M1-MOSIG - Crypto - Exercises : DES

1 S-Boxes

Table 1 describes the S-boxes of the DES cipher. Recall that each S-box has 6 input bits and 4 output bits. For an input vector $(x_0, x_1, x_2, x_3, x_4, x_5)$, the output value is the hexadecimal entry located at position (i, j) in the table, where the binary representation of i and j are respectively (x_0, x_5) and (x_1, x_2, x_3, x_4).

Suppose that the 48 bits register of input to the S-boxes contains the hexadecimal value `1 5 D A 0 5 8 B E 4 1 8`. What is the output of the S-Boxes?

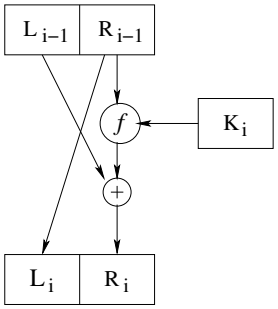
S_1															
E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7
0	F	7	4	E	2	D	1	A	6	C	B	9	5	3	8
4	1	E	8	D	6	2	B	F	C	9	7	3	A	5	0
F	C	8	2	4	9	1	7	5	B	3	E	A	0	6	D
S_2															
F	1	8	E	6	B	3	4	9	7	2	D	C	0	5	A
3	D	4	7	F	2	8	E	C	0	1	A	6	9	B	5
0	E	7	B	A	4	D	1	5	8	C	6	9	3	2	F
D	8	A	1	3	F	4	2	B	6	7	C	0	5	E	9
S_3															
A	0	9	E	6	3	F	5	1	D	C	7	B	4	2	8
D	7	0	9	3	4	6	A	2	8	5	E	C	B	F	1
D	6	4	9	8	F	3	0	B	1	2	C	5	A	E	7
1	A	D	0	6	9	8	7	4	F	E	3	B	5	2	C
S_4															
7	D	E	3	0	6	9	A	1	2	8	5	B	C	4	F
D	8	B	5	6	F	0	3	4	7	2	C	1	A	E	9
A	6	9	0	C	B	7	D	F	1	3	E	5	2	8	4
3	F	0	6	A	1	D	8	9	4	5	B	C	7	2	E
S_5															
2	C	4	1	7	A	B	6	8	5	3	F	D	0	E	9
E	B	2	C	4	7	D	1	5	0	F	A	3	9	8	6
4	2	1	B	A	D	7	8	F	9	C	5	6	3	0	E
B	8	C	7	1	E	2	D	6	F	0	9	A	4	5	3
S_6															
C	1	A	F	9	2	6	8	0	D	3	4	E	7	5	B
A	F	4	2	7	C	9	5	6	1	D	E	0	B	3	8
9	E	F	5	2	8	C	3	7	0	4	A	1	D	B	6
4	3	2	C	9	5	F	A	B	E	1	7	6	0	8	D
S_7															
4	B	2	E	F	0	8	D	3	C	9	7	5	A	6	1
D	0	B	7	4	9	1	A	E	3	5	C	2	F	8	6
1	4	B	D	C	3	7	E	A	F	6	8	0	5	9	2
6	B	D	8	1	4	A	7	9	5	0	F	E	2	3	C
S_8															
D	2	8	4	6	F	B	1	A	9	3	E	5	0	C	7
1	F	D	8	A	3	7	4	C	5	6	B	0	E	9	2
7	B	4	1	9	C	E	2	0	6	A	D	F	3	5	8
2	1	E	7	4	A	8	D	F	C	9	0	3	5	6	B

Table 1: Les boîtes S de DES

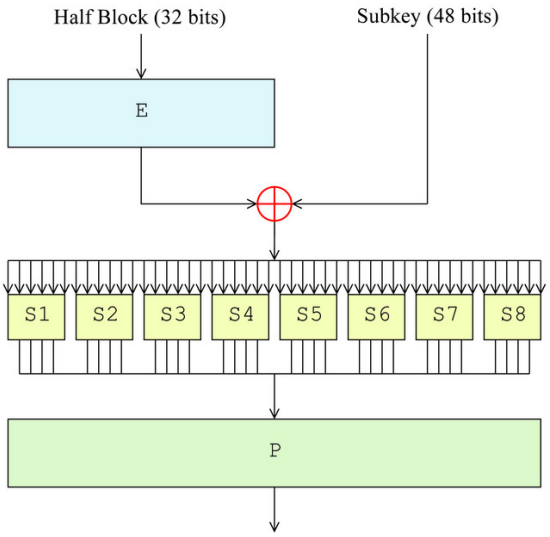
2 Diffusion in the DES cipher

We recall that the DES cipher (Data Encryption Standard) proceeds in 16 rounds. IN the following, we will not consider the initial permutation IP nor the final permutation. The $j-$th bit from the left of a block L_i will be denoted by $L_i(j)$, the $j-$th bit from the left of a block R_i will be denoted by $R_i(j)$.

Each round is of the form



where f is the Feistel function :



The expansion function E extends a 32 bits block into a 48 bits block where some bits are repeated. The permutation P permutes the output of the eight SBox. These two functions are described as follows:

$$\mathrm{E} = \begin{array}{|cccccc|}\hline 32 & 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 10 & 11 & 12 & 13 \\ 12 & 13 & 14 & 15 & 16 & 17 \\ 16 & 17 & 18 & 19 & 20 & 21 \\ 20 & 21 & 22 & 23 & 24 & 25 \\ 24 & 25 & 26 & 27 & 28 & 29 \\ 28 & 29 & 30 & 31 & 32 & 1 \\ \hline \end{array} \qquad \mathrm{P} = \begin{array}{|cccccccc|}\hline 16 & 7 & 20 & 21 & 29 & 12 & 28 & 17 \\ 1 & 15 & 23 & 26 & 5 & 18 & 31 & 10 \\ 2 & 8 & 24 & 14 & 32 & 27 & 3 & 9 \\ 19 & 13 & 30 & 6 & 22 & 11 & 4 & 25 \\ \hline \end{array}$$

For example, these tables indicate that the 4th input bit of E is copied in the fifth and seventh position in the output. Similarly the fifteenth input bit of P is output in the tenth position.

We consider the first bit of the message M to be encrypted (the leftmost bit $L_1(1)$ of the left half block L_1).

1. After a round, which bits of L_2 and R_2 depend on $L_1(1)$? Why ?
2. After a second round, which bits of L_3 depend on $R_2(1)$? Why?
3. During this second round, which bits of the output of the function E (denoted by $E_2(i)$) depend on $R_2(1)$?
4. During this second round, which bits in the output of the SBOX, (denoted by $S_2(i)$) depend a priori on $R_2(1)$? For the sake of simplicity, we will assume that all output bits are modified if at least one bit in the input is modified.
5. During this second round, which bits of the output of the permutation P (denoted by $P_2(i)$) depend on $R_2(1)$?
6. After the second round, which bits of R_3 depend on $L_1(1)$?
7. For each of these bits, list the SBOX that will be affected in the third round.
8. Conclude on the minimal number of rounds required to ensure the diffusion of $L_1(1)$ in all the bits of the block R.
9. After 3 rounds, how many bits of L_4 depend on $L_1(1)$?
10. What is the minimal number of rounds required to ensure the diffusion of $L_1(1)$ into the whole cipher-text ?

3 Triple cipher modes

To improve the security of DES, triple cipher modes have been introduced. The most classical one is the triple mode $ECB|ECB|ECB : C_i = DES_{K3}(DES_{K2}(DES_{K1}(M_i))$. In other terms, there is three distinct ciphers applied in sequence. The blocks are treated independently one with each other (ECB mode).

In class we considered the the 3DES as a particular cipher, parameterized by a triple key: $C_i = 3DES_{K1,K2,K3}(M_i)$.

1. Recall the principle of the CBC mode. Blocks of source-text are denoted by M_i and blocks of cipher-text by C_i,
2. Compare a DES in triple mode $ECB|ECB|ECB$ and a $3DES - EEE$ in mode ECB.
3. Is a DES in triple mode $ECB|ECB|CBC$ identical to a 3DES with a CBC mode ?
4. We now consider a triple D.E.S in mode $CBC|CBC|ECB$, as illustrated on figure 1 where E is the encoding of D.E.S. :

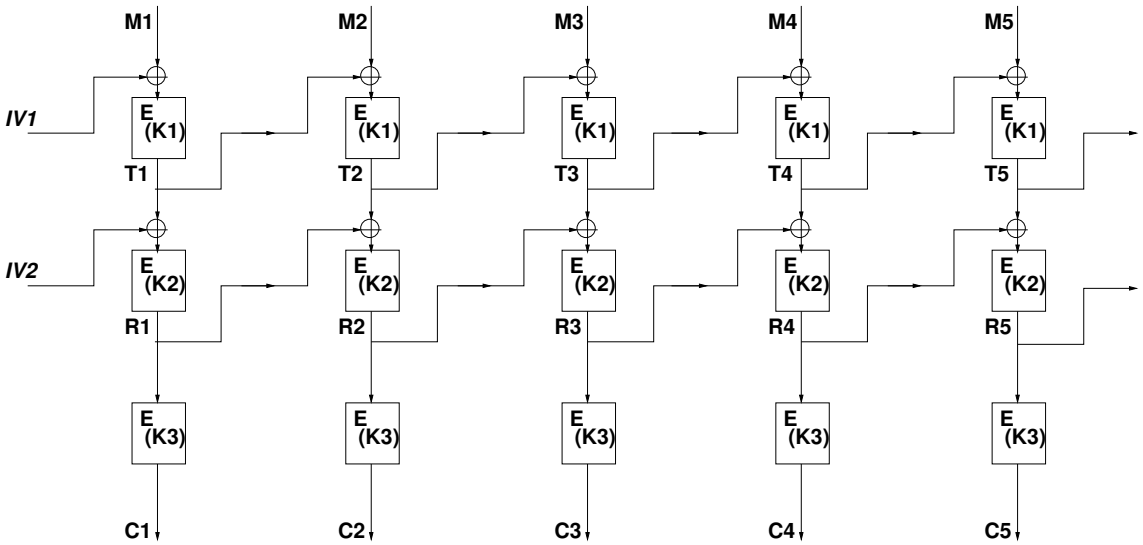


Figure 1: Triple DES in mode $CBC|CBC|ECB$.

(a) Express the the formula between the M_i and T_i ; the T_i and R_i and the R_i and C_i.

(b) Express the decoding formula.

(c) Recall what is a *chosen cipher-text attack*.

(d) We consider a chosen cipher-text attack with the cipher-texts C_1, C_2, C_3 and C_1^*, C_2, C_3 which only differ on the first block. We obtain M_1, M_2, M_3 and M_1^*, M_2^*, M_3^*. Express $M_3 \oplus M_3^*$.

(e) Deduce from the previous questions a brute force attack to recover one of the three keys. What is the worst case complexity of this attack

(f) Can this exhaustive method produce erroneous keys?

(g) What is the probablility that the actual key is the only one found by the exhaustive attack? Give an estimate?

(h) How to improve this probability? Quantify this improvement.

(i) Once that a key is obtained, propose an attack to recover the two other ones.

(j) What is the overall complexity to recover the 3 keys?

(k) How to protect yourself against such an attack?