T-79.5501 Cryptology
Homework 5
February 20, 2007

1. For each of the following 5-bit sequences determine its linear complexity and find one of the shortest LFSR that generates the sequence.

   a) 0 0 1 1 1
   b) 0 0 0 1 1
   c) 1 1 1 0 0

2. Find the shortest LFSR which generates all three sequences of problem 1.

3. Let $S$ be a sequence of bits with linear complexity $L$. Its complemented sequence $\bar{S}$ is the sequence obtained from $S$ by complementing its bits, that is, by adding 1 *modulo* 2 to each bit.

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

4. Use the Berlekamp-Massey Algorithm to find the shortest LFSR that generates the sequence:

   `0 0 1 0 1 0 1 1 1 1 1 0 0 .`

   Is this LFSR uniquely determined?

5. Consider the 4-bit to 4-bit permutation $\pi_S$ defined as follows:

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 3 | F | 0 | 6 | A | 1 | D | 8 | 9 | 4 | 5 | B | C | 7 | 2 | E |

   (This is the fourth row of the DES S-box $S_4$.) Denote by $(x_1, x_2, x_3, x_4)$ and by $(y_1, y_2, y_3, y_4)$ the input bits and output bits respectively. Find the output bit $y_j$ for which the bias of $x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus y_j$ is the largest.

6. Suppose that $\mathbf{X}_1$ and $\mathbf{X}_2$ are independent random variables defined on the set $\{0, 1\}$. Let $\epsilon_i$ denote the bias of $\mathbf{X}_i$, $\epsilon_i = \Pr[\mathbf{X}_i = 0] - \frac{1}{2}$, for $i = 1, 2$. Prove that if the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent, then $\epsilon_2 = 0$ or $\epsilon_1 = \pm\frac{1}{2}$. (Hint: If the random variables $\mathbf{X}_1$ and $\mathbf{X}_1 \oplus \mathbf{X}_2$ are independent, then Piling-up lemma can be used to compute the bias of the $\oplus$-sum of these random variables.)