 2.

The secret key K is the initial state of the three LFSRs. Hence, we can write the key as a 3-tuple, $K = (K_1, K_2, K_3)$, where K_i is the initial state of the ith LFSR.

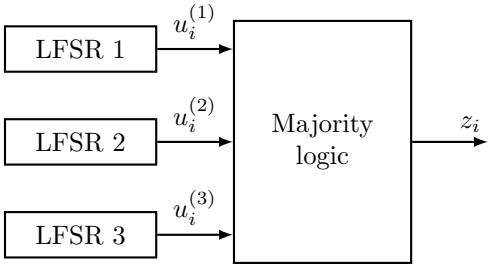


Figure 2: The keystream generator.

3 Project Exercises

Exercise 1:

Each group is given a keystream $z_1, z_2, \ldots, z_N$ of some length N. Find the key K that was used to produce this keystream.

Exercise 2:

Assume that the attack takes T seconds. How long would it take to attack by an exhaustive search over the entire keyspace?

Hint: Correlation Attacks

From a cryptanalysis point of view, a good stream cipher should be resistant against a *known-plaintext attak*. In a known-plaintext attack the cryptanalyst is given a plaintext and the corresponding ciphertext, and the task is to determine a key K. For a synchronous stream cipher, this is equivalent to the problem of finding the key K that produces a given keystream $z_1, z_2, \ldots, z_N$. As an example, consider an additive stream cipher. Given a certain plaintext $m_1, m_2, \ldots, m_N$ and the corresponding ciphertext $c_1, c_2, \ldots, c_N$, the keystream $z_1, z_2, \ldots, z_N$ can be calculated $z_i = c_i + m_i \mod 2$. Hence, we assume that a given keystream $z_1, z_2, \ldots, z_N$ is the cryptanalyst's possession and that cryptanalysis is the problem of restoring the secret key. In LFSR based stream ciphers, the secret key is often given as the initial state of the shift registers. The attack can then be stated as follows. Given a keystream sequence of length N, find the initial state of the LFSRs.

There exist several classes of general cryptanalytic attacks against stream ciphers. One of the most important class of attacks on LFSR-based stream ciphers is *correlation attacks*. If one can find a correlation between the output of one of the shift registers and the keystream, i.e., $\Pr(u_i = z_i) \neq 0.5$, where u_i is the output of the LFSR and z_i is the known keystream symbol, then one can try to find the initial state of this LFSR independently of the other LFSRs, see Figure 3.

Let $u_i^{(j)}$ be the output of the jth LFSR and assume that $\Pr(u_i^{(j)} = z_i) = p$, where $p \neq 0.5$. What is the exact value of p in Figure 2. Guess that the initial state of the jth LFSR is $\hat{\mathbf{u}}_\mathbf{0} = (\hat{u}_1^{(j)}, \hat{u}_2^{(j)}, \ldots, \hat{u}_{L_j}^{(j)})$. Since the feedback polynomial $C_j(D)$ is known, we can calculate an LFSR output sequence $\hat{\mathbf{u}} = (\hat{u}_1, \hat{u}_2, \ldots, \hat{u}_N)$, where

$$\begin{aligned} \hat{u}_i &= \hat{u}_i^{(j)}, \quad 0 < i \leq L_j, \\ \hat{u}_i &= \sum_{l=1}^{L_j} c_l \hat{u}_{i-l}, \quad L_j < i \leq N. \end{aligned}$$

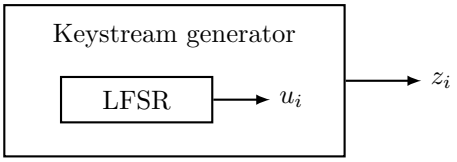


Figure 3: A sufficient requirement for a correlation attack, $\Pr(u_i = z_i) \neq 0.5$.

For two binary vectors $\mathbf{x}$ and $\mathbf{y}$, *the Hamming distance* between $\mathbf{x}$ and $\mathbf{y}$, $d_H(\mathbf{x}, \mathbf{y})$, is defined to be the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ differ.

Estimate the correlation p with p^*, where

$$p^* = 1 - \frac{d_H(\hat{\mathbf{u}}, \mathbf{z})}{N}.$$

If the guessed initial state, $\hat{\mathbf{u}}_\mathbf{0}$, is correct, we get $p^* \approx p$, otherwise $p^* \approx 0.5$.

Thus, we get the following algorithm for a correlation attack.

1. For each possible initial state, calculate p^*;
2. Output the initial state for which p^* deviates from $\frac{1}{2}$ as much as possible.

There is a very nice way of visualizing this – for your own understanding, but also for inclusion in your report. Plotting each state along the x-axis vs. the corresponding p^* value along the y-axis, one such point should be clearly separated from the others. This outlier corresponds to the correct initial state.