Cybersecurity MSc: Applied Cryptography 2023-24

1st Project: Enhanced DES (E-DES)

October 12, 2023 Due date: November 5, 2023

Changelog

- v1.0 - Initial version.
- v1.1 - Fixed errors in the indexes used to compute input values for S-Boxes.
- v1.2 - Added figure to show how S-Boxes are used.
- v1.3 - The C code in page 3 was using the `^` operator instead of the `+`. The type of `index` also changed to `uint8_t`.

1 Introduction

DES is a milestone in the universe of symmetric block ciphers. However, due to the time at which it was conceived, it became obsolete due to two factors: slowness and reduced key size. The slowness is mainly due to bit operations performed in software, namely permutations. The original dimension of the key, of only 56 bit, was indeed considered by several people to be too short at the time of the algorithm standardization.

In this project we want to explore a variant of DES, so-called E-DES. This variant uses less operations to implement a cipher with a DES resemblance, namely it uses solely Feistel Networks and S-Boxes. S-Boxes are a normal building block in many ciphers, and DES is no exception. However, DES uses static S-Boxes, an option that often raises concerns about hidden cryptanalysis trapdoors. In E-DES we will use variable, key-dependent S-Boxes. Furthermore, E-DES will use longer, 256-bit keys.

2 Homework

The work consists on implementing a variant of DES (E-DES), which will be similar to DES but with a longer, 256-bit key and faster functions on the Feistel networks (16, as in DES). The input and output blocks must have the same size, 64 bits.

The (normally unidirectional) function used in each Feistel Network should be implemented exclusively by an S-Box. All 16 S-Boxes should be different and not generated from each other. In other words, they should be generated from the key, the generation process should not allow to discover an S-Box from the value of any of the 15 other, and S-Boxes cannot be equal. Finally, it should not be easy to discover the key from any subset of the S-Boxes.

The values of the 16 S-Boxes should be deterministically computed only once, during the key set-up, in order to speed-up encryptions and decryptions. Do not use language-dependent shuffling features, such as in Python, because you do not know how they operate (usually, they use some degree of randomness).

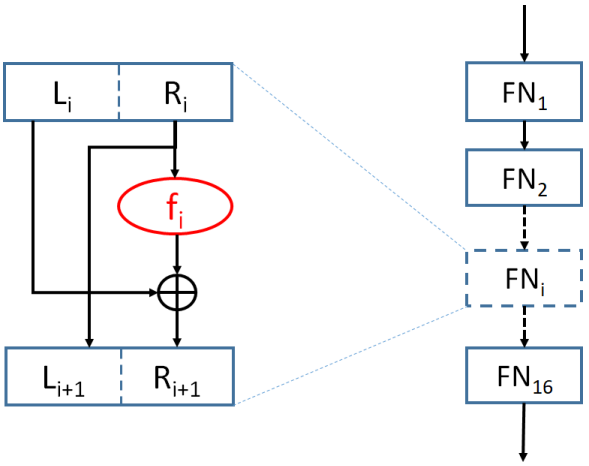

Figure 1: Overview of E-DES, with 16 Feistel Networks. Each f_i function is implemented by a different S-Box. Unlike DES, there is no initial and final bit permutations.

The totality of the 16 S-Boxes must have exactly 16 equal byte values, but these do not need to be equally distributed by all S-Boxes. For instance, one S-Box can have many zero values, and another one no zero values, but the totallity of the S-Boxes must have exactly 16 zeros.

The values in each S-Box are the output for a byte-long input. Each S-Box must be used to transform all individual bytes presented as input for the function used on the respective Feistel Network.

Since S-Boxes will be used to transform 4-byte values a byte at the time, the algorithm to increase the entropy introduced by each S-Box within an f function should be the following (see Figure 2):

- The output byte in the lowest memory address (offset 0) should be the output of the S-Box for the input byte in the higher memory address (offset 3);
- The output byte in the next memory address (offset 1) should be the output of the S-Box for an input with the sum modulo 256 of the two input bytes in the higher memory addresses (offsets 2 and 3);
- The output byte in the next memory address (offset 2) should be the output of the S-Box for an input with the sum modulo 256 of the three input bytes in the higher memory addresses (offsets 1, 2 and 3);
- The output byte in the highest memory address (offset 3) should be the output of the S-Box for an input with the sum modulo 256 of the four input bytes.

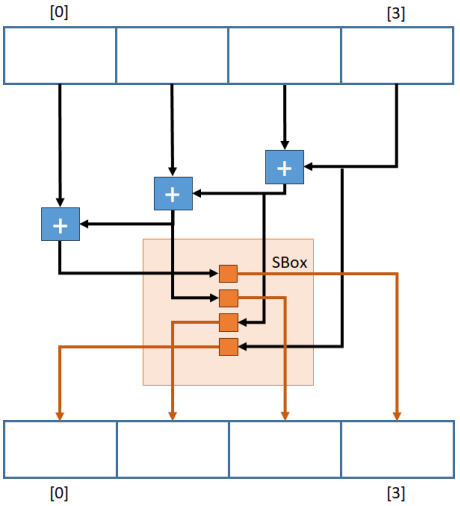

Figure 2: Overview of byte transformations with an S-Box in E-DES.

In C, an f function for a given S-Box should work as follows:

```
uint8_t SBox[256];

uint8_t in[4];
uint8_t out[4];

uint8_t index = in[3];
out[0] = sbox[index];

index = (index + in[2]);
out[1] = sbox[index];

index = (index + in[1]);
out[2] = sbox[index];

index = (index + in[0]);
out[3] = sbox[index];
```

Note that the 4-byte input and output values of the f functions only process half the bytes of the input and output of Feistel networks used in E-DES (which deal with 64-bit input/output values).

2.1 Applications

Besides implementing E-DES in a module (or library), you should implement two applications, `encrypt` and `decrypt`. These should receive one textual password as argument, which will be used to generate the 256-bit key of E-DES. An option should also be available to default to the normal DES.

The applications should process the input from `stdin` and produce a result to `stdout`. E-DES (or DES) should be used to process the input in ECB mode with a PKCS#7 padding.

Each of these applications must be implemented in two different languages, say A and B. You should be able to encrypt with a program written in A and decrypt with a program written in B; and vice-versa.

Create a third application, `speed`, to evaluate the relative performance of your E-DES implementation and one or more library implementation of DES. For that, allocate a 4KiB buffer (a memory page), fill it with random values (you can use `/dev/urandom` for that), and evaluate the time it takes to encrypt and decrypt the buffer with DES (from the library) and E-DES (both in ECB mode). Perform at least 100 000 measurements of each operation, and present the lowest values observed for each (i.e. the maximum achievable speed). For each measurement, use new, random keys. For accurate timing you can use the Linux system call `clock_gettime` function, which provides a nanosecond precision. Note that the measurements must encompass only encryptions and decryptions, and not DES or E-DES key-related set-up operations.

For improving the accuracy of measurements, it is advised to use some degree of loop unrolling for reducing the relative weight of cycle-related branching along the measurement. With the C language, loop unrolling can be easily achieved by means of preprocessor macros.

2.2 Library implementations of DES in Linux

In C, you can use these library implementations:

- The OpenSSL crypto library;
- The Nettle library.

In C++, you can use this library implementations:

- The Crypto++ library.

In Java, you can use these library implementations:

- The Java Runtime Environment;

- IAIK JCE;
- Bouncy Castle Crypto Library.

In Python, you can use these library implementations:

- Cryptography;
- PyCrypto.

3 Evaluation

The project will be evaluated as follows:

- Implementation of E-DES (in any two different languages): 40%;
- Implementation of the applications (in any two languages): 10% for `encrypt`, 10% for `decrypt`, 10% for `speed`;
- Written report, with a complete explanations of the strategies followed and the results achieved: 30%

4 Homework delivery

Send your code to the course teachers through Elearning (a submission link will be provided). Include a small report, with no more than 6 pages, describing the implementation (not a complete copy of the code developed!). Code snippets may be used to illustrate your implementation.

Every piece of code imported from anywhere must be stated in the report and in the code itself. Failure to do so will be penalised.

5 Test vectors

With the following S-Boxes (defined in C):

```
uint8_t SBox_01 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_02 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_03 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
```

```
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_04 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_05 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_06 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_07 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_08 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_09 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
```

```
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_10 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_11 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_12 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_13 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_14 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
uint8_t SBox_15 = {
    0x00, 0x00, 0x01, 0x01, 0x02, 0x02, 0x03, 0x03, 0x04, 0x04, 0x05, 0x05, 0x06, 0x06, 0x07, 0x07,
    0x08, 0x08, 0x09, 0x09, 0x0a, 0x0a, 0x0b, 0x0b, 0x0c, 0x0c, 0x0d, 0x0d, 0x0e, 0x0e, 0x0f, 0x0f,
    0x10, 0x10, 0x11, 0x11, 0x12, 0x12, 0x13, 0x13, 0x14, 0x14, 0x15, 0x15, 0x16, 0x16, 0x17, 0x17,
    0x18, 0x18, 0x19, 0x19, 0x1a, 0x1a, 0x1b, 0x1b, 0x1c, 0x1c, 0x1d, 0x1d, 0x1e, 0x1e, 0x1f, 0x1f,
    0x20, 0x20, 0x21, 0x21, 0x22, 0x22, 0x23, 0x23, 0x24, 0x24, 0x25, 0x25, 0x26, 0x26, 0x27, 0x27,
    0x28, 0x28, 0x29, 0x29, 0x2a, 0x2a, 0x2b, 0x2b, 0x2c, 0x2c, 0x2d, 0x2d, 0x2e, 0x2e, 0x2f, 0x2f,
    0x30, 0x30, 0x31, 0x31, 0x32, 0x32, 0x33, 0x33, 0x34, 0x34, 0x35, 0x35, 0x36, 0x36, 0x37, 0x37,
    0x38, 0x38, 0x39, 0x39, 0x3a, 0x3a, 0x3b, 0x3b, 0x3c, 0x3c, 0x3d, 0x3d, 0x3e, 0x3e, 0x3f, 0x3f,
    0x40, 0x40, 0x41, 0x41, 0x42, 0x42, 0x43, 0x43, 0x44, 0x44, 0x45, 0x45, 0x46, 0x46, 0x47, 0x47,
    0x48, 0x48, 0x49, 0x49, 0x4a, 0x4a, 0x4b, 0x4b, 0x4c, 0x4c, 0x4d, 0x4d, 0x4e, 0x4e, 0x4f, 0x4f,
    0x50, 0x50, 0x51, 0x51, 0x52, 0x52, 0x53, 0x53, 0x54, 0x54, 0x55, 0x55, 0x56, 0x56, 0x57, 0x57,
    0x58, 0x58, 0x59, 0x59, 0x5a, 0x5a, 0x5b, 0x5b, 0x5c, 0x5c, 0x5d, 0x5d, 0x5e, 0x5e, 0x5f, 0x5f,
    0x60, 0x60, 0x61, 0x61, 0x62, 0x62, 0x63, 0x63, 0x64, 0x64, 0x65, 0x65, 0x66, 0x66, 0x67, 0x67,
```

```
    0x68, 0x68, 0x69, 0x69, 0x6a, 0x6a, 0x6b, 0x6b, 0x6c, 0x6c, 0x6d, 0x6d, 0x6e, 0x6e, 0x6f, 0x6f,
    0x70, 0x70, 0x71, 0x71, 0x72, 0x72, 0x73, 0x73, 0x74, 0x74, 0x75, 0x75, 0x76, 0x76, 0x77, 0x77,
    0x78, 0x78, 0x79, 0x79, 0x7a, 0x7a, 0x7b, 0x7b, 0x7c, 0x7c, 0x7d, 0x7d, 0x7e, 0x7e, 0x7f, 0x7f };
uint8_t SBox_16 = {
    0x80, 0x80, 0x81, 0x81, 0x82, 0x82, 0x83, 0x83, 0x84, 0x84, 0x85, 0x85, 0x86, 0x86, 0x87, 0x87,
    0x88, 0x88, 0x89, 0x89, 0x8a, 0x8a, 0x8b, 0x8b, 0x8c, 0x8c, 0x8d, 0x8d, 0x8e, 0x8e, 0x8f, 0x8f,
    0x90, 0x90, 0x91, 0x91, 0x92, 0x92, 0x93, 0x93, 0x94, 0x94, 0x95, 0x95, 0x96, 0x96, 0x97, 0x97,
    0x98, 0x98, 0x99, 0x99, 0x9a, 0x9a, 0x9b, 0x9b, 0x9c, 0x9c, 0x9d, 0x9d, 0x9e, 0x9e, 0x9f, 0x9f,
    0xa0, 0xa0, 0xa1, 0xa1, 0xa2, 0xa2, 0xa3, 0xa3, 0xa4, 0xa4, 0xa5, 0xa5, 0xa6, 0xa6, 0xa7, 0xa7,
    0xa8, 0xa8, 0xa9, 0xa9, 0xaa, 0xaa, 0xab, 0xab, 0xac, 0xac, 0xad, 0xad, 0xae, 0xae, 0xaf, 0xaf,
    0xb0, 0xb0, 0xb1, 0xb1, 0xb2, 0xb2, 0xb3, 0xb3, 0xb4, 0xb4, 0xb5, 0xb5, 0xb6, 0xb6, 0xb7, 0xb7,
    0xb8, 0xb8, 0xb9, 0xb9, 0xba, 0xba, 0xbb, 0xbb, 0xbc, 0xbc, 0xbd, 0xbd, 0xbe, 0xbe, 0xbf, 0xbf,
    0xc0, 0xc0, 0xc1, 0xc1, 0xc2, 0xc2, 0xc3, 0xc3, 0xc4, 0xc4, 0xc5, 0xc5, 0xc6, 0xc6, 0xc7, 0xc7,
    0xc8, 0xc8, 0xc9, 0xc9, 0xca, 0xca, 0xcb, 0xcb, 0xcc, 0xcc, 0xcd, 0xcd, 0xce, 0xce, 0xcf, 0xcf,
    0xd0, 0xd0, 0xd1, 0xd1, 0xd2, 0xd2, 0xd3, 0xd3, 0xd4, 0xd4, 0xd5, 0xd5, 0xd6, 0xd6, 0xd7, 0xd7,
    0xd8, 0xd8, 0xd9, 0xd9, 0xda, 0xda, 0xdb, 0xdb, 0xdc, 0xdc, 0xdd, 0xdd, 0xde, 0xde, 0xdf, 0xdf,
    0xe0, 0xe0, 0xe1, 0xe1, 0xe2, 0xe2, 0xe3, 0xe3, 0xe4, 0xe4, 0xe5, 0xe5, 0xe6, 0xe6, 0xe7, 0xe7,
    0xe8, 0xe8, 0xe9, 0xe9, 0xea, 0xea, 0xeb, 0xeb, 0xec, 0xec, 0xed, 0xed, 0xee, 0xee, 0xef, 0xef,
    0xf0, 0xf0, 0xf1, 0xf1, 0xf2, 0xf2, 0xf3, 0xf3, 0xf4, 0xf4, 0xf5, 0xf5, 0xf6, 0xf6, 0xf7, 0xf7,
    0xf8, 0xf8, 0xf9, 0xf9, 0xfa, 0xfa, 0xfb, 0xfb, 0xfc, 0xfc, 0xfd, 0xfd, 0xfe, 0xfe, 0xff, 0xff };
```

you should obtain the following outputs on a cipher operation (all values in hexadecimal):

Input bytes (LSB on the left)								Output bytes (LSB on the left)							
01	00	00	00	00	00	00	00	3c	58	2b	44	04	4b	5f	1c
00	01	00	00	00	00	00	00	3d	55	20	41	06	4e	69	64
00	00	01	00	00	00	00	00	3d	59	2b	47	05	45	58	19
00	00	00	01	00	00	00	00	3c	5b	21	43	07	4c	6c	63
00	00	00	00	01	00	00	00	3a	53	19	48	0c	6a	60	7c
00	00	00	00	00	01	00	00	3f	15	18	62	1d	0c	7f	62
00	00	00	00	00	00	01	00	3e	28	12	7e	12	7a	63	7c
00	00	00	00	00	00	00	01	02	6d	16	4b	0d	6a	26	6c

6 References

- *Data Encryption Standard*, `https://en.wikipedia.org/wiki/Data_Encryption_Standard`
- *Feistel Cipher*, `https://en.wikipedia.org/wiki/Feistel_cipher`