T-79.5501 Cryptology
First midterm exam, solutions
March 3rd, 2007

1. Let us first calculate the entropy of one block. There can be 0, 1 or 2 ones in a block (and 5, 4 or 3 zeros, respectively). Hence, there are

$$\binom{5}{0} + \binom{5}{1} + \binom{5}{2} = 16$$

different blocks each of which can be chosen equiprobably. Hence entropy of one block is $\log_2 16 = 4$ and the entropy of 20 equiprobable blocks is $20 * 4 = 80$. The maximum entropy of a 100 bit string is $100 > 80$..

2. The first output sequence is `1 1 1 1 ...` of period length 1, and it can also be generated using an LFSR of length 1 with polynomial $x + 1$ which is a divisor of polynomial $f(x) = x^3 + x^2 + x + 1 = (x + 1)^3$. The second output sequence is `0 1 0 1 1 1 1 0 0 0 1 0 0 1 1 | 0 1 0...` of period length 15. It follows that the sum sequence can be generated with an LFSR of length 5 with feedback polynomial $\mathrm{lcm}(x + 1, g(x)) = (x + 1)(x^4 + x + 1) = x^5 + x^4 + x^2 + 1$. This is the shortest length, because the sum sequence has 4 consecutive zeros. The feedback polynomial of degree 5 is uniquely determined as soon as at least 10 terms of the sequence are given.

3. From the given plaintext and ciphertext we get two equations for R_1

$$\begin{cases} R_1 &= 100 + f(001 + K) \text{ (encrypting over the first round)} \\ R_1 = L_2 &= 100 + f(110 + K^3) \text{ (decrypting over the third round)} \end{cases}$$

It follows that

$$f(001 + K) = f(110 + K^3). \tag{1}$$

Since f is a bijection in $\mathbb{F} = \mathbb{Z}_2[x]/(x^3 + x + 1)$ it follows that (1) can hold if and only if

$$001 + K = 110 + K^3$$

which is equivalent to

$$K + K^3 = 111 \tag{2}$$

To find a solution $K \in \mathbb{F}$, we compute the values of $z + z^3$ for all $z \in \mathbb{F}$:

z	z^3	$z+z^3$
000	000	000
001	001	000
010	011	001
011	100	111
100	101	001
101	110	011
111	010	101

It follows that there is a unique solution $K = 011$ that satisfies equation (2).

4. We denote by ε_{ij} the bias of $\mathbf{X}_i \oplus \mathbf{X}_j$. By Piling Up Lemma we have $\varepsilon_{12} = 2\varepsilon_1\varepsilon_2$ and $\varepsilon_{23} = 2\varepsilon_2\varepsilon_3$. The assumption is that the random variables $\mathbf{X}_1 \oplus \mathbf{X}_2$ and $\mathbf{X}_2 \oplus \mathbf{X}_3$ are independent. Then using the Piling Up Lemma again we have that the bias of $\mathbf{X}_1 \oplus \mathbf{X}_2 \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3)$ is equal to $2\varepsilon_{12}\varepsilon_{23} = 8\varepsilon_1\varepsilon_3\varepsilon_2^2$. But $(\mathbf{X}_1 \oplus \mathbf{X}_2) \oplus (\mathbf{X}_2 \oplus \mathbf{X}_3) = \mathbf{X}_1 \oplus \mathbf{X}_3$ which is known to have the bias equal to $\varepsilon_{13} = 2\varepsilon_1\varepsilon_3$. We get the equation

$$8\varepsilon_1\varepsilon_3\varepsilon_2^2 = 2\varepsilon_1\varepsilon_3.$$

This equation holds if and only if either $\varepsilon_2 = \pm\frac{1}{2}$ or $\varepsilon_1 = 0$ or $\varepsilon_3 = 0$.