T-79.503 Foundations of Cryptology
Homework 5
October 15, 2003

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 (2,11) and the ciphertext is (8,1). Apply the meet-in-the-middle solution to find the keys K_1 and K_3. (Create tables as depicted in the figure, and find K_1 and K_3 such that $D(K_1) = D(K_3)$.

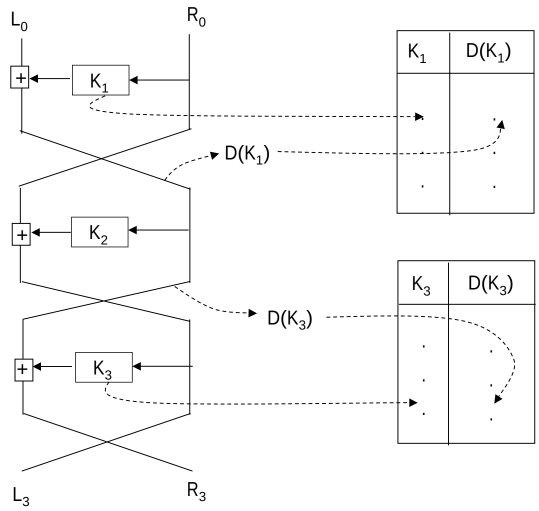

Figure 1: Meet-in-the-Middle solution

2. (cf. Stinson Exercise 3.3) Consider a Feistel cipher, where the ith round is defined as follows:

$$\begin{aligned} L_i &= R_{i-1} \\ R_i &= L_{i-1} \oplus F_i(R_{i-1} \oplus K_i), \end{aligned}$$

where K_i is the round key and F_i is the round function. Given a bit sequence A we denote by $c(A)$ the bit sequence obtained by complementing the bits of A, for example, if $A = 001$, then $c(A) = 110$. Let $Y = (L_r, R_r)$ be the ciphertext obtained by encrypting the plaintext $X = (L_0, R_0)$ (= concatenation of L_0 and R_0) using the r-round Feistel cipher with round keys $K_1, K_2, \ldots, K_r$. Show that then the plaintext $c(X)$ encrypted using the round keys $c(K_1), c(K_2), \ldots, c(K_r)$ gives the ciphertext $c(Y)$.

3. (Stinson 3.11 a)) The DES S-box S_4 has some unusual properties:

7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

Prove that the second row of S_4 can be obtained from the first row by means of the following mapping:

$$(y_1, y_2, y_3, y_4) \mapsto (y_2, y_1, y_4, y_3) \oplus (0, 1, 1, 0)$$

4. Consider the S_4. Let us set $a = 101110$. Which values the difference $S_4(x \oplus a) \oplus S_4(x)$ takes as x varies through the sixteen values $x = (1, x_2, x_3, x_4, x_5, 1)$?

5. (Stinson 3.7) Suppose a sequence of plaintext blocks, $x_1, x_2, ..., x_n$ yields the ciphertext sequence $y_1, y_2, ..., y_n$. Suppose that one ciphertext block, say y_i, is transmitted incorrectly (i.e., some `1`'s are changed to `0`'s and vice versa). Show that the number of plaintex blocks that will be decrypted incorrectly is equal to 1 if ECB or OFB modes are used for encryption; and equal to two if CBC or CFB modes are used.