T-79.4501 Cryptography and Data Security
2006 Autumn/ Homework 3
Oct 4-5, 2006

1. Given a positive integer r and a combiner function $f : \mathbb{Z}_{26} \times \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ we define a kind of *Feistel cipher* as follows:

$$
\begin{aligned}
L_i &= R_{i-1}, \\
R_i &= (L_{i-1} + f(R_{i-1}, K_i)) \bmod 26,
\end{aligned}
$$

where $K_i \in \mathbb{Z}_{26}$, and $i = 1, 2, \ldots, r$, and L_j, $R_j \in \mathbb{Z}_{26}$, $j = 0, 1, 2, \ldots, r$. The plaintext is (L_0, R_0) and the ciphertext is (L_r, R_r).

Consider a case where $r = 3$ and the combiner function f is defined as $f(X, K) = (X \times K) \bmod 26$. The plaintext is (21,10) and the ciphertext is (13,21). Apply the meet-in-the-middle solution to find the keys K_1 and K_3. (Create tables as depicted in Figure 1, and find K_1 and K_3 such that $D(K_1) = D(K_3)$.

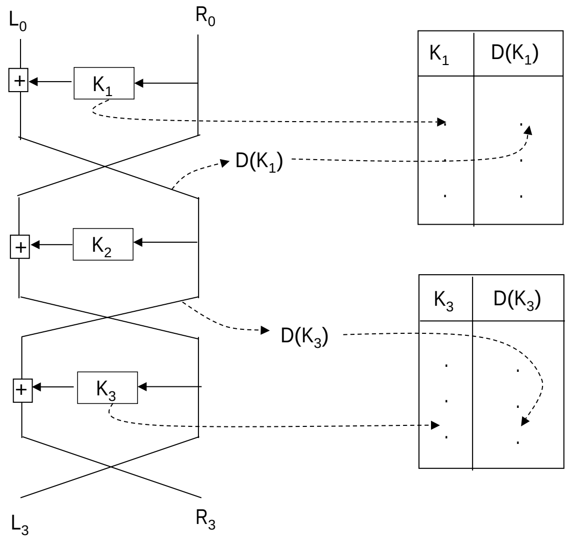

Figure 1: Meet-in-the-Middle solution

2. Consider an LFSR with feedback polynomial $f(x) = x^4 + x^3 + x^2 + x + 1$.
   (a) What are the cycles (periods) of the sequences generated by this LFSR?
   (b) Compute the values for the autocorrelation function for each cycle.

3. Consider a threshold generator (Lecture 4) with three LFSRs defined by the connection polynomials and initial states:

$$
\begin{aligned}
f_1(x) &= x^2 + x + 1, \text{ initial state } \texttt{01} \\
f_2(x) &= x^3 + x + 1, \text{ initial state } \texttt{001} \\
f_3(x) &= x^3 + x^2 + 1, \text{ initial state } \texttt{001}
\end{aligned}
$$

Compute the first 30 bits of the output sequence of the threshold generator.

(a) Is the output sequence balanced, that is, has it about equally many zeroes and ones?

(b) Compare the bits of the output sequence and the corresponding bits of the sequence generated by the third LFSR. For how many bits they are equal?

4. Suppose that a block cipher is used in CBC mode.

   (a) Suppose that a sequence P_i, $i = 1, 2, 3, ...$ of plaintext blocks have been encrypted. Assume that two equal ciphertext blocks are detected, say C_k and C_ℓ such that $C_k = C_\ell$. What can one say about the corresponding plaintexts P_k and P_ℓ?

   (b) Let n denote the block length. Using the result of (a) describe an attack which reveals some information about the plaintext, and which succeeds with probability $1/2$ after about $2^{n/2}$ plaintext blocks have been encrypted using the same key.

5. DESX was proposed by R.Rivest to protect DES against exhaustive key search. DESX uses one 64-bit secret key W to perform pre- and postwhitening of data and a 56-bit DES key K, and operates as follows:

$$C = W \oplus E_K(P \oplus W)$$

   Originally two different keys were used for pre- and postwhitening, but Kilian and Rogaway showed (Crypto '96) that the same key can be used for both. Show that a similar construction

$$C = W \oplus E_K(P)$$

   without prewhitening is insecure, and can be broken using an attack of complexity 2^{56}.

6. We consider a polynomial MAC with 4-bit coefficients in the Galois field $GF(2^4)$ with polynomial $x^4 + x + 1$. Given an one time pad $=$ `0110`, and a point $X =$ `0011`, evaluate the polynomial MAC for the message $P = (P_0, P_1, P_2) =$ `101010111100`.

7. Show that the bitwise operation of the function $F_t(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$ used in SHA-1 is exactly the same as the operation of the threshold function (also called as majority function) t used in the threshold key stream generator (see Lecture 4).