TMA4155 — Solutions to exercise 2

Kristian Gjøsteen

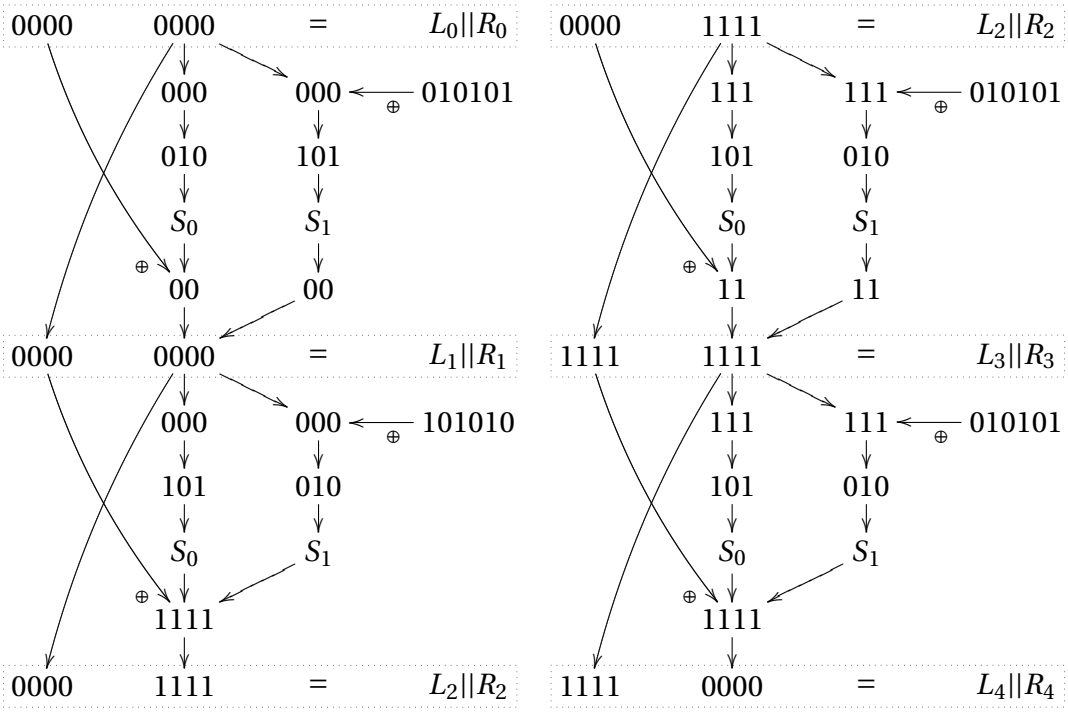
2006-11-27

Task 1

a. Let $(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)$ be the block and $(k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ be the key. After round 0 we have the block blokken $(b_4, b_5, b_6, b_7, b_0 \oplus k_0, b_1 \oplus k_1, b_2 \oplus k_2, b_3 \oplus k_3)$ and after round 1 we have the block $(b_0 \oplus k_0, b_1 \oplus k_1, b_2 \oplus k_2, b_3 \oplus k_3, b_4 \oplus k_4, b_5 \oplus k_5, b_6 \oplus k_6, b_7 \oplus k_7)$. The encryption c of the block b under the key k is simply $c = b \oplus k$.

A known plaintext attack (where we get b and c) trivially reveals the key, since $k = c \oplus b$.

b. The key is $k = 01010101$, giving round keys $k^{(0)} = 010101$, $k^{(1)} = 101010$, $k^{(2)} = 010101$, $k^{(3)} = 010101$. In diagram form, we get:



To decrypt we do this in the opposite direction.

For the key $k = 11111111$ all the round keys are $k^{(i)} = 111111$. Encrypting the block 00000000 goes as follows:

In round 0 the right hand side expansion gives 000000. Adding the round key gives 111111, and applying the S-boxes gives $1101 = F(0000, k^{(0)})$. We get the block 00001101 after round 0.

In round 1 the right hand side expansion gives 101011. Adding the round key gives 010100, and applying the S-boxes gives $0011 = F(1101, k^{(1)})$. We get the block 11010011 after round 1.

In round 2 the right hand side expansion gives 010101. Adding the round key gives 101010, and applying the S-boxes gives $1111 = F(0011, k^{(2)})$. We get the block 00110010 after round 2.

In round 3 the right hand side expansion gives 010100. Adding the round key gives 101011, and applying the S-boxes gives $1110 = F(0010, k^{(3)})$. We get the block 00101101 after round 3.

We get one attack on the block cipher by observing that in the S-box S_0 the second output bit is always equal to the third input bit. Suppose the key is $k = (k_0, k_1, k_2, k_3, k_4, k_5, k_6, k_7)$ and the block is $b^{(0)} = (b_0^{(0)}, b_1^{(0)}, b_2^{(0)}, b_3^{(0)}, b_4^{(0)}, b_5^{(0)}, b_6^{(0)}, b_7^{(0)})$. Then after round i, where the input block is $b^{(i)}$ and the output block is $b^{(i+1)}$, we have

$$b_5^{(i+1)} = b_1^{(i)} \oplus b_5^{(i)} \oplus k_2^{(i)}.$$

Because of the Feistel structure we have that $b_1^{(i+1)} = b_5^{(i)}$. Therefore, b_1 and b_5 are never influenced by the other input bits.

Now we can track the evolution of these two bits through the cipher. After round 0 we get that $b_5^{(1)} = b_1^{(0)} \oplus b_5^{(0)} \oplus k_2$.

After round 1 we get that $b_5^{(2)} = b_5^{(0)} \oplus (b_1^{(0)} \oplus b_5^{(0)} \oplus k_2) \oplus k_3 = b_1^{(0)} \oplus k_2 \oplus k_3$.

After round 2 we get that $b_5^{(3)} = (b_1^{(0)} \oplus b_5^{(0)} \oplus k_2) \oplus (b_1^{(0)} \oplus k_2 \oplus k_3) \oplus k_4 = b_5^{(0)} \oplus k_3 \oplus k_4$.

After round 3 we get that $b_5^{(4)} = (b_1^{(0)} \oplus k_2 \oplus k_3) \oplus (b_5^{(0)} \oplus k_3 \oplus k_4) \oplus k_2 = b_1^{(0)} \oplus b_5^{(0)} \oplus k_4$.

When we know $b_5^{(0)}$ og $b_5^{(4)}$, we get the equation $k_4 = b_5^{(0)} \oplus b_5^{(4)}$. We also get $b_1^{(4)} = b_5^{(3)} = b_5^{(0)} \oplus k_3 \oplus k_4$.

This gives us two equations with two unknowns (k_3 and k_4). Then we can search through the remaining six bits to find the correct key. This reduces the work load to 2^6 key trials, a significant improvement on an exhaustive search of 2^8 keys.

Task 2

a. The inverse table for SB is:

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

The inverse rearrangement for SR is:

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

The inverse operation for MC is:

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

On matrix form, we can write this as

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

The decryption operations are: $ARK(2)$, SR^{-1}, SB^{-1}, $ARK(1)$, MC^{-1}, SR^{-1}, SB^{-1}, $ARK(0)$.

b. Map the nibble (b_0, b_1, b_2, b_3) to the number $b_0 2^3 + b_1 2^2 + b_2 2^1 + b_3 2^0 \in \{0, 1, \ldots, 15\}$, and write this number as a hexadecimal digit, where 10 is A, 11 is B, ..., and 15 is F. The round keys are

$$K_0 = \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix}, \quad K_1 = \begin{pmatrix} D & D & D \\ B & B & B \\ D & D & D \end{pmatrix}, \quad K_2 = \begin{pmatrix} A & A & A \\ 4 & 4 & 4 \\ F & F & F \end{pmatrix}.$$

We proceed with the encryption operations:

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \overset{ARK0}{\rightarrow} \begin{pmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{pmatrix} \overset{SB}{\rightarrow} \begin{pmatrix} D & D & D \\ D & D & D \\ D & D & D \end{pmatrix}$$

$$\overset{SR}{\rightarrow} \begin{pmatrix} D & D & D \\ D & D & D \\ D & D & D \end{pmatrix} \overset{MC}{\rightarrow} \begin{pmatrix} D & D & D \\ 0 & 0 & 0 \\ D & D & D \end{pmatrix} \overset{ARK1}{\rightarrow} \begin{pmatrix} 0 & 0 & 0 \\ B & B & B \\ 0 & 0 & 0 \end{pmatrix}$$

$$\overset{SB}{\rightarrow} \begin{pmatrix} B & B & B \\ F & F & F \\ B & B & B \end{pmatrix} \overset{SR}{\rightarrow} \begin{pmatrix} B & B & B \\ F & F & F \\ B & B & B \end{pmatrix} \overset{ARK2}{\rightarrow} \begin{pmatrix} 1 & 1 & 1 \\ B & B & B \\ 4 & 4 & 4 \end{pmatrix}$$

c. The idea is that the nibbles on the top row are only touched by $ARK(i)$ and SB, and those operations apply independently to each nibble. Therefore, we can analyse the block cipher action on these nibbles independently.

Further we note that the part of the round key exclusive-ored to these three nibbles are derived just from the corresponding key nibbles. So the action on each of the three nibbles is solely determined by the the corresponding key nibble, so we can search for each key nibble independently. Therefore, three searches through 16 possibilities give us 12 key bits. While we could continue the analysis, searching for the remaining 24 bits is easy.

Task 3

a. Diagram for ECB mode decryption:

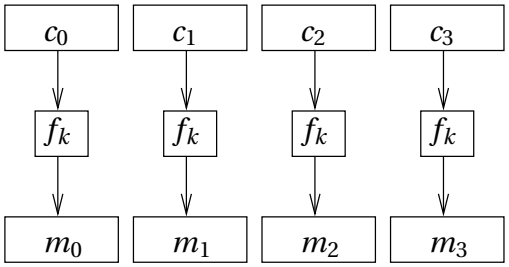
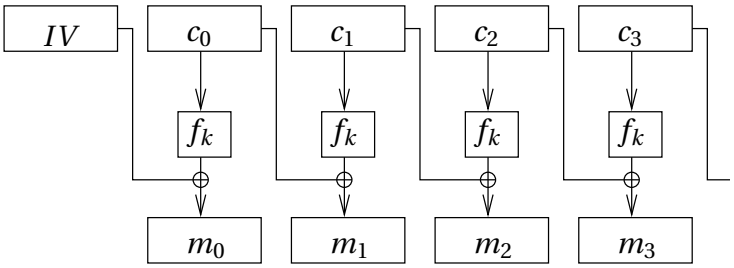


Diagram for CBC mode decryption:



b. Every time Alice sends a given command, the ciphertext is the same. So Eve observes the command sent and notes it to the action performed the next day. The next time Eve sees the command, she will know what action Bob performs the next day.

The simplest countermeasure is to encrypt the command using CBC mode. Then every ciphertext will be different, even if they decrypt to the same command.