Homework 9, due September 25

(1) (Page 61, problem 11) The following sequence was generated by a linear feedback shift register. Determine the recurrence that generated it.

```
1, 0, 1, 0, 0, 1, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1,
1, 0, 0, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0,
0, 1, 1, 0, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 0, 1,
1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 1, 1, 0, 0, 0
```

(2) (Page 146, problem 1) Consider the following DES–like encryption method. Start with a message of $2n$ bits. Divide it into two blocks of length n, a left half and a right half: M_0M_1. The key K consists of k bits, for some integer k. There is a function $f(K, M)$ that takes inputs of k and n bits and gives an output of n bits. One round of encryption starts with a pair M_jM_{j+1}. The output is the pair $M_{j+1}M_{j+2}$, where

$$M_{j+2} = M_j \oplus f(K, M_{j+1}).$$

(Here $\oplus$ means XOR, or addition mod 2 on each bit.) This is done for m rounds, so the ciphertext is M_mM_{m+1}.

If you have a machine that does the m-round encryption just described, how would you use the same machine to decrypt the ciphertext M_mM_{m+1} using the same key K?

(3) (Continued.)

(a) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose that the encryption process consists of $m = 2$ rounds. If you know only a ciphertext, can you deduce the plaintext and the key? If you know a ciphertext and the corresponding plaintext, can you deduce the key? Justify your answers.

(b) Suppose K has n bits and $f(K, M) = K \oplus M$, and suppose the encryption process consists of $m = 3$ rounds. Why is this system not secure?