T-79.503 Foundations of Cryptology
Homework 2
September 30, 2004

1. Define a stream cipher as follows:

$$\begin{aligned} \mathcal{P} &= \mathcal{C} = \mathbb{Z}_7,\ \mathcal{K} = \{(a,b) \mid \gcd(a,7) = 1\} \\ z_i &= (a \times i + b) \bmod 7,\ i = 1, 2, \ldots, \text{ where } (a,b) \text{ is the key.} \\ e_z(x) &= (x + z) \bmod 7 \end{aligned}$$

   a) Using (5,3) as the key, compute the decryption of the message 25542531.

   b) If you know that some part of the plaintext is 110503, and this encrypts to give the ciphertext 501153, then derive as much as you can about the unknown key (a, b). What additional information you need to derive the entire key?

2. Assume that we know an efficient method for breaking any Vigenère cipher. The purpose of this exercise is to show how any such method can be used to break the autokey cipher. Develop a method for transforming the ciphertext produced by an autokey cipher to a ciphertext produced by a Vigenère cipher.

3. Consider a binary LFSR with connection polynomial $x^4 + x^3 + x^2 + x + 1$.

   a) Show that the periods of the binary sequences generated by this LFSR are 1 and 5.

   b) Consider a stream cipher based on this LFSR. The ciphertext sequence is
   1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0
   and it is given that the 4th and 12th plaintext bits are equal to **0** and the 8th and 16th bits are equal to **1**. Find the initial state of the LFSR, that is, the four first bits of the keystream sequence.

4. Consider the LFSRs with polynomials $f(x) = x^3 + x^2 + 1$ and $g(x) = x^4 + x^2 + 1$. Initialize the first LFSR with 100, and the second one with 1011 (the LFSRs are shifted from right to left). Generate the two output sequences and take their xor-sum. The task is to determine the shortest LFSR which generates the sum-sequence.

5. Let $G(x)$ be a generating function of a binary sequence $S = (z_i)_{i=0}^{\infty}$ with period p. Show that

$$G(x) = \frac{\sigma(x)}{1 + x^p}$$

   where $\sigma(x) = z_0 + z_1 x + z_2 x^2 + \ldots + z_{p-1} x^{p-1}$ is determined by the first period of the sequence. Hint:

$$G(x) = (1 + x^p + x^{2p} + ...)\sigma(x).$$

6. Let e be the exponent of $f(x)$. Show that then there is a sequence $S \in \Omega(f)$ such that the period of S is equal to e.

7. Determine the exponent of the polynomial $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$.