Understanding Cryptography

Homework No.2 **Due Date: 99.01.07**

1. We know LFSRs in three categories. These three categories are:

- Primitive polynomials
- Irreducible polynomials
- Reducible polynomials

1.1. State the difference between these three categories of LFSRs.
1.2. Draw the corresponding LFSR for each of the three polynomials.

$$x^4 + x^2 + 1$$
$$x^3 + x + 1$$
$$x^4 + x^3 + x^2 + x + 1$$

1.3. Which of the polynomials is primitive, which is reducible, and which is irreducible?

1.4. Determine the lengths of sequences produced by each of these LFSRs.

Note:

> **Theorem 2.3.1** *The maximum sequence length generated by an LFSR of degree m is* $2^m - 1$.

2. We know that LFSR is used to generate a keystream for a shift cipher. The LFSR has five bits $(s_4 s_3\, s_2\, s_1 s_0)$. the feedback bit is given by the formula $s_3 + s_0 \pmod 2$ and the sequence of s_0 values forms the keystream. The LFSR is initialized with the $(s_4\, s_3 s_2 s_1 s_0) = (11011)$.

2.1. How many keystream bits will be generated before the keystream starts repeating?

2.2. What is the sequence of keystream bits?

3. State the Advantages and problems of One-Time Pad.

4. We want to perform an attack on a LFSR-based stream cipher. In order to process letters, each of the 26 uppercase letters and the numbers 0, 1, 2, 3, 4, 5 are represented by a 5-bit vector according to the following mapping:

$$\begin{aligned} A \leftrightarrow 0 &= 00000_2 \\ &\vdots \\ Z \leftrightarrow 25 &= 11001_2 \\ 0 \leftrightarrow 26 &= 11010_2 \\ &\vdots \\ 5 \leftrightarrow 31 &= 11111_2 \end{aligned}$$

We happen to know the following facts about the system:

- The degree of the LFSR is m=6.
- Every message starts with the header WPI.

We observe now on the channel the following message (the fourth letter is a zero):

- j5a0edj2b

4.1. Write a program in your favorite programming language which generates the whole sequence, and find the whole plaintext.

4.2. What is the initialization vector?

4.3. What are the feedback coefficients of the LFSR?

4.4. Where does the thing after WPI live?

4.5. What type of attack did we perform?

5. Assume the *IV* and the key of Trivium each consist of 80 all-zero bits. Write a program in your favorite programming language to compute the first 70 bits $s_1,...,s_{70}$ during the warm-up phase of Trivium. Note that these are only internal bits which are not used for encryption since the warm-up phase lasts for 1152 clock cycles.

Optional Question

- Alex and Blake are encrypting messages using RC4. Harry the Hacker, are eavesdropping on their communications. Each plaintext message is a sequence of characters; each character is represented as an 8-bit binary number using the ASCII character encoding. Alex and Blake are using the same key to encrypt every message. Because RC4 does not define how to incorporate a nonce into the keystream generator algorithm, Alex and Blake are using this (insecure) scheme: Generate the key stream using the (fixed) key, then add (mod 256) the nonce to each byte of keystream. You

happen to know that when Alex sends the plaintext BARACKOBAMA with a nonce of 1, the cipher text was:

```
01000011 00011011 00010010 00110000 11111000 10100111 10001110
11101001 00010100 00011101 01100100
```

You now observe Blake send the following cipher text with a nonce of 2:

```
01000110 00010100 00001111 00110011 11110000 10101001 10010110
11111110 00000011 00011100 01110110
```

1. What is the plaintext of Blakes message?

2. Explain how you found the plaintext with description.

Deliverables

- Put the answer to each of the questions in your answer sheet. For exercises #4 and #5, make sure to put the related codes you wrote in your answer file, as well. Otherwise, you won't get their scores.