1 Symmetric Encryption

In the lecture we discussed the Data Encryption Standard (DES) as an example of a modern symmetric encryption cipher. In the following, we briefly introduce a simplified version of the DES.

1.1 Key Generation

In simplified DES, one master key is used to generate multiple sub-keys (so called round keys). Figure 1 depicts the algorithm to generate round keys in our simplified version of DES: It takes a 10-bit master key as input and produces two 8-bit round keys using permutations and shifts.

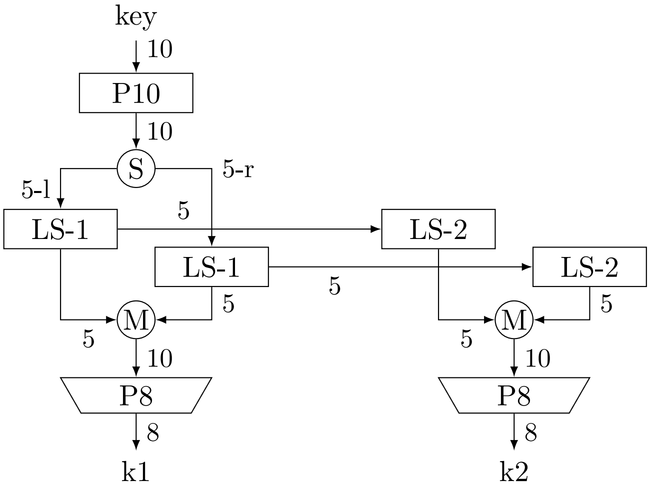

Figure 1: Round Key Generation

The operator S splits a bit sequence of length 10 into two bit sequences of length 5: 5-l (for left) denote the first 5 bits and 5-r (for right) denote the second 5 bits. The operator M concatenates two bit sequences of length 5 to produce a bit sequence of length 10 (again, the left input denotes the first 5 bits and the right input the second 5 bits). The functioning of the permutation tables P10 and P8 as well as the shifts LS-1 and LS-2 are described in Tab. 1. The table shows the position of each input bit in the output bit sequence after applying the corresponding permutation. Using P10, for example, the 3^{th} input bit becomes the 1^{st} output bit, the 5^{th} input bit becomes the 2^{nd} output bit, etc.

1.2 Encryption and Decryption

Encryption in our simplified version of DES is described by the Feistel structure depicted in Fig. 2. The internal functioning of the f function is shown in Fig. 3. The permutation tables IP, IP^{-1}, E/P, and P4 are described in Tab. 2.

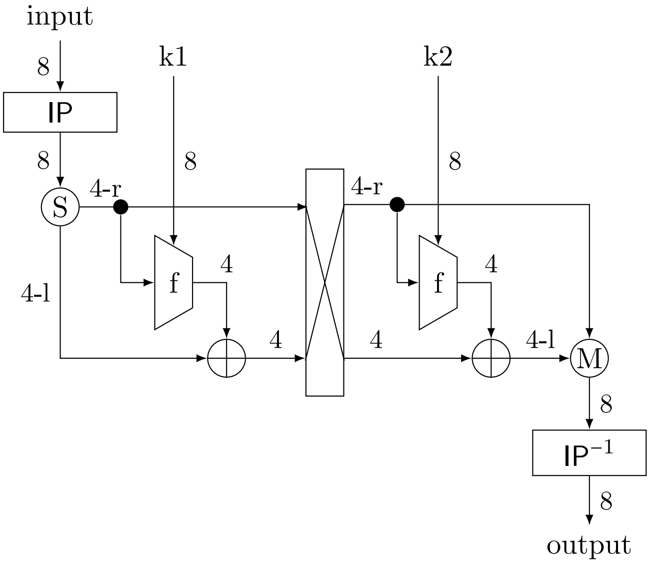

Figure 2: Encryption

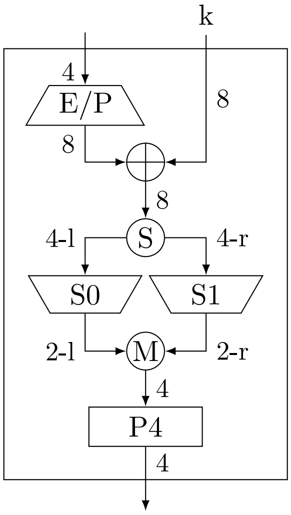

Figure 3: Function f

The substitution tables S0 and S1 are depicted in Tab. 3 and Tab. 4. The tables get 4 bits as input: the first and the last bit specify the row, and the second and the third specify the column of the corresponding output. For example, 0101 denotes the row 01 (which corresponds to 1 in decimal notation) and the column 10 (which corresponds to 2 in decimal notation). Thus, the corresponding output for table S0, for example, can be found in row 1 and column 2 of the table, which is 1 (which corresponds to 01 in binary notation).

Decryption in our simplified version of DES is similar to encryption except that we swap the round keys k1 and k2.

1.3 Tasks

In the following you will encrypt and decrypt the following text using our simplified version of DES:

EXETER

Table 1: Permutation Tables.

	1	2	3	4	5	6	7	8	9	10
P10	3	5	2	7	4	10	1	9	8	6
LS-1	2	3	4	5	1	-	-	-	-	-
LS-2	3	4	5	1	2	-	-	-	-	-
P8	6	3	7	4	8	5	10	9	-	-

To this end you should use the following key:

0110100111

T1.1 Compute the round keys (including intermediate results).

T1.2 Convert the above text to bit representation in ASCII and encrypt the first letter using the algorithm (including intermediate results).

T1.3 Decrypt the first letter using the algorithm (including intermediate results).

T1.4 Implement our simplified version of DES in Python. The program should be called `myDes` and take three input parameters:

- the first parameter is either `enc` or `dec` to encrypt or decrypt.
- the second parameter is a string representing the 10-bit key.
- the third parameter is a string representing the 8-bit input.

The program should return only the 8-bit result. For example:

```
>myDes enc "1010101010" "00110011"
>01010101
```

Table 2: Permutation Tables.

	1	2	3	4	5	6	7	8
IP	2	6	3	1	4	8	5	7
IP^{-1}	4	1	3	5	7	2	8	6
E/P	4	1	2	3	2	3	4	1
P4	2	4	3	1	-	-	-	-

Table 3: S_0

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

Table 4: S_1,

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3