TMA4155 — Exercise 2

Kristian Gjøsteen

2006-09-07

Task 1 — Feistel ciphers

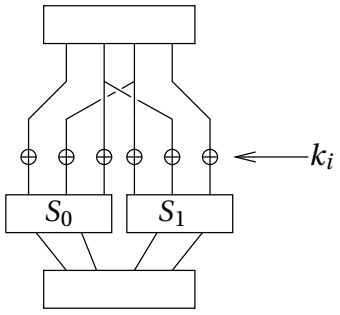
In a known plaintext attack, we can always find the key by trying all possible keys (exhaustive search). One class of interesting attacks try to find the key faster than exhaustive search.

a. The block cipher has block length 8, key length 8 and two rounds. The round function $F : \{0,1\}^4 \times \{0,1\}^4 \to \{0,1\}^4$ is given by $F(R_i, k_i) = k_i$. The round keys are derived from the key k as follows: k_0 is the first four bits of k, and k_1 is the last four bits.

Encrypt the block 0000 0000 with the key 0101 0101, and the block 0000 0000 with the key 1111 1111. Decrypt and check that everything works correctly.

Find a known plaintext attack that works better than brute force.

b. The block cipher has block length 8, key length 8 and four rounds. The round function is given by the diagram:



S_0 and S_1 are two S-boxes given by the table:

	000	001	010	011	100	101	110	111
S_0	00	01	00	01	10	11	10	11
S_1	10	00	11	10	11	00	01	01

The round keys are 6 bits and are derived from the key k as follows: k_0 is the first six bits, k_1 the middle six, k_2 the last six, and k_3 the three first and three last bits.

Encrypt the block 0000 0000 with the key 0101 0101 and the block 0000 0000 with the key 1111 1111. Decrypt and check that everything works correctly.

Try to find a known plaintext attack that works better than brute force. (Hint: Try to break just the first round. Then you try two rounds, then three, and finally four rounds.)

Task 2 — Non-Feistel cipher

In this task, we will look at a non-Feistel block cipher.

The block cipher has block length 36 and key length 36. Vi divide the block into nine *nibbles*, each of four bits, and arrange the nibbles in a 3×3-matrix.

To describe the cipher we need four matrix operations.

The first is a substitution operation. We define a substitution on nibbles (b_0, b_1, b_2, b_3) by the following table:

$b_2b_3 \setminus b_0b_1$	00	01	10	10
00	1011	0110	0111	1000
01	1100	0101	1001	1010
10	1101	0100	0000	0001
11	0010	0011	1111	1110

This is extended to an operation on the 3×3-matrix by applying the substitution on all nibbles independently. This operation is denoted by *SB*.

The next operation is to rearrange the nibbles in the table rows, according to the following map:

$$\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{11} & m_{12} & m_{10} \\ m_{22} & m_{20} & m_{21} \end{pmatrix}$$

This operation is denoted by *SR*.

The third operation is to mix the nibbles downwards in the columns as follows:

$$\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix} \mapsto \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{00} \oplus m_{10} & m_{01} \oplus m_{11} & m_{02} \oplus m_{12} \\ m_{00} \oplus m_{10} \oplus m_{20} & m_{01} \oplus m_{11} \oplus m_{21} & m_{02} \oplus m_{12} \oplus m_{22} \end{pmatrix}$$

On matrix form, we can write this as:

$$\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix}$$

This operation is denoted by *MC*.

Finally, we have an operation that applies the round key. Each round key is 36 bits long, and we arrange it into nine nibbles in a 3×3-matrix. The round key $K^{(i)}$ is applied as follows:

$$\begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix} \quad \mapsto \quad \begin{pmatrix} k_{00}^{(i)} \oplus m_{00} & k_{01}^{(i)} \oplus m_{01} & k_{02}^{(i)} \oplus m_{02} \\ k_{10}^{(i)} \oplus m_{10} & k_{11}^{(i)} \oplus m_{11} & k_{12}^{(i)} \oplus m_{12} \\ k_{20}^{(i)} \oplus m_{20} & k_{21}^{(i)} \oplus m_{21} & k_{22}^{(i)} \oplus m_{22} \end{pmatrix}$$

Applying the ith round key is denoted by $ARK(i)$.

The round keys are derived from the key as follows: Split the key into nine nibbles and arrange them in a 3×3-matrix. Apply the operations *SB* and *SR* to the matrix to get K_0. Then apply *MC*, *SB* and *SR* to K_0 to get K_1. Finally apply *MC*, *SB* and *SR* to K_1 to get K_2.

The encryption function for the block cipher is: $ARK(0)$, *SB*, *SR*, *MC*, $ARK(1)$, *SB*, *SR*, $ARK(2)$.

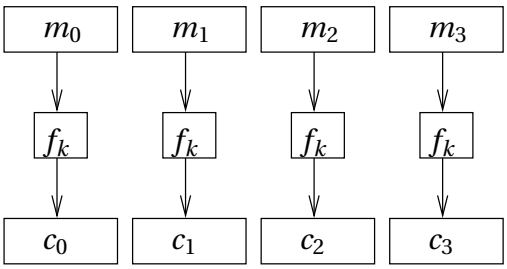
a. Find inverse operations for *SB*, *SR* and *MC*. Use these inverse operations to describe the decryption function for the block cipher.

b. Encrypt 0000 0000 0000 0000 0000 0000 0000 0000 0000 with the key 0011 0011 0011 0011 0011 0011 0011 0011 0011.

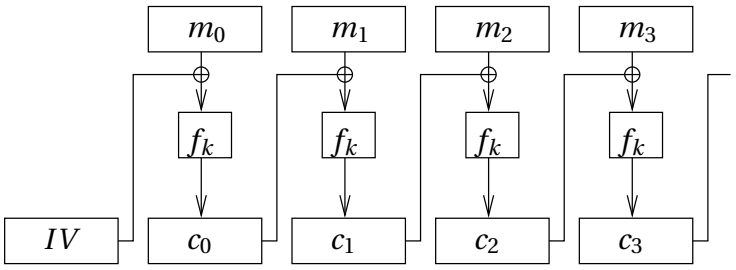
c. Find a known plaintext attack that works better than brute force. (Hint: See if any operations leave any nibbles untouched, and concentrate on these nibbles.)

Task 3 — Block cipher modes

Let (f, g) be a block cipher. In ECB mode we encrypt like this:



In CBC mode we encrypt like this (IV is *initialization vector*):



a. Explain using diagrams how to decrypt in ECB mode and in CBC mode.

b. In a certain protocol, Alice will at a given time send one of 16 possible commands to Bob. Based on this command, Bob will perform some action (observable by anyone, and Eve in particular) the day after the protocol completes. This is repeated every day, so that the action Bob performs on Monday is determined by the command sent by Alice on Sunday.

The channel used for the protocol is insecure, so to keep the command secret it is encrypted using f and a key k shared by Alice and Bob. Four bits are used to represent the command, and the remainder of the bits in the block m are set to 0. Then Alice sends $c = f(k, m)$ over the insecure channel.

Eve wants to know which command was sent by Alice before Bob actually performs the specified action. Explain how Eve is able to determine this after listening to the protocol executions for a few weeks.

Can you suggest a simple modification to the protocol that will protect against the passive listener Eve.