T-79.503 Foundations of Cryptology
Homework 2
September 24, 2003

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. 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 where the keystream is generated as output of this LFSR. The first 19 bits of the ciphertext sequence are

   `0 1 1 0 0 0 1 1 0 0 0 1 1 0 0 0 1 1 0`

   and it is given that the 16th, 17th, 18th and 19th plaintext bits are `0 0 0 0`. Decrypt the ciphertext.

3. 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.

4. Determine the exponent of the polynomial

$$x^5 + x^4 + x^3 + x^2 + x + 1.$$

   For example, you may try to find the factors of this reducible polynomial, or you may determine the periods of the sequences generated by this polynomial.

5. Let $S^{(m)}$ be a finite binary sequence, with linear complexity L. Its complemented sequence $\bar{S}^{(m)}$ is the sequence obtained from $S^{(m)}$ by complementing its terms, that is, by adding 1 *modulo* 2 to each term.

   a) Show that $LC(\bar{S}^{(m)}) \leq L + 1$.

   b) Show that $LC(\bar{S}^{(m)}) = L - 1,$ or $L,$ or $L + 1.$

6. a) Prove: If $\Omega(f) \subset \Omega(g)$, then $f(x)$ divides $g(x)$. *Hint: Handout 1, Theorem 1*

   b) Prove: For all $S(x) \in \Omega(f)$ also $\bar{S}(x) \in \Omega(f)$, if and only if $x + 1$ divides $f(x)$. (Here $\bar{S}(x)$ denotes the complemented sequence of $S(x)$.)