Introduction to Cryptography: Homework 1

September 15, 2021

Requirements about the delivery of this assignment:

- Submit a pdf-document via Brightspace;
- Any additional files (e.g., Python scripts) can be added as well;
- Make sure that you write both name and student number on all documents (not only in the file name).

Deadline: Monday, September 27, 17:00 sharp!

Grading: You can score a total of 100 points for the hand in assignments. To get full points, please **explain all answers clearly**.

Exercises:

1. **Vigenère cipher security strength.** Historical ciphers, like the Vigenère cipher discussed in this exercise, used the regular alphabet of 26 latin characters $(A, B, C, \ldots, Z)$. In the exercise, all interpunction (spaces, comma's, periods, etc.) is removed.

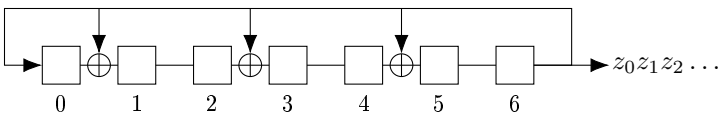
   (a) Suppose that we somehow know that the key used in a Vigenère cipher is seven characters long. Show that we have 32 bits of security, assuming we only consider exhaustive key search.

   (b) One way to determine information about the length of the key (and therefore reducing the security strength of the Vigenère cipher with respect to exhaustive key search) is to look for repeating patterns in the ciphertext. For instance, one may observe that a block of five consecutive letters appears more than once. In that case, it is likely that the same string is enciphered with the same (part of) the key. Given the following ciphertext, what can you conclude about the length of the key, using this property?

   ```
   qhcyrjxurstxzzkoamazzxerylpqajehdrymiwazzxnvkdwablttzye
   qhcyrxhztklmprymgqanalrrgdhcfycrifcwpiyqagnvkdwablyhtq
   ```

   (c) Can you decrypt the above ciphertext and determine the error in the plaintext? [You can use any programming you want, but make sure you use your answer to (b) instead of brute-forcing all possible key-lengths.]

2. **Linear Feedback Shift Register – basics.** In this exercise we consider the following LFSR:



   (a) Assume the LFSR is initialized with state `1001101`.

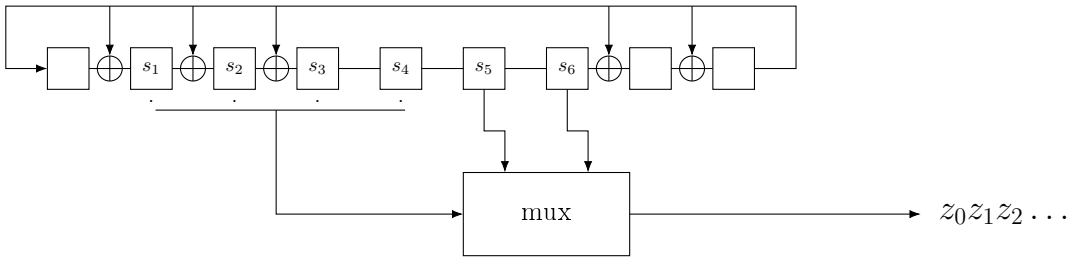
      i. Show that the state of the LFSR equals `1100011` after four iterations.

      ii. Show that the first five bits of the output stream are `10011`.

   (b) Assume that the output stream is $(z_0 z_1 z_2 z_3 z_4 z_5 z_6)$ =`1101110`. Show that the initial state of the LFSR is `0100111`.

   (c) What is the current state of the LFSR after z_6 was outputted?

3. **Filtered Linear Feedback Shift Register – basics.** In this exercise we consider the following filtered LFSR.



The multiplexer outputs $z = s_A$ where A is determined by $A = 1 + s_5 + 2s_6$.

(a) Given an initial state $s^0 =$`100110011`, show that the first five output bits are `01111`. [Outputs occur just before iterating the filtered LFSR.]

(b) Show that the output function for z can be expressed as

$$z_i = s_1(s_5 + 1)(s_6 + 1) + s_2 s_5(s_6 + 1) + s_3(s_5 + 1)s_6 + s_4 s_5 s_6.$$

Hand in assignments:

1. **(30 points) Security goals and cryptography.** Suppose that a client and server have established a unilaterally authenticated shared key (i.e., only the server is authenticated towards the client, but not vice versa), which they use for encryption. They also use a cryptographic signature scheme such that the public keys are all authenticated. Explain, for each of the following security properties, whether client and server achieve

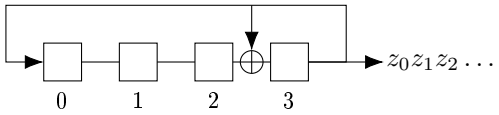
   (a) Confidentiality

   (b) Data integrity

   (c) Origin authentication

   if the client sends an encrypted message to the server with a cryptographic signature on the ciphertext. Assume that the signature verifies correctly to the server.

2. **(70 points) Linear Feedback Shift Register – linear attack.** In Exercise 2, we saw that the initial state is retrievable from n consecutive bits of the output stream. In this exercise, we will extend that attack to show how the initial state is retrievable from any n bits of the output stream. Consider the following 4-bit LFSR.



   Represent the state after t iterations by a vector s^t. Let z_t denote the tth output bit. It is known that with this cipher, the output stream is decimated and the attacker will learn the following output bits: z_3, z_6, z_8, z_{14}. [You are allowed to compute powers of matrices (e.g., M^4) using a computer algebra system.]

   (a) Give the matrix M corresponding to the LFSR, that is the matrix M such that $s^{t+1} = M \cdot s^t$. 4 pt

   (b) Let $s^0 = (s_0, s_1, s_2, s_3)$, so that $z_0 = s_3$. Express z_2 in terms of (s_0, s_1, s_2, s_3). [Remember that z_2 is the output after applying M two times.] 15 pt

   (c) Express z_3 in terms of (s_0, s_1, s_2, s_3) as in (b). 15 pt

   (d) Let $z = (z_3, z_6, z_8, z_{14})^T$. Find a matrix N such that $z = N \cdot s^0$. 20 pt

   (e) As in (d), let $z = (1, 1, 0, 1)^T$. Recover the key (that is the initial state s^0). 16 pt