

Changelog

• v1.0 - Initial version.

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.

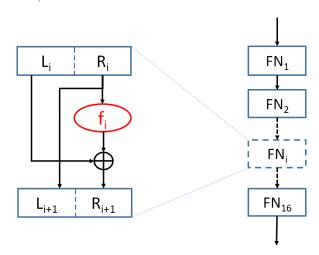


Figure 1: Overview o E-DES, with 16 Feistel Networks. Each f_i function is implemented by a different S-Box. Unlike DES, there is no initial and final bit permutations.

The (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). Each S-Box will have 256 unique bytes, which 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:

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

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];
int index = in[0];
out[3] = sbox[index];
index = (index + in[1]) % 256;
out[2] = sbox[index];
index = (index + in[2]) % 256;
out[1] = sbox[index];
index = (index + in[3]) % 256;
out[0] = 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, <code>speed</code>, 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 <code>/dev/urandom</code> 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 <code>clock_gettime</code> 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
         0 \times 01,
                       0 \times \overline{0}2 ,
                                     0 \times 0.3
                                                    0 \times 04,
                                                                  0 \times 0.5
                                                                                0 \times 06.
                                                                                               0 \times 07 .
                                                                                                             0 \times 08,
                                                                                                                           0 \times 09.
                                                                                                                                          0 \times 0 a,
                                                                                                                                                        0x0b,
                                                                                                                                                                      0x0c,
                                                                                                                                                                                     0 \times 0 d.
                                                                                                                                                                                                   0 \times 0 e
                                                    0 x 14,
                                                                                 0 \times 16
                                                                                                             0x18,
                                                                                                                            0x19,
                                                                                                                                          0 x 1 a ,
                                                                                                                                                        0 x 1 b ,
                                                                                                                                                                                                   0 \times 1 e
         0 x 21.
                       0 \times 22
                                     0 \times 23
                                                   0 x 24.
                                                                  0 \times 25
                                                                                0 \times 26
                                                                                               0 \times 27
                                                                                                             0 \times 28
                                                                                                                           0x29.
                                                                                                                                          0 x 2 a .
                                                                                                                                                        0 x 2 b .
                                                                                                                                                                       0 \times 2 c
                                                                                                                                                                                     0x2d.
                                                                                                                                                                                                   0 x 2 e
                                                                                                                                                                                                                 0 \times 2 f
                                                                                                                                                                                                                                0 \times 30
                                                                                 0 \times 36
                                                                                                             0 \times 38
                                                                                                                            0 \times 39
                                                                                                                                                        0 x 3 b ,
                                                                                                                                          0 \times 3 a
         0 \times 41 .
                       0 \times 42
                                     0 \times 43
                                                    0 \times 44 .
                                                                  0 \times 45
                                                                                0 \times 46
                                                                                               0 \times 47
                                                                                                             0 \times 48
                                                                                                                           0 \times 49.
                                                                                                                                          0 x 4 a .
                                                                                                                                                        0 \times 4 b.
                                                                                                                                                                       0 \times 4 c
                                                                                                                                                                                     0 x 4 d .
                                                                                                                                                                                                   0 \times 4 e
                                                                                                                                                                                                                                0 \times 50
                                                                                                                           0 x 59,
                                                                                                                                                        0x5b,
                                                                                                                                                        0x6b,
         0 \times 61
                       0 \times 62
                                     0 \times 63
                                                    0 \times 64
                                                                  0 \times 65
                                                                                0 \times 66
                                                                                               0 \times 67
                                                                                                             0 \times 68
                                                                                                                           0 \times 69
                                                                                                                                          0 \times 6 a
                                                                                                                                                                       0 \times 6 c
                                                                                                                                                                                     0x6d.
                                                                                                                                                                                                   0 \times 6 e
                                                                                                                                                                                                                 0 \times 6 f
                                                    0 x 7 4
                                                                                                             0 x 7 8
                                                                                                                           0 x 7 9
         0 \times 81
                       0 \times 82
                                     0 \times 83
                                                    0 \times 84
                                                                  0x85
                                                                                0 \times 86
                                                                                               0 \times 87
                                                                                                             0 \times 88
                                                                                                                           0x89.
                                                                                                                                          0x8a
                                                                                                                                                        0x8b.
                                                                                                                                                                      0 \times 8c
                                                                                                                                                                                     0x8d.
                                                                                                                                                                                                   0 x 8 e
                                                                                                                                                                                                                 0 x 8 f
                                                                                                                                                                                                                                0 \times 90
         0 x 9 1
                       0 \times 92
                                     0 \times 93
                                                    0 \times 94
                                                                  0 \times 95
                                                                                0 \times 96
                                                                                                0 \times 97
                                                                                                             0 \times 98
                                                                                                                           0 \times 99
                                                                                                                                          0 \times 9 a
                                                                                                                                                        0х9ь,
                                                                                                                                                                       0х9с
                                                                                                                                                                                     0 x 9 d ,
                                                                                                                                                                                                   0 \times 9 e
                                                                                                                                                                                                                  0 \times 9 f
         0 \times a1
                       0 \times a2
                                     0 \times a 3
                                                   0 xa4
                                                                  0 \times a5
                                                                                0 \times a6
                                                                                               0 \times a 7
                                                                                                             0xa8,
                                                                                                                           0 \times a9,
                                                                                                                                          0 \, \mathrm{xaa}
                                                                                                                                                        0 xab,
                                                                                                                                                                      0 \, \mathrm{xac}
                                                                                                                                                                                     0 xad,
                                                                                                                                                                                                   0 \, \mathrm{xae}
                                                                                                                                                                                                                 0 \times a f
                                                                                                                                                                                                                                0 \times b0
                                                                  0 x b 5
                       0 \times b2
                                     0 \times b3
                                                                                                             0 x b 8
                                                                                                                                                        0xbb,
         0 \times c1
                       0 \times c2
                                     0 \times c3
                                                   0 \times c4
                                                                  0 \times c5
                                                                                0 \times c6
                                                                                               0 \times c7
                                                                                                             0 \times c 8
                                                                                                                           0 \times c9
                                                                                                                                          0 \times ca
                                                                                                                                                        0xcb.
                                                                                                                                                                      0 хсс
                                                                                                                                                                                     0xcd.
                                                                                                                                                                                                   0xce.
                                                                                                                                                                                                                 0 \times cf
                                                                                                                                                                                                                                0 \times d0
                       0 \times d2
                                     0 \times d3,
                                                    0xd4 ,
                                                                  0 \; x \, d \, 5
                                                                                0\,x\,d\,6
                                                                                               0 \times d7
                                                                                                             0 \times d8
                                                                                                                           0 \times d9,
                                                                                                                                                        0 \times db,
                                                                                                                                                                      0 \times dc ,
                                                                                                                                                                                     0xdd,
                                                                                                                                                                                                   0 \times de,
                       0 x e 2
                                     0 \times e3
                                                   0 \times e4,
                                                                  0 \times e5
                                                                                0 \times e 6
                                                                                                             0 xe8,
                                                                                                                           0 xe9,
                                                                                                                                          0 xea,
                                                                                                                                                        0 xeb,
                                                                                                                                                                      0 xec
                                                                                                                                                                                     0 xed,
                                                                                                                                                                                                   0 xee,
         0 \times f1
                       0 \times f2
                                     0 \times f3
                                                   0 \times f4
                                                                  0 \times f5
                                                                                0 \times f6
                                                                                               0 \times f7
                                                                                                             0 \times f8
                                                                                                                           0 \times f9
                                                                                                                                                        0xfb,
                                                                                                                                                                      0 \ \mathrm{x} \, \mathrm{fc}
                                                                                                                                                                                     0 \times fd,
                                                                                                                                                                                                   0 \times fe
                                                                                                                                                                                                                 0 \times ff
                                                                                                                                                                                                                               0 \times 00
                                                                                                                                          0xfa,
                 SBox 02
                                                                                                                                                                                     0 \ge 0 \, \mathrm{e} ,
                                                                                                                                          0 \times 0 b,
                                                                                                                                                                                                   0 \times 0 f,
         0 \times 0.2
                       0 \times \overline{0}3
                                     0 \times 04
                                                    0 \times 05,
                                                                  0 \times 06,
                                                                                0 \ge 0.7
                                                                                               0 \times 08,
                                                                                                             0 \times 09,
                                                                                                                           0\,\mathrm{x}\,0\,\mathrm{a} ,
                                                                                                                                                        0 \times 0 \, \mathrm{c} ,
                                                                                                                                                                      0 \times 0 d
                       0 \times 13
                                     0 \times 14
                                                                                                             0x19,
         0 \times 12
                                                    0 \times 15
                                                                  0 \times 16
                                                                                0 \times 17
                                                                                               0 \times 18
                                                                                                                           0x1a,
                                                                                                                                          0x1b,
                                                                                                                                                        0 x 1 c ,
                                                                                                                                                                      0 \times 1 d
                                                                                                                                                                                     0x1e,
                                                                                                                                                                                                   0 \times 1 f
                                                                                                                                                        0 x 2 c ,
         0 \times 22
                       0 \times 23
                                     0 \times 24
                                                   0 \times 25
                                                                  0 \times 26
                                                                                0 \times 27
                                                                                               0 \times 28
                                                                                                             0 \times 29
                                                                                                                           0 \times 2 a
                                                                                                                                          0 \times 2b
                                                                                                                                                                      0 \times 2 d
                                                                                                                                                                                     0 x 2 e ,
                                                                                                                                                                                                   0 \times 2 f
                                                                                                                                                                                                                 0 \times 30
                                                                                                                                                                                                                                0 \times 31
                                                    0 \times 35
                                                                  0 \times 36
                                                                                0 \times 37
                                                                                                             0 x 39,
                                                                                                                                          0x3b,
         0 \times 32
                       0 \times 33
                                     0 \times 34
                                                                                               0 \times 38
                                                                                                                           0 x 3a,
                                                                                                                                                        0 x 3 c ,
                                                                                                                                                                      0 \times 3 d
                                                                                                                                                                                     0 \times 3e,
                                                                                                                                                                                                   0 \times 3 f
                                                                                                                                                                                                                                0 \times 41
                                                                                                                                                                                                                  0 \times 40
                                                                                                                                                                                     0 x 4 e ,
         0 \times 42
                       0 \times 43
                                                                                               0 \times 48
                                                                                                                                                        0х4с,
                                     0 \times 44
                                                    0 \times 45
                                                                  0 \times 46
                                                                                0 \times 47
                                                                                                             0 \times 49
                                                                                                                           0 x 4 a ,
                                                                                                                                          0 \times 4 b
                                                                                                                                                                       0 \times 4 d
                                                                                                                                                                                                   0 \times 4 f
                       0 x 5 3 ,
         0 \times 52 ,
                                     0 x 54,
                                                                                0 \times 57
                                                                                                             0 \times 59,
                                                    0 \times 55
                                                                  0 \times 56,
                                                                                               0x58,
                                                                                                                           0 x 5 a ,
                                                                                                                                          0x5b,
                                                                                                                                                        0 x 5 c ,
                                                                                                                                                                      0 x 5 d,
                                                                                                                                                                                     0 x 5 e ,
                                                                                                                                                                                                   0 \times 5 f
                                                                                                                                                                                                                  0 \times 60,
                       \begin{array}{c} 0 \times 63 \\ 0 \times 73 \end{array}
                                     0 \times 64 \\ 0 \times 74
                                                                  0 x 6 6
0 x 7 6
                                                                                \begin{array}{c} 0 \times 67 \\ 0 \times 77 \end{array}
                                                                                                             0 \times 69,
0 \times 79,
                                                                                                                           0 x 6 a ,
0 x 7 a ,
                                                                                                                                          \begin{array}{c} 0 \ x \, 6 \, b \\ 0 \ x \, 7 \, b \end{array}
                                                                                                                                                        \begin{array}{c} 0 \, x \, 6 \, c \; , \\ 0 \, x \, 7 \, c \; , \end{array}
                                                                                                                                                                      0x6d,
0x7d,
                                                                                                                                                                                     0 x 6 e ,
0 x 7 e ,
         0 \times 62
                                                    0 \times 65
                                                                                               0 \times 68
                                                                                                                                                                                                   0 \times 6 f
                                                    0 x 7 5
         0x82,
                                                                                                                                                        0 x 8 c ,
                       0x83.
                                     0 \times 84
                                                    0 \times 85
                                                                  0 \times 86
                                                                                0 \times 87
                                                                                               0 \times 88
                                                                                                             0 \times 89
                                                                                                                           0 x 8a.
                                                                                                                                          0x8b.
                                                                                                                                                                       0x8d
                                                                                                                                                                                     0x8e,
                                                                                                                                                                                                   0 \times 8 f
                                                                                                                                                                                                                  0 \times 90
                                                                                                                                                                                                                                0 \times 91
                                                    0 x 9 5
                                                                  0 \times 96
                                                                                                             0x99,
         0x92,
                       0 \times 93
                                     0 \times 94
                                                                                0 \times 97
                                                                                               0 \times 98
                                                                                                                           0 x 9 a ,
                                                                                                                                          0x9b,
                                                                                                                                                        0 x 9 c ,
                                                                                                                                                                       0 x 9 d ,
                                                                                                                                                                                     0 x 9 e ,
                                                                                                                                                                                                   0 \times 9 f
                                                                                                                                                                                                                  0 \times a 0
         0 \times a.2
                       0 \times a.3
                                     0 \times a 4
                                                    0 \times a.5
                                                                  0 \times a6
                                                                                0 \times a.7
                                                                                               0 \times a.8
                                                                                                             0 x a 9 ,
0 x b 9 ,
                                                                                                                           0 \, \mathrm{xaa}
                                                                                                                                          0 \times ab
                                                                                                                                                        0 xac,
                                                                                                                                                                       0 xad
                                                                                                                                                                                     0 xae
                                                                                                                                                                                                                  0 \times b0
                                                                                                                                                                                                                                0 \times b1
                       0 \times b3
                                                                  0 x b 6
                                                                                                                           0 \, \mathrm{xba} ,
                                     0 \times b4
                                                    0 \times b = 5
                                                                                0 \times b 7
                                                                                               0 \times b 8
                                                                                                                                          0xbb,
                                                                                                                                                        0xbc,
                                                                                                                                                                       0xbd,
                                                                                                                                                                                     0 \times be,
                                                                                                                                                                                                   0 \times b f
                                                                                                                                                        0xcc,
         0 \times c2
                       0 \times c3
                                     0 \times c4
                                                    0 \times c5
                                                                  0 \times c6
                                                                                0 \times c7
                                                                                               0 \times c 8
                                                                                                             0 \times c9
                                                                                                                           0 xca.
                                                                                                                                          0 \times cb
                                                                                                                                                                      0 \times cd
                                                                                                                                                                                     0xce.
                                                                                                                                                                                                   0 \times cf
                                                                                                                                                                                                                 0 \times d0
         0 \times d2
                       0 \times d3,
                                     0 x d4,
                                                    0 \times d5
                                                                  0 \times d6,
                                                                                0\,x\,d\,7
                                                                                               0 \times d 8
                                                                                                             0 x d9 ,
                                                                                                                           0\,\mathrm{xd}\,\mathrm{a} ,
                                                                                                                                          0xdb,
                                                                                                                                                        0\;x\,d\,c\ ,
                                                                                                                                                                      0xdd,
                                                                                                                                                                                     0xde,
                                                                                                                                                                                                   0xdf,
                                                                                                                                                                                                                 0 \; x \, e \, 0
                       0 \text{ xe} 3
                                     0 \times e4
                                                    0 \times e5
                                                                  0 \times e6
                                                                                                             0 \times e9
                                                                                                                                          0 \times eb
                                                                                                                                                                       0 \times ed
                       0 x f3
                                                                  0 x f6,
                                                                                               0 x f8
                                                                                                             0 x f9 ,
                                                                                                                                          0xfb,
                                                                                                                                                        0 x fc ,
                                                                                                                           0 x fa,
                SBox_03
         0 x 0 3 ,
         0 x 13.
                       0 x 14
                                     0 \times 15
                                                   0 x 16.
                                                                  0 \times 17
                                                                                0 \times 18
                                                                                               0x19.
                                                                                                             0x1a.
                                                                                                                           0 x 1b.
                                                                                                                                          0 x 1 c,
                                                                                                                                                        0 x 1 d ,
                                                                                                                                                                      0 x 1 e .
                                                                                                                                                                                     0 x 1 f.
                                                                                                                                                                                                   0x20.
                                                                                                                                                                                                                 0 \times 21
                                                                                                                                                                                                                               0 \times 22
                                                                                                                                                        0 x 2 d ,
                                                                                                             0 \times 2 a ,
                                                                                                                            0 \times 2b,
         0 \times 33.
                       0 \times 34.
                                     0 \times 35
                                                    0 \times 36
                                                                  0 \times 37
                                                                                0 \times 38
                                                                                               0 \times 39
                                                                                                             0 x 3 a .
                                                                                                                           0 \times 3b.
                                                                                                                                          0 \times 3 c
                                                                                                                                                        0 \times 3 d.
                                                                                                                                                                       0 \times 3 e
                                                                                                                                                                                     0 \times 3 f
                                                                                                                                                                                                   0 \times 40
                                                                                                                                                                                                                  0 \times 41
                                                                                                                                                                                                                                0 \times 42
                                     0 x 4 5
                                                                                                                           0 x 4 b ,
                                                                                                                                                        0 x 4 d ,
                                                                                 0 \times 48
                                                                                                             0х4а,
         0 \times 53 .
                       0 \times 54
                                     0 \times 55
                                                    0 \times 56
                                                                  0 \times 57
                                                                                0 \times 58
                                                                                               0 \times 59
                                                                                                             0 \times 5 a
                                                                                                                           0x5b,
                                                                                                                                          0 \times 5 c
                                                                                                                                                        0 \times 5 d.
                                                                                                                                                                       0 x 5 e
                                                                                                                                                                                     0 \times 5 f
                                                                                                                                                                                                   0 \times 60
                                                                                                                                                                                                                 0 \times 61
                                                                                                                                                                                                                                0 \times 62
         0 x 7 3 .
                       0 \times 74
                                     0 \times 75
                                                    0 \times 76
                                                                  0 \times 77
                                                                                0 \times 78
                                                                                               0x79.
                                                                                                             0 x 7 a .
                                                                                                                           0x7b.
                                                                                                                                          0 \times 7 c
                                                                                                                                                        0 x 7 d.
                                                                                                                                                                       0 x 7 e
                                                                                                                                                                                     0 \times 7 f
                                                                                                                                                                                                   0 \times 80
                                                                                                                                                                                                                 0 \times 81
                                                                                0 \ge 88
                                                                                                                           0 x8b ,
                                                                                                                                                        0 x 8 d ,
                                                                                                                                                                                                   0 \times 90
                                                                                                                                                                                                                  0 x 9 1
         0x93,
                       0 \times 94
                                     0 \times 95
                                                    0 \times 96
                                                                  0 \times 97
                                                                                0 \times 98
                                                                                               0x99,
                                                                                                             0 x 9 a ,
                                                                                                                           0x9b,
                                                                                                                                          0 x 9 c
                                                                                                                                                        0x9d,
                                                                                                                                                                       0 x 9 e ,
                                                                                                                                                                                     0 \times 9 f
                                                                                                                                                                                                   0 \times a 0
                                                                                                                                                                                                                 0 \times a1
                                                                                                                                                                                                                                0 \times a2
         0xb3.
                       0 \times b4
                                     0 \times b5
                                                    0 \times b = 6
                                                                  0 \times b7
                                                                                0xb8
                                                                                               0xb9
                                                                                                             0xba.
                                                                                                                           0xbb.
                                                                                                                                          0 \times bc
                                                                                                                                                        0xbd.
                                                                                                                                                                      0xbe.
                                                                                                                                                                                     0 \times b f
                                                                                                                                                                                                   0 \times c0
                                                                                                                                                                                                                 0 \times c1
                                                                                                                                                                                                                                0 \times c2
                                                                                                                                                                                                   0\,x\,d\,0
         0xd3,
                       0 \times d4
                                     0 \times d5
                                                   0 \times d6,
                                                                  0 \times d7
                                                                                0xd8,
                                                                                               0xd9,
                                                                                                             0xda,
                                                                                                                           0xdb,
                                                                                                                                          0xdc,
                                                                                                                                                        0xdd,
                                                                                                                                                                      0xde,
                                                                                                                                                                                     0xdf,
                                                                                                                                                                                                   0 \times e0,
                                                                                                                                                                                                                 0 \times e1
                                                                                                                                                                                                                                0 \times e2
                       0 \times e 4
                                     0 \ge 5
                                                                  0 \ge 7
                                                                                               0 x e 9
                                                                                                                           0\;x\,e\,b
                                                                                                                                                        0 xed,
                                                                                                                                                                      Охее
                                                                                                                                                                                                   0 \times f0
         0 \times f3
                       0 \times f4
                                     0 \times f5
                                                   0 x f6,
                                                                  0 \times f7,
                                                                                0xf8
                                                                                               0 \times f9,
                                                                                                             0xfa,
                                                                                                                           0xfb,
                                                                                                                                          0xfc,
                                                                                                                                                        0xfd,
                                                                                                                                                                     0 \times fe
                                                                                                                                                                                     0 \times ff,
                                                                                                                                                                                                   0 \times 00,
                                                                                                                                                                                                                 0 \times 01
                                                                                                                                                                                                                               0 \times 02
                 SBox_0
1, 0x05
                              04
         0 x 0 4 ,
                                     0x06,
                                                    0x07,
                                                                  0x08,
                                                                                0 \times 09
                                                                                                             0x0b,
                                                                                                                                                                                     0x10,
                                                                                               0x0a.
                                                                                                                           0х0с.
                                                                                                                                          0x0d.
                                                                                                                                                        0x0e, 0x0f
                                                                                                                                                                                                   0 \times 11
                                                                                                                                                                                                                 0 \times 12
         0 x 14,
                       0 \times 15
                                     0 \ge 16
                                                    0 \times 17
                                                                  0 \times 18
                                                                                0 \times 19
                                                                                               0x1a,
                                                                                                             0x1b,
                                                                                                                           0 \times 1 c
                                                                                                                                          0 \times 1 d
                                                                                                                                                        0 x 1 e ,
                                                                                                                                                                      0~\mathrm{x}\,1\,\mathrm{f}
                                                                                                                                                                                     0 \times 20
                                                                                                                                                                                                   0 \times 21
                                                                                                                                                                                                                 0 \times 22
         0 x 24,
                                     0 \times 26
                                                   0 \times 27
                                                                  0 \times 28
                                                                                0 \times 29
                                                                                               0x2a,
                                                                                                             0x2b,
                                                                                                                                                        0 x 2 e ,
                                                                                                                                                                     0 \times 2 f
                                                                                                                                                                                     0 \times 30,
                                                                                                                                                                                                   0 \times 31
                                                                                                                                                                                                                 0 \times 32
                                                                                                                                                                                                                                0 \times 33
                       0 \times 25
                                                                                                                           0 x 2 c ,
                                                                                                                                          0 \times 2d
         0 x 3 4 ,
                                                                                                                                                        0 x 3 e ,
0 x 4 e ,
                       0 \times 35
                                     0 \times 36
                                                    0 \times 37
                                                                  0 \times 38
                                                                                0 \times 39
                                                                                               0 \times 3 a
                                                                                                             0 \times 3b,
                                                                                                                           0х3с,
                                                                                                                                          0 \times 3d
                                                                                                                                                                      0 \times 3 f
                                                                                                                                                                                     0 \times 40
                                                                                                                                                                                                   0 \times 41
         0 x 44,
                       0 x 4 5
                                     0 x 46
                                                                                0 \times 49
                                                                                                             0 x 4b ,
                                                                                                                           0 x 4 c ,
                                                                                                                                          0 x 4d,
                                                                                                                                                                      0 \times 4 f
                                                                                                                                                                                     0 \times 50,
                                                                                                                                                                                                   0 \times 51
                                                    0 \times 47
                                                                  0 \times 48
                                                                                               0 x 4a,
                                                                                                                                                                                                                  0 \times 52
                                                                                               0 x 5 a
         0 \ge 54
                       0 \times 55
                                     0 \ge 56
                                                    0 \times 57
                                                                  0 \ge 58
                                                                                0 \ge 59
                                                                                                             0x5b,
                                                                                                                           0 \ge 5 \ c
                                                                                                                                          0 \times 5 d
                                                                                                                                                        0 x 5 e ,
0 x 6 e ,
                                                                                                                                                                      0 \times 5 f
                                                                                                                                                                                     \begin{array}{c} 0 \times 60 \\ 0 \times 70 \end{array}
                                                                                                                                                                                                   0 \times 61 \\ 0 \times 71
                                                                                                                                                                                                                  0 \times 62
                                                                                                                                                                                                                                0 \times 63
                       0 \times 65
                                     0 x 6 6
                                                    0 x 6 7
                                                                  0 x 68
                                                                                0 x 69
                                                                                                             0x6b,
                                                                                                                           0~{\rm x}\,6~{\rm c}
                                                                                                                                                                      0 \times 6 f
         0 \times 64 ,
                                                                                               0x6a,
                                                                                                                                          0 \times 6 d
                                                                                               0x7a,
         0 \times 74,
                       0 \times 75
                                     0 \times 76
                                                    0 \times 77
                                                                  0 \times 78
                                                                                0 \times 79
                                                                                                             0\,\mathrm{x}\,7\,\mathrm{b} ,
                                                                                                                           0 \times 7 c
                                                                                                                                          0 \times 7 d
                                                                                                                                                        0 \ge 7\,\mathrm{e} ,
                                                                                                                                                                      0 \ge 7 \, \mathrm{f}
                                                                                                                                                                                     0 \times 80
                                                                                                                                                                                                   0 \times 81
                                                                                                                                                                                                                  0x82
                                                                                0 \times 89
                                                                                                             0x8b,
                                                    0 \times 87
                                                                                                                                          0x8d,
                                                                                                                                                                      0 x 8 f
                                                                                                                                                                                     0x90,
                                                                                                                                                                                                   0 \times 91
                                                                                                                                                                                                                                0 \times 93
         0x84,
                       0 \times 85
                                     0 \times 86
                                                                  0x88
                                                                                               0x8a,
                                                                                                                           0 x 8 c
                                                                                                                                                        0 x 8e,
                                                                                                                                                                                                                  0 \times 92
         0x94,
                       0 \times 95
                                     0 \times 96
                                                    0 \times 97
                                                                  0 \times 98
                                                                                0 \times 99
                                                                                               0 x 9 a
                                                                                                             0 x 9 b
                                                                                                                           0 \times 9 c
                                                                                                                                          0 \times 9 d
                                                                                                                                                        0х9е,
                                                                                                                                                                      0 \times 9 f
                                                                                                                                                                                     0 \times a0
                                                                                                                                                                                                   0 \times a.1
                                                                                                                                                                                                                  0 \times a 2
                       0 x a 5
                                                                  0 x a 8
                                                                                                                           0\,x\,a\,c
                                                                                                                                          0 \, \mathrm{xad}
                                                                                                                                                                                                   0 \times b 1
         0 \times a4,
                                     0xa6
                                                                                 0 \times a9
                                                                                                             0xab,
                                                                                                                                                        0 xae,
                                                                                                                                                                      0 \times af
                                                                                                                                                                                     0xb0,
                                                    0xa7
                                                                                               0 xaa,
                                                                                                                                                                                                                  0 \times b2
         0xb4.
                       0 \times b5
                                     0 \times b6
                                                    0 \times b7
                                                                  0 \times b 8
                                                                                0xb9
                                                                                               0xba.
                                                                                                             0xbb.
                                                                                                                           0 \times bc
                                                                                                                                          0xbd.
                                                                                                                                                        0 \times be,
                                                                                                                                                                      0 \times bf
                                                                                                                                                                                     0xc0.
                                                                                                                                                                                                   0 \times c1
                                                                                                                                                                                                                  0 \times c2
                                                                                                                                                                                                                                0 \times c3
         0 x c 4 ,
                       0 \times c5
                                     0 \ge c 6
                                                    0 x c 7
                                                                  0 \ge 0.8
                                                                                0 \ge 0
                                                                                               0 x ca ,
                                                                                                             0xcb,
                                                                                                                           0\,\mathrm{x\,c\,c} ,
                                                                                                                                          0 xcd,
                                                                                                                                                        0 \times ce ,
                                                                                                                                                                     0 x c f ,
                                                                                                                                                                                     0 \times d0,
                                                                                                                                                                                                   0 \times d1
                                                                                                                                                                                                                 0 \times d2
                                                                                                                                                                                                                                0 \times d3
                                                                                                                                                        0xde,
         0 \times d4
                       0 \times d5
                                     0 \times d6
                                                    0 \times d7
                                                                  0 \times d8
                                                                                0 \times d9
                                                                                               0 x d a
                                                                                                             0xdb.
                                                                                                                           0 \times dc
                                                                                                                                          0 xdd
                                                                                                                                                                      0 \times df
                                                                                                                                                                                     0 \times e0
                                                                                                             0 xeb,
                                      0 \times e 6
                                                                                               0 xea,
                                                                                                                           Охес
                                                                                                                                          0 \times ed
                                                                                                                                                        0 xee,
                  , 0xf5
SBox_0
                                                                                                                                                       0 \ \mathrm{xfe} ,
         0 \ge f4
                                     0 \times f6
                                                   0 \times f7
                                                                  0 x f8,
                                                                                0 \times f9,
                                                                                               0xfa,
                                                                                                             0xfb,
                                                                                                                           0 \times fc
                                                                                                                                          0xfd,
                                                                                                                                                                     0 \times ff
                                                                                                                                                                                     0 \times 00,
                                                                                                                                                                                                   0 \times 01,
                                                                                                                                                                                                                 0 \times 02
                                                                                                                                                                                                                               0 \times 03
         0 \times 05,
                       0 \times 06
                                                    0x08.
                                                                                                                                                        0 x 0 f .
                                     0 \times 07
                                                                  0x09.
                                                                                0 x 0a.
                                                                                               0x0b.
                                                                                                             0x0c.
                                                                                                                           0x0d.
                                                                                                                                          0 x 0 e .
                                                                                                                                                                      0 x 10.
                                                                                                                                                                                     0x11.
                                                                                                                                                                                                   0 x 12.
                                                                                                                                                                                                                                0 x 14.
                                                                                                                                                                                                                 0 \times 13 .
                                      0 \times 17
                                                    0 \times 18
                                                                  0 \ge 19
                                                                                 0 \times 1a,
                                                                                               0 \times 1 \, \mathrm{b}
                                                                                                             0 x 1 c ,
                                                                                                                           0 x 1 d ,
                                                                                                                                          0 x 1 e ,
                                                                                                                                                        0 \times 1 f,
                                                                                                                                                                      0 \times 20,
                                                                                                                                                                                     0 \ge 21
                                                                                                                                                                                                   0 \ge 2 \ 2
         0 \times 25 .
                       0 \times 26
                                     0 \times 27
                                                    0 \times 28
                                                                  0 \times 29
                                                                                0 x 2a.
                                                                                               0 \times 2 b
                                                                                                             0 \times 2c.
                                                                                                                           0 \times 2d
                                                                                                                                          0 x 2 e .
                                                                                                                                                        0 \times 2f.
                                                                                                                                                                       0 \times 30
                                                                                                                                                                                     0 \times 31
                                                                                                                                                                                                   0 \times 32
                                                                                                                                                                                                                  0 \times 33
                                                                                                                                                                                                                                0 \times 34
         0 \times 45
                       0 \times 46
                                     0 \times 47
                                                    0 \times 48
                                                                  0 \times 49
                                                                                0 x 4a.
                                                                                               0 \times 4 b
                                                                                                             0 x 4 c .
                                                                                                                           0 \times 4 d
                                                                                                                                          0 x 4 e .
                                                                                                                                                        0 x 4 f .
                                                                                                                                                                       0 \times 50
                                                                                                                                                                                     0 \times 51
                                                                                                                                                                                                   0 \times 52
                                                                                                                                                                                                                 0 \times 53
                                                                                                                                                                                                                                0 \times 54
                                                                  0 \times 59
                                                                                                                           0 \times 5 d
                                                                                                0 x 5 b
         0x65.
                       0 \times 66
                                     0 \times 67
                                                    0 \times 68
                                                                  0 \times 69
                                                                                0x6a.
                                                                                               0x6b
                                                                                                             0 x 6 c
                                                                                                                           0 \times 6d
                                                                                                                                          0x6e.
                                                                                                                                                        0 x 6f.
                                                                                                                                                                       0 \times 70
                                                                                                                                                                                     0 \times 71
                                                                                                                                                                                                   0 \times 72
                                                                                                                                                                                                                 0 \times 73
                                                    0 x 7 8
                                                                                                             0х7с
                                                                                                                           0 \times 7 d
                                                                                                                                                        0 \times 7 f
         0 \times 85
                       0 \times 86
                                     0 \times 87
                                                    0x88
                                                                  0 \times 89
                                                                                0x8a,
                                                                                               0x8b
                                                                                                             0 x 8 c
                                                                                                                           0 x8d,
                                                                                                                                          0x8e,
                                                                                                                                                        0 x 8f,
                                                                                                                                                                       0 \times 90
                                                                                                                                                                                     0 \times 91
                                                                                                                                                                                                   0 \times 92
                                                                                                                                                                                                                 0 \times 93
                                                                                                                                                                                                                                0 \times 94
         0 x 9 5
                       0 x 9 6
                                     0 \times 97
                                                    0 x 9 8
                                                                  0 x 9 9
                                                                                                0 x 9 b
                                                                                                                           0 x 9 d
                                                                                                                                          0х9е,
         0 \times a5.
                       0xa6
                                     0 \times a7
                                                    0xa8
                                                                  0 \times a9
                                                                                0 x aa .
                                                                                               0xab
                                                                                                             0 \, \mathrm{xac}
                                                                                                                           0 xad .
                                                                                                                                          0 xae.
                                                                                                                                                        0 xaf.
                                                                                                                                                                       0 \times b = 0
                                                                                                                                                                                     0 \times b 1
                                                                                                                                                                                                   0xb2
                                                                                                                                                                                                                  0xb3.
                                     0 \times b7
                                                                                                                                                        0 \times b f,
                       0 \times b6
                                                    0 x b 8
                                                                  0 \times b 9
                                                                                 0xba,
                                                                                                             0xbc,
                                                                                                                           0xbd,
         0 \times c5
                       0 \times c6
                                     0 \times c7
                                                    0 \times c 8
                                                                  0 \times c9
                                                                                0xca,
                                                                                               0 \times cb
                                                                                                             0 хсс
                                                                                                                           0 xcd,
                                                                                                                                          Охсе
                                                                                                                                                        0xcf,
                                                                                                                                                                       0 \text{ x d } 0
                                                                                                                                                                                     0 \times d1
                                                                                                                                                                                                   0 \times d2
                                                                                                                                                                                                                 0xd3.
                                                                                                                                                                                                                                0 \times d4
         0 \times d5
                       0 \times d6
                                     0 \times d7
                                                    0 \times d8
                                                                  0 \times d9
                                                                                0 \times da,
                                                                                               0xdb
                                                                                                             0xdc,
                                                                                                                           0xdd,
                                                                                                                                          0xde,
                                                                                                                                                        0xdf,
                                                                                                                                                                                                                 0 \times e3
         0 \times e5,
                       0 \times e6
                                     0 \times e7
                                                    0 \times e 8
                                                                  0 \times e9
                                                                                0 xea,
                                                                                               0 \times eb
                                                                                                             0 xec,
                                                                                                                           0 xed,
                                                                                                                                          0 \, \mathrm{xee}
                                                                                                                                                        0 xef,
                                                                                                                                                                       0 \times f0
                                                                                                                                                                                     0 \times f1
                                                                                                                                                                                                   0 \times f2
                       0 \times f6
                                     0 \times f7
                                                    0 \times f8,
                                                                  0 \times f9,
                                                                                0 \times fa,
                                                                                               0 \times fb,
                                                                                                             0 \, x \, fc ,
                                                                                                                           0xfd,
                                                                                                                                          0xfe,
                                                                                                                                                        0 \times ff,
                                                                                                                                                                       0 \times 0 
                                                                                                                                                                                                   0 \times 02,
                                                                                                                                                                                                                 0 \times 03,
                                                                                                                                                                                                                               0\ge 0.4
                                                                                                                                                                                     0 \times 01,
                  SBox
                              06
         0 \times 06,
                       0 \times \overline{07},
                                                   0 \times 09
                                                                  0x0a.
                                                                                0x0b.
                                                                                               0х0с,
                                                                                                                           0х0е,
                                                                                                                                          0 x 0 f .
                                                                                                                                                        0x10.
                                                                                                                                                                                                   0x13.
                                     0 \times 0.8
                                                                                                             0 \times 0 d.
                                                                                                                                                                      0 \times 11
                                                                                                                                                                                     0 \times 12
                                                                                                                                                                                                                 0 \times 14
                       0 \times 17
                                     0x18,
                                                   0 x 19,
                                                                  0 \times 1 a,
                                                                                \begin{array}{c} 0 \, x \, 1 \, b \; , \\ 0 \, x \, 2 \, b \; , \end{array}
                                                                                                            0x1d, 0x1e,
0x2d, 0x2e,
0x3d, 0x3e,
                                                                                                                                                        0\,x\,2\,0\ ,\quad 0\,x\,2\,1\ ,
                                                                                                                                                                                     0 \times 22,
         0 x 16,
                                                                                              0 x 1 c ,
                                                                                                                                         0 \times 1 f,
                                                                                                                                                                                                   0 \times 23, 0 \times 24,
                                                                  0 x 2 a ,
                                                    0 \times 29
                                                                                               0 x 2 c
                                                                                                                                          0 \times 2f
                                                                                                                                                        0 \times 30 ,
                                                                                                                                                                      0 \times 31
                                                                                                                                                                                     0 \times 32
                                                                                                                                                                                                   0 \times 33,
                                                   0 \times 39,
                                                                                                                                         0x3f, 0x40, 0x41,
         0x36, 0x37,
                                     0 x 38,
                                                                 0 x 3 a ,
                                                                                0x3b,
                                                                                                                                                                                   0 x 42,
                                                                                              0 x 3 c
                                                                                                                                                                                                   0 \times 43, 0 \times 44,
```

```
0 \times 52,
                                                                                                                                                                                                0 \times 53,
        0 \times 46,
                      0 \times 47
0 \times 57
                                    0 \times 48
                                                   0 \times 49,
                                                                 0x4a ,
                                                                               0 x 4 b ,
                                                                                             0 \times 4c ,
                                                                                                           0 \times 4d, 0 \times 5d,
                                                                                                                          0x4e ,
                                                                                                                                        0 \times 4f,
                                                                                                                                                      0 \times 50,
                                                                                                                                                                    0 \ge 51
                                                                                                                                                                                                               0 \times 54
                                                                                                                                                                                                                             0 \times 55
                                                                                                                                        0 x 5 f ,
                                                   0 \times 59
                                                                 0 x 5 a ,
                                                                                                                                                                                   0 \times 62 ,
        0 \times 56,
                                    0 \times 58
                                                                               0x5b,
                                                                                             0 \times 5 c,
                                                                                                                          0 x 5 e,
                                                                                                                                                      0x60, 0x61,
                                                                                                                                                                                                 0 \times 63,
                                                                                                                                                                                                               0 \times 64.
                                                                                                                                                                                                                             0 \times 65
                                                                 0x6a,
                                                                                                                                                      0x70,
                                                                                                                                                                                                 0x73.
        0 \times 66,
                      0 \times 67
                                    0 \times 68
                                                   0 \times 69
                                                                               0x6b
                                                                                              0 x 6 c
                                                                                                            0x6d.
                                                                                                                          0х6е,
                                                                                                                                        0 \times 6 f
                                                                                                                                                                    0 \times 71
                                                                                                                                                                                   0 \times 72
                                                                                                                                                                                                               0 \times 74
                                                                                                                                                                                                                             0 \times 7.5
                                                                                                                                        0 x 7 f
                      0 \times 77
                                                                 0 \times 7 a,
                                                                                0х7ь,
                                                                                                                          0 \times 7 e,
                                                                                                                                                                                   0 x 82 .
                                                                                                                                                                                                 0x83.
         0x76,
                                     0 \times 78
                                                   0 \times 79
                                                                                                            0x7d,
                                                                                                                                                       0x80,
                                                                                                                                                                                                                0 \times 84
                                                                                                                                                                                                                              0 \times 85
                                                                                              0х7с
                                                                                                                                                                     0 \times 81
        0x86,
                                                                 0 x8a
                      0 \times 87
                                    0 \times 88
                                                   0 \times 89
                                                                               0 \times 8 b
                                                                                              0 \times 8c
                                                                                                            0 \times 8d
                                                                                                                          0 \times 8 e
                                                                                                                                        0 \times 8 f
                                                                                                                                                       0 \times 90
                                                                                                                                                                     0 \times 91
                                                                                                                                                                                   0 \times 92
                                                                                                                                                                                                 0 \times 93
                                                                                                                                                                                                               0 \times 94
                                                                                                                                                                                                                             0 \times 95
                      0 \times 97
                                     0 \times 98
                                                   0 \times 99
                                                                 0 x 9 a ,
                                                                                0х9ь,
                                                                                                            0x9d,
                                                                                                                                        0 \times 9 f
                                                                                                                                                       0 \times a0,
                                                                                                                                                                                   0 \times a2
                                                                                                                                                                                                 0 \times a 3
                                                                                                                                                                                                                0 \times a 4
         0x96,
                                                                                              0х9с
                                                                                                                          0 x 9 e,
                                                                                                                                                                     0 \times a1
                                                                                                                                                                                                                              0 \times a5
        0 x a 6 ,
                                                                 0 xaa,
                      0 \times a7
                                    0xa8
                                                   0 \times a 9
                                                                               Oxab
                                                                                              0 vac
                                                                                                            0xad
                                                                                                                          0 xae.
                                                                                                                                        0 \text{ yaf}
                                                                                                                                                       0 \times b \cdot 0
                                                                                                                                                                     0 \times b 1
                                                                                                                                                                                   0 \times h2
                                                                                                                                                                                                 0xb3
                                                                                                                                                                                                               0 \times b = 4
                                                                                                                                                                                                                              0 \times b5
         0xb6,
                      0 \times b7
                                    0 \times b8
                                                   0xb9,
                                                                 0 \times ba ,
                                                                               0xbb,
                                                                                              0xbc,
                                                                                                            0xbd,
                                                                                                                          0 \times be,
                                                                                                                                        0xbf,
                                                                                                                                                       0 \times c0,
                                                                                                                                                                    0 \ge c \ 1
                                                                                                                                                                                   0 \times c 2
                                                                                                                                                                                                 0 \times c3,
                                                                                                                                                                                                               0 \times c 4
                                                                                                                                                                                                                              0 \times c5
         0 \times c6
                      0 \times c7
                                    0 \times c8
                                                   0 \times c9
                                                                 0 x ca.
                                                                               0 \times cb
                                                                                              0 \times cc
                                                                                                            0 \times cd
                                                                                                                          Охсе
                                                                                                                                        0 \times c f
                                                                                                                                                       0 \times d0
                                                                                                                                                                     0 \times d1
                                                                                                                                                                                   0 \times d2
                                                                                                                                                                                                 0 \times d3
                                                                                                                                                                                                               0 \times d4
                                                                                                                                                                                                                              0 \times d5
                                                                 0\;x\,d\,a\ ,
                                                                                                                          0 \times de,
                                                                                                                                                                    0\ge 1
                                                                                                                                                                                                 0\,\mathrm{xe}\,3 ,
                                                                                                                                                                                                               0 \ge 4
                      0 \times d7
                                                   0 \times d9
                                                                                0xdb,
                                                                                                            0xdd,
                                                                                                                                        0 \times df,
                                                                                                                                                       0 \times e0,
                                                                                                                                                                                   0 \times e2 ,
         0xd6.
                                     0 \times d8
                                                                                              0xdc,
                                                                                                                                                                                                                              0 \times e5
        0 xe6 ,
                                                                                                                                                      0 x f0,
                                                                                                                                                                                                 0 x f3,
                                                                 0xea ,
                                                                               0 x eb
                                                                                                            0 \text{ xed},
                      0 \times e7
                                    0 \times e 8
                                                   0 \times e9
                                                                                              0 \times ec
                                                                                                                          0 \times e e
                                                                                                                                        0 \times ef
                                                                                                                                                                    0 \times f1
                                                                                                                                                                                   0 \times f2
                                                                                                                                                                                                               0 \times f4
                                                                                                                                                                                                                              0 \times f5
                       0 x f7
                                     0 \times f8
                                                                                                                          0 \times fe ,
         0 x f6
                                                   0 x f9,
                                                                 0 xfa,
                                                                               0xfb,
                                                                                              0 \times fc
                                                                                                            0xfd,
                                                                                                                                        0xff,
                                                                                                                                                       0 \times 00,
                                                                                                                                                                    0 \times 01
                                                                                                                                                                                   0 \times 02 ,
                                                                                                                                                                                                 0 \times 03,
                                                                                                                                                                                                               0 \times 04
                                                                                                                                                                                                                             0 \times 05
nin
                 SBox
                              07
        0 \times 07,
                      0 \times \overline{08}
                                                                                                                                                                                   0 \times 13,
                                     0 \times 09
                                                   0 x 0 a ,
                                                                 0 \times 0 \, \mathrm{b}
                                                                               0~\mathrm{x}~0~\mathrm{c}
                                                                                                                          0 \times 0 f,
                                                                                                                                                      0 \times 11
                                                                                                                                                                     0 \times 12
                                                                                                                                                                                                 0 \times 14,
                                                                                                                                                                                                               0 \times 15
                                                                                              0 \times 0 d
                                                                                                            0x0e,
                                                                                                                                        0 \times 10
                                                                                                                                                                                                                              0 \times 16
                                                   0 x 1 a ,
                                                                                                            0 x 1 e ,
        0 \times 17
                      0 \times 18
                                    0 \times 19
                                                                 0 \times 1 b.
                                                                               0 \times 1 c
                                                                                              0 \times 1 d
                                                                                                                          0 \times 1 f
                                                                                                                                        0 \times 20
                                                                                                                                                      0 \times 21
                                                                                                                                                                    0 \times 22
                                                                                                                                                                                   0 \times 23.
                                                                                                                                                                                                 0 \times 24.
                                                                                                                                                                                                               0 \times 25
                                                                                                                                                                                                                             0 \times 26
         0 x 37 .
                      0 \times 38
                                    0 \times 39
                                                   0 x 3 a .
                                                                 0 x 3 b .
                                                                               0 \times 3 c
                                                                                              0 \times 3 d
                                                                                                            0 x 3 e .
                                                                                                                          0 \times 3 f
                                                                                                                                        0 \times 40
                                                                                                                                                      0 \times 41
                                                                                                                                                                     0 \times 42
                                                                                                                                                                                   0 x 43.
                                                                                                                                                                                                 0x44.
                                                                                                                                                                                                               0 \times 45
                                                                                                                                                                                                                             0 \times 46
                                                   0 \times 4 a ,
                                                                 0 \ge 4 \ \mathrm{b}
                                                                                              0 \times 4 d
                                                                                                            0 x 4 e ,
                                                                                                                                                       0 \times 5
         0 x 57,
0 x 67,
                                                   0 \times 5 a,
                      0 \times 58
                                    0 \times 59
                                                                 0x5b,
                                                                               0 \times 5 c
                                                                                              0 \times 5 d
                                                                                                            0x5e,
                                                                                                                          0 \times 5 f
                                                                                                                                        0 \times 60
                                                                                                                                                       0 \times 61
                                                                                                                                                                    0 \times 62
                                                                                                                                                                                   0 \times 63,
                                                                                                                                                                                                 0x64,
                                                                                                                                                                                                               0 \times 65
                                                                                                                                                                                                                              0 \times 66
                       0 \times 68
                                    0 \times 69
                                                   0 x 6a,
                                                                 0x6b,
                                                                               0 \times 6 c
                                                                                              0 x 6 d
                                                                                                            0x6e,
                                                                                                                          0x6f,
                                                                                                                                        0 \times 70
                                                                                                                                                       0 \times 71
                                                                                                                                                                     0 \times 72
                                                                                                                                                                                   0 \times 73,
                                                                                                                                                                                                 0 \times 74
                                                                                                                                                                                                               0 \times 75
                                                                                                            0x7e,
         0 \times 77
                      0 \times 78
                                    0 \times 79
                                                   0 x 7 a .
                                                                 0 \times 7 b.
                                                                               0 \times 7 c
                                                                                              0 \times 7 d
                                                                                                                          0 \times 7 f
                                                                                                                                        0 \times 80
                                                                                                                                                      0 \times 81
                                                                                                                                                                     0 \times 82
                                                                                                                                                                                   0 \times 83 .
                                                                                                                                                                                                 0 \times 84 .
                                                                                                                                                                                                               0 \times 85
                                                                                                                                                                                                                             0 \times 86
                                                                 0 x 8 b
                                                                                                                                                       0 x 9 1
                                                                                                                                                                                   0 x 93
                                                                                                                                                                                                 0 x 9 4
                                                                                                                                                                                                                0 x 9 5
                                     0 \times 89
                                                                                                                                        0 \times 90
                                                                                                                                                                     0 \times 92
        0x97,
                      0 \times 98
                                    0 \times 99
                                                   0 x 9 a .
                                                                 0x9b.
                                                                               0 x 9 c .
                                                                                              0 \times 9 d
                                                                                                            0 x 9 e .
                                                                                                                          0 \times 9 f
                                                                                                                                        0 \times a 0
                                                                                                                                                       0 \times a 1
                                                                                                                                                                    0 \times a2
                                                                                                                                                                                   0 \times a3.
                                                                                                                                                                                                 0xa4.
                                                                                                                                                                                                               0 \times a5
                                                                                                                                                                                                                             0xa6
                                                                               0 \, \mathrm{xac} ,
                                     0 \times a9
                                                   0 хаа ,
                                                                 0 xab,
                                                                                              0xad
                                                                                                            0 xae ,
                                                                                                                          0 \times af,
                                                                                                                                                       0xb1,
                                                                                                                                                                                                 0xb4,
         0 \times b7,
                      0xb8,
                                    0 \times b9
                                                   0xba,
                                                                 0xbb,
                                                                               0 \times b c
                                                                                              0 \times bd
                                                                                                            0xbe,
                                                                                                                          0xbf,
                                                                                                                                        0 \times c 0
                                                                                                                                                       0 \times c1
                                                                                                                                                                     0 \times c2
                                                                                                                                                                                   0 \times c3
                                                                                                                                                                                                 0 \times c 4
                                                                                                                                                                                                               0 \times c5
                                                                                                                                                                                                                              0 \times c6
                                    0 \times c9
                                                                 0 \times cb
                                                                               0 \, \mathrm{xcc}
                                                                                                            0xce,
                                                                                                                                        0 \times d0
                                                                                                                                                       0 \times d1
                                                                                                                                                                     0 \times d2
                                                                                                                                                                                                 0 \times d4
                                                                                                                                                                                                                0 \times d5
                                                                 0xdb.
         0 \times d7
                      0 \times d8
                                    0 x d9.
                                                   0xda.
                                                                               0xdc.
                                                                                              0xdd
                                                                                                            0xde.
                                                                                                                          0xdf.
                                                                                                                                        0 \times e 0
                                                                                                                                                      0 x e 1 .
                                                                                                                                                                    0 x e 2
                                                                                                                                                                                   0 \times e3.
                                                                                                                                                                                                 0 \times e4
                                                                                                                                                                                                               0 \times e5
                                                                                                                                                                                                                             0 \times e6
                      0 x e 8
                                    0 \times e 9
                                                                 0 xeb,
                                                                               0 xec,
                                                                                              0 \times e d
                                                                                                            0 xee,
                                                                                                                          0 \times ef
                                                                                                                                        0 \times f0
                                                                                                                                                      0 \times f1
                                                                                                                                                                     0 x f 2
                                                                                                                                                                                   0 \times f3
                                                                                                                                                                                                 0 \times f4 ,
                                                                                                                                                                                                               0 \times f5
        0 \times f7
                      0 \times f8
                                    0 x f9.
                                                   0xfa, 0xfb,
                                                                               0xfc.
                                                                                             0xfd.
                                                                                                           0xfe, 0xff,
                                                                                                                                        0 \times 00.
                                                                                                                                                     0 \times 01 , 0 \times 02 ,
                                                                                                                                                                                   0 \times 03.
                                                                                                                                                                                                0 \times 04.
                                                                                                                                                                                                              0 \times 05.
                                                                                                                                                                                                                             0 \times 06
                 SBox
uin
                             0.8
        0\overline{x}08, 0x\overline{0}9,
                                                   0x0b,
                                    0 \times 0 a,
                                                                 0 \times 0 c,
                                                                               0x0d,
                                                                                                            0 \times 0 f,
                                                                                                                                                                                                 0 \times 15
                                                                                              0 \times 0 e,
                                                                                                                          0x10,
                                                                                                                                        0x11,
                                                                                                                                                       0 x 12,
                                                                                                                                                                     0 \times 13
                                                                                                                                                                                   0x14,
                                                                                                                                                                                                                0 \times 16
                                                                                                                                                                                                                              0 \times 17
                       0 \times 19
                                    0x 1 a ,
                                                   0x1b,
                                                                 0 \times 1\,\mathrm{c} ,
                                                                               0 \times 1 d
                                                                                                                          0 \times 20
                                                                                                                                        0 \times 21
                                                                                                                                                      0 \times 22,
                                                                                              0 \times 1 e
                                                                                                            0 \times 1 \; f ,
                                                                                                                                                                    0 \times 23
                                                                                                                                                                                                 0 \times 25
                                                                                                                                                                                                               0 \times 26
         0 \times 18
                                                                                                                                                                                   0 \times 24
                                                   0x2b,
                                                                                                            0 \times 2 f,
                                                                                                                                                      0 \times 32
                                                                                                                                                                    0 \times 33
                                                                                                                                                                                                 0 \times 35,
                      0 \times 29
                                    0 x 2 a ,
                                                                 0 x 2 c ,
                                                                               0x2d,
                                                                                             0 \times 2e,
                                                                                                                          0 \times 30,
                                                                                                                                        0 \times 31
                                                                                                                                                                                   0 \times 34,
                                                                                                                                                                                                               0 \times 36
                                                                                                                                                                                                                             0 \times 37
         0 \times 28,
         0 \times 38
                      0 \times 39
                                    0 \times 3 a
                                                   0 \times 3 b
                                                                 0 \times 3 c
                                                                               0 \times 3 d
                                                                                              0 \times 3 e
                                                                                                            0 \times 3 f
                                                                                                                          0 \ge 40
                                                                                                                                        0 \times 41
                                                                                                                                                       0 \times 42
                                                                                                                                                                     0 \times 43
                                                                                                                                                                                   0 \times 44
                                                                                                                                                                                                 0 \times 45
                                                                                                                                                                                                                0 x 4 6
                                                                 0 x 4 c ,
                                                                                                            0 \times 4 f
         0 x 48,
                      0 \times 49
                                    0 x 4 a ,
                                                   0 x 4 b ,
                                                                               0 \times 4 d
                                                                                              0 x 4 e
                                                                                                                          0 \times 50
                                                                                                                                        0 \times 51
                                                                                                                                                       0 \times 52,
                                                                                                                                                                     0 \times 53
                                                                                                                                                                                   0 \times 54,
                                                                                                                                                                                                 0 \times 55
                                                                                                                                                                                                                0 \times 56
                                                                                                                                                                                                                              0 \times 57
        0 x 58,
                                                   0x5b,
                                                                 0х5с,
                                                                                                                                                      0x62,
                                    0 x 5 a ,
                                                                                              0 х5е
                      0 \times 59
                                                                               0 \times 5 d
                                                                                                            0 \times 5 f
                                                                                                                          0 \times 60
                                                                                                                                        0 \times 61
                                                                                                                                                                    0 \times 63
                                                                                                                                                                                   0 \times 64
                                                                                                                                                                                                 0 \times 65
                                                                                                                                                                                                               0 \times 66
                                                                                                                                                                                                                              0 \times 67
                                    0 \times 6 a ,
                                                                 0\,\mathrm{x}\,6\,\mathrm{c} ,
                                                                               0x6d,
                                                                                                                                        0 \ge 71
                                                                                                                                                       0 \times 72, 0 \times 73,
                                                                                                                                                                                                 0 \times 75,
         0x68,
                      0x69,
                                                   0x6b,
                                                                                              0x6e,
                                                                                                            0x6f,
                                                                                                                          0 \times 70,
                                                                                                                                                                                   0x74,
                                                                                                                                                                                                               0 \times 76
                                                                                                                                                                                                                              0 \times 77
        0x78,
                                    0 x 7 a
                                                                                                                                                      0x82,
                                                   0x7b,
                      0 \times 79
                                                                 0 \times 7 c
                                                                               0 \times 7 d
                                                                                              0 \times 7 e
                                                                                                            0 \times 7 f
                                                                                                                          0 \times 80
                                                                                                                                        0 \times 81
                                                                                                                                                                    0 \times 83
                                                                                                                                                                                   0 \times 84
                                                                                                                                                                                                 0 \times 85
                                                                                                                                                                                                               0 \times 86
                                                                                                                                                                                                                             0 \times 87
                                                                 0\,\mathrm{x}\,8\,\mathrm{c} ,
                                                                                                            0 \times 8 f,
                      0x89
                                                   0x8b,
                                                                               0 \times 8 d
                                                                                              0x8e,
                                                                                                                          0x90,
                                                                                                                                        0 \times 91
                                                                                                                                                       0x92,
                                                                                                                                                                    0 \times 93
                                                                                                                                                                                   0 \times 94,
                                                                                                                                                                                                 0 \times 95
                                                                                                                                                                                                                              0 \times 97
         0x88,
                                    0x8a,
                                                                                                                                                                                                               0 \times 96
                                                   0x9b,
                                                                                              0x9e,
                                                                                                                                                      0 xa2
                                                                 0 x 9 c
         0x98,
                      0 \times 99
                                    0 x 9 a
                                                                               0×9d
                                                                                                            0 x 9 f.
                                                                                                                          0 \times a 0
                                                                                                                                        0 \times a 1
                                                                                                                                                                    0 \times a3
                                                                                                                                                                                   0 \times a4
                                                                                                                                                                                                 0 \times a5
                                                                                                                                                                                                               0xa6
                                                                                                                                                                                                                              0 \times a7
                                                                                                                                                       0 x b 2 ,
                                                                 0 \, \mathrm{xac} ,
                                                                                                            0 \times af ,
                                                                                                                          0 \times b0,
                                                                                                                                                                    0 \times b3
                                                                                                                                                                                                 0\,\mathrm{x}\,\mathrm{b}\,5
         0 xa8,
                      0 \times a9
                                    0 xaa,
                                                   0 xab,
                                                                               0 xad,
                                                                                              0 \, \text{xae},
                                                                                                                                        0 \times b1
                                                                                                                                                                                   0xb4,
                                                                                                                                                                                                               0 \times b6
                                                                                                                                                                                                                              0 \times b7
         0 x b8 .
                      0 \times b9
                                    0 \, \mathrm{xba}
                                                   0 \times bb
                                                                 0 \times bc
                                                                               0 \times bd \times 0
                                                                                              0 \times b e
                                                                                                            0 \times b f
                                                                                                                          0 \times c0
                                                                                                                                        0 \times c1
                                                                                                                                                       0 \times c2
                                                                                                                                                                    0 \times c3
                                                                                                                                                                                   0 \times c4
                                                                                                                                                                                                 0 \times c5
                                                                                                                                                                                                               0 \times c6
                                                                                                                                                                                                                              0 \times c7
                      0 \times c 9
                                                                 0\,\,\mathrm{xcc} ,
                                                                                                            0 \times cf ,
                                                                                                                          0 \times d0
                                                                                                                                        0 \times d1
                                                                                                                                                                    0 x d 3 ,
                                                                                                                                                                                                 0 \times d5
         0 x c 8 .
                                     0 \times ca,
                                                   0 хсь ,
                                                                                0\,x\,c\,d
                                                                                              0 \, \mathrm{xce} ,
                                                                                                                                                       0 \times d2,
                                                                                                                                                                                   0xd4,
                                                                                                                                                                                                               0 \times d6
                                                                                                                                                                                                                              0 \times d7
                                                                                                                                                      0 x e 2 ,
                                                   0xdb,
                                                                                              0xde,
                                                                                                                                                                                   0 x e 4 ,
        0xd8,
                                                                                                            0 \times df,
                      0 \times d9
                                    0 \times da
                                                                 0 \times dc
                                                                               0xdd
                                                                                                                          0 \times e0
                                                                                                                                        0 \times e1
                                                                                                                                                                    0 \ge e 3
                                                                                                                                                                                                 0 \times e5
                                                                                                                                                                                                               0 \times e6
                                                                                                                                                                                                                             0 \times e7
                      0 \times e9 ,
                                                                 0\,\,\mathrm{xec} ,
                                                                                                            0 x e f ,
                                                                                                                          0 x f0 ,
                                                                                                                                         0 x f 1
                                                                                                                                                       0 x f2 ,
                                                                                                                                                                     0 \times f3
                                                                                                                                                                                   0 x f4,
                                                                                                                                                                                                 0 x f5,
                                     0 \times ea ,
                                                   0 xeb,
                                                                                0 \times ed,
                                                                                              0 \, \mathrm{xee} ,
                                                                                                                                                                                                                0 \times f6
         0 x e 8 ,
        0 \times f8
                      0 \times f9
                                    0 \times fa
                                                   0 \times fb
                                                                 0 \times fc
                                                                               0 \times fd
                                                                                              0 \times fe
                                                                                                            0 \times ff
                                                                                                                          0 \times 00
                                                                                                                                        0 \times 0.1
                                                                                                                                                      0 \times 0.2
                                                                                                                                                                    0 \times 0.3
                                                                                                                                                                                   0 \times 0.4
                                                                                                                                                                                                 0 \times 0.5
                                                                                                                                                                                                               0 \times 06
                                                                                                                                                                                                                             0 \times 0.7
                  SBox_
                             09
                                                                                                                                                      0 x 1 3 ,
        0 \times 09, 0 \times \overline{0}a,
                                    0 x 0 b .
                                                   0 \times 0 c,
                                                                 0 \times 0 d.
                                                                               0 \times 0 e.
                                                                                              0 \times 0 f.
                                                                                                            0 \times 10 .
                                                                                                                          0 \times 11
                                                                                                                                        0 \times 12 .
                                                                                                                                                                     0 \times 14
                                                                                                                                                                                   0 \times 15.
                                                                                                                                                                                                 0 \times 16.
                                                                                                                                                                                                               0 \times 17
                                                                                                                                                                                                                             0 \times 18
                       0 \times 1 a ,
                                                                                0 x 1 e .
         0x29.
                      0 x 2 a .
                                    0 x 2 b
                                                   0 x 2 c .
                                                                 0 x 2 d .
                                                                               0 x 2 e .
                                                                                             0 \times 2 f
                                                                                                            0 x 30.
                                                                                                                          0 \times 31
                                                                                                                                        0 \times 32
                                                                                                                                                      0 x 3 3 .
                                                                                                                                                                    0 \times 34
                                                                                                                                                                                   0 \times 35
                                                                                                                                                                                                 0 \times 36
                                                                                                                                                                                                               0 \times 37
                                                                                                                                                                                                                             0 \times 38
                       0 x 3 a ,
                                     0 \times 3b
                                                                 0 \times 3 d
                                                                                0х3е,
                                                                                              0 \times 3 f
                                                                                                                                         0 \times 42
                                                                                                                                                       0 x 43,
                                                                                                                                                                                                 0 \times 46
                                                                                                                                                       0 \times 53,
         0 \times 49.
                      0 x 4 a .
                                    0 \times 4 b
                                                   0 \times 4 c.
                                                                 0 \times 4 d.
                                                                               0 x 4 e .
                                                                                              0 \times 4 f
                                                                                                            0 \times 50.
                                                                                                                          0 \times 51
                                                                                                                                        0 \times 52
                                                                                                                                                                    0 \times 54
                                                                                                                                                                                   0 \times 55
                                                                                                                                                                                                 0 \times 56
                                                                                                                                                                                                               0 \times 57
                                                                                                                                                                                                                              0 \times 58
         0 x 59 ,
                                                                                                                                                       0 \times 63, 0 \times 64
                      0 x 5 a ,
                                    0x5b,
                                                                 0 x 5 d ,
                                                                               0 x 5 e ,
                                                                                                            0 \times 60
                                                                                                                          0 \times 61
                                                                                                                                        0 \times 62
                                                                                                                                                                                   0 \times 65,
                                                                                                                                                                                                 0 \times 66
                                                                                                                                                                                                               0 \times 67
                                                                                                                                                      0 \times 73,
         0x69,
                      0 x 6 a .
                                    0 \times 6 b
                                                   0 \times 6c.
                                                                 0 \times 6 d.
                                                                               0x6e.
                                                                                              0 \times 6 f.
                                                                                                            0 \times 70.
                                                                                                                          0 \times 71
                                                                                                                                        0 \times 72
                                                                                                                                                                    0 \times 74
                                                                                                                                                                                   0 \times 75
                                                                                                                                                                                                 0 \times 76 .
                                                                                                                                                                                                               0 \times 77
                                                                                                                                                                                                                             0 \times 78
                                                   0 x 7 c
                                                                 0 \times 7 d
                                                                                              0 x 7
                                                                                                            0 x 8 0
                                                                                                                                        0 \times 82
                                                                                                                                                      0 x 8 3
                                                                                                                                                                                   0 \times 85
                                    0 \times 7 b
        0x89,
                      0 x 8 a .
                                    0x8b.
                                                   0x8c.
                                                                 0x8d.
                                                                               0x8e.
                                                                                              0x8f.
                                                                                                            0x90.
                                                                                                                          0 \times 91
                                                                                                                                        0 \times 92
                                                                                                                                                      0 \times 93, 0 \times 94
                                                                                                                                                                                   0x95.
                                                                                                                                                                                                 0x96.
                                                                                                                                                                                                               0 \times 97
                                                                                                                                                                                                                              0 \times 98
                      0 x 9 a ,
         0 x 99 ,
                                    0 \times 9 b
                                                   0 x 9 c
                                                                 0 \times 9 d
                                                                               0х9е
                                                                                              0 \times 9 f
                                                                                                            0 \times a 0
                                                                                                                          0 \times a 1
                                                                                                                                        0 \times a 2
                                                                                                                                                      0 \times a3,
                                                                                                                                                                     0 \times a4
                                                                                                                                                                                                 0 \times a 6
                                                                                                                                                                                                               0 \times a7
         0 \times a9,
                      0 xaa,
                                    0 xab.
                                                   0 xac,
                                                                 0 xad,
                                                                               0 xae,
                                                                                              0 \times a f
                                                                                                            0 \times b0,
                                                                                                                          0 \times b1
                                                                                                                                        0 \times b2
                                                                                                                                                      0 \times b3,
                                                                                                                                                                    0 \times b 4
                                                                                                                                                                                   0xb5,
                                                                                                                                                                                                 0 \times b 6
                                                                                                                                                                                                               0 \times b7
                                                                                                                                                                                                                              0 \times b8
                       0xba,
                                    0 \times b b
                                                   Охьс
                                                                 0 \times bd
                                                                               0xbe,
                                                                                                            0 \times c 0
                                                                                                                                                       0 \times c 3
         0 x c 9
                      0 xca.
                                    0xcb.
                                                   0 \times cc
                                                                 0 xcd.
                                                                               0xce.
                                                                                              0 \times cf
                                                                                                            0 \times d0.
                                                                                                                          0 \times d1
                                                                                                                                        0 \times d2
                                                                                                                                                       0 x d 3.
                                                                                                                                                                    0 \times d4
                                                                                                                                                                                   0xd5.
                                                                                                                                                                                                 0xd6
                                                                                                                                                                                                               0 \times d7
                                                                                                                                                                                                                              0 \times d8
                                                   0\,\mathrm{xd}\,\mathrm{c} ,
                                                                               0\,\mathrm{x}\,\mathrm{d}\,\mathrm{e} ,
                                                                                                            0\,\mathrm{x}\,\mathrm{e}\,0 ,
                                                                                                                                                       0 x e 3 , 0 x e 4
                                                                                                                                                                                                               0 x e 7
         0 x d9,
                      0 xda,
                                    0xdb,
                                                                 0xdd,
                                                                                              0 \times df
                                                                                                                          0 x e 1
                                                                                                                                        0 \ge 2
                                                                                                                                                                                   0 \times e5,
                                                                                                                                                                                                 0 \times e 6
         0 x e 9 .
                      0 \, \text{xea} .
                                    0 xeb.
                                                   0 \, \mathrm{xec}
                                                                 0 xed.
                                                                               0 xee.
                                                                                              0 \times ef
                                                                                                            0 \times f0.
                                                                                                                          0 \times f1
                                                                                                                                        0 \times f2
                                                                                                                                                      0 \times f3.
                                                                                                                                                                    0 \times f4
                                                                                                                                                                                   0 x f5.
                                                                                                                                                                                                 0 x f6.
                                                                                                                                                                                                               0 \times f7
                                                                                                                                                                                                                              0 \times f8
                      0 \times fa
                                    0 \times fb
                                                   0 \times fc
                                                                 0 x fd .
                                                                               0 \times fe
                                                                                              0 \times ff
                                                                                                            0 \times 00.
                                                                                                                                                      0 \times 03.
                                                                                                                                                                    0 \times 04
                                                                                                                                                                                                 0 \times 06
                                                                                                                                                                                                               0 \times 0.7
        0 \times f9
                                                                                                                          0 \times 01
                                                                                                                                        0 \times 02
                                                                                                                                                                                   0 \times 05
                                                                                                                                                                                                                             0 \times 08
            t SBox 10
                                    = {
        0 \times 0 a,
                      0 \times \overline{0} b,
                                                                                                                                                                                   0×16,
                                    0 x θc,
                                                   0 x 0 d .
                                                                 0 x 0 e ,
                                                                                              0x10,
                                                                                                                          0 \times 12
                                                                                                                                        0 x 13,
                                                                                                                                                                                                 0 \times 17
                                                                               0 \times 0 f
                                                                                                            0 \times 11
                                                                                                                                                       0x14,
                                                                                                                                                                     0 \times 15
                                                                                                                                                                                                                0 \times 18
                                                                                                                                                                                                                              0 \times 19
         0x1a.
                      0 \times 1 b,
                                    0 x 1 c .
                                                   0 x 1 d .
                                                                 0x1e.
                                                                               0 x 1 f.
                                                                                              0 \times 20.
                                                                                                            0 \times 21 .
                                                                                                                          0 x 2 2 .
                                                                                                                                        0 x 23.
                                                                                                                                                      0 \times 24 .
                                                                                                                                                                    0 \times 25
                                                                                                                                                                                   0 \times 26.
                                                                                                                                                                                                 0 \times 27
                                                                                                                                                                                                               0 \times 28
                                                                                                                                                                                                                             0 \times 29
                                    0 \times 2 c
                                                   0 \times 2 d
                                                                 0\ge 2\,\mathrm{e} ,
                                                                                                            0 \times 31
                                                                                                                                        0 \ge 3 \ 3
                                                                                                                                                       0 \times 34
                                                                                                                                                                     0 \times 35
                                                                                                                                                                                   0 \times 36
                                                                                                                                                                                                 0 \times 37
                                                                                                                                                                                                               0 \times 38
                                                                                                                                                                                                                             0 x 3 9
         0 x 2a,
                      0 \times 2 b
                                                                               0 \times 2 f
                                                                                              0 \times 30
                                                                                                                          0 \times 32
         0 x 3 a ,
                      0 x 3 b ,
                                    0 x 3 c
                                                   0 \times 3 d
                                                                 0 x 3 e ,
                                                                               0 \times 3 f
                                                                                              0 \times 40
                                                                                                            0 \times 41
                                                                                                                          0 \times 42
                                                                                                                                        0 \times 43
                                                                                                                                                       0 x 44,
                                                                                                                                                                     0 \times 45
                                                                                                                                                                                   0 \times 46
                                                                                                                                                                                                 0 \times 47
                                                                                                                                                                                                                0 \times 48
                                                                                                                                                                                                                              0 \times 49
        0 x 4 a ,
                      0 x 4b ,
                                                                 0 \ge 4\,\mathrm{e} ,
                                    0 x 4 c
                                                   0 \times 4 d
                                                                               0 \times 4 f
                                                                                              0 \times 50
                                                                                                            0 \times 51
                                                                                                                          0 \times 52
                                                                                                                                        0 \times 53
                                                                                                                                                       0 \times 54
                                                                                                                                                                     0 \times 55
                                                                                                                                                                                   0 \times 56
                                                                                                                                                                                                 0 \times 57
                                                                                                                                                                                                                0 \times 58
                                                                                                                                                                                                                              0 \times 59
                                                                                                                          0 \times 6\overline{2},
                      0 \times 5b,
                                    0х5с,
                                                                                                                                                                                   0 \times 66 .
                                                                                                                                                                                                 0 \times 67
         0 x 5 a ,
                                                   0 x 5 d ,
                                                                 0 x 5 e ,
                                                                               0 \times 5 f
                                                                                              0x60,
                                                                                                            0 \times 61
                                                                                                                                        0 \times 63,
                                                                                                                                                       0x64,
                                                                                                                                                                    0 \times 65
                                                                                                                                                                                                                0 \times 68
                                                                                                                                                                                                                              0 \times 69
        0x6a,
                      0 \times 6b
                                    0 \times 6c
                                                   0 \times 6d
                                                                 0х6е,
                                                                               0 \times 6 f
                                                                                              0 \times 70
                                                                                                            0 \times 71
                                                                                                                          0 \times 72
                                                                                                                                        0 \times 73
                                                                                                                                                      0 \times 74
                                                                                                                                                                    0 \times 75
                                                                                                                                                                                   0 \times 76
                                                                                                                                                                                                 0 \times 77
                                                                                                                                                                                                               0 \times 78
                                                                                                                                                                                                                             0 \times 79
                      0 \times 7b,
                                                                 0 \times 7 e,
                                                                               0 \times 7 f
                                                                                                            0 \times 81
                                                                                                                          0 \times 82
                                                                                                                                        0x83,
                                                                                                                                                       0 \times 84, 0 \times 85
                                                                                                                                                                                   0x86,
         0x7a,
                                    0х7с
                                                   0 \times 7 d,
                                                                                              0x80,
                                                                                                                                                                                                 0 \times 87
                                                                                                                                                                                                                0 \times 88
                                                                                                                                                                                                                              0 \times 89
                                                                 0 x 8e,
        0 x8a,
                      0x8b,
                                                                                                                                                      0x94,
                                    0 \times 8c
                                                   6x \times 0
                                                                               0 \times 8 f
                                                                                              0 \times 90
                                                                                                            0 \times 91
                                                                                                                          0 \times 92
                                                                                                                                        0 \times 93
                                                                                                                                                                    0 \times 95
                                                                                                                                                                                   0 \times 96
                                                                                                                                                                                                 0 \times 97
                                                                                                                                                                                                               0 \times 98
                                                                                                                                                                                                                              0 \times 99
                      0 x9b ,
                                                   0 x 9 d ,
                                                                 0х9е,
                                                                               0 x 9 f
         0 x 9 a ,
                                    0 x 9 c.
                                                                                              0 \times a0,
                                                                                                            0 \times a1
                                                                                                                          0 \times a \cdot 2
                                                                                                                                        0 \times a3,
                                                                                                                                                       0 \times a4,
                                                                                                                                                                    0 \times a5
                                                                                                                                                                                   0xa6,
                                                                                                                                                                                                 0 \times a 7
                                                                                                                                                                                                                0xa8
                                                                                                                                                                                                                             0 \times a 9
                      0 \times ab
                                    0 \times ac
                                                   0 \times a d
                                                                 0 \times a.e
                                                                               0 \times a f
                                                                                              0 \times b = 0
                                                                                                            0 \times b1
                                                                                                                          0 \times b2
                                                                                                                                        0 \times b3
                                                                                                                                                      0 \times b4.
                                                                                                                                                                     0 \times b5
                                                                                                                                                                                   0 \times b = 6
                                                                                                                                                                                                 0 \times b = 7
                                                                                                                                                                                                                0 \times b = 8
                                                                                                                                                                                                                              0 \times b9
         0 xaa,
                      0xbb,
                                                                 0 \times be ,
                                                                               0 x b f ,
                                                                                                            0 \ge c \ 1
                                                                                                                                                       0 \times c 4 ,
         0xba,
                                    0xbc,
                                                                                              0 x c 0
                                                                                                                                        0 \times c3,
                                                                                                                                                                    0 \times c5
                                                                                                                                                                                                 0 \times c7
                                                                                                                                                                                                               0 \times c 8
                                                   0 \times bd
                                                                                                                          0 \times c 2
                                                                                                                                                                                   0 \times c6,
                                                                                                                                                                                                                              0 \times c9
                                                                                                                                                      0 x d 4 ,
        0 xca,
                      0 xcb,
                                                                 0 xce,
                                                                                                            0 \times d1,
                                                                                                                                                                                   0xd6,
                                    0 \times cc
                                                                               0 \times c f
                                                                                              0 \times d0
                                                                                                                          0 \times d2
                                                                                                                                        0 \times d3.
                                                                                                                                                                    0 \times d5
                                                                                                                                                                                                 0 \times d7
                                                                                                                                                                                                               0 \times d8
                                                                                                                                                                                                                             0 \times d9
                                                   0 \times cd
                      0xdb,
                                     0xdc,
                                                   0xdd,
                                                                 0xde,
                                                                               0 \ge d f ,
                                                                                              0 \times e 0
                                                                                                            0\,\mathrm{xe}\,1 ,
                                                                                                                          0 \times e2,
                                                                                                                                        0 \times e3,
                                                                                                                                                       0 x e 4 , 0 x e 5 ,
                                                                                                                                                                                   0 \times e6,
                                                                                                                                                                                                 0xe7 ,
                                                                                                                                                                                                               0 \times e 8
                                                                                                                                                                                                                              0 \times e9
         0xda,
        0 xea ,
                                                                                                                                                      0 x f4,
                      0 veb
                                    Oxec
                                                   0 xed
                                                                 0 xee
                                                                               0 \times ef
                                                                                              0 \times f0
                                                                                                            0 \times f1
                                                                                                                          0 \times f2
                                                                                                                                        0 \times f3
                                                                                                                                                                    0 \times f5
                                                                                                                                                                                   0 \times f6
                                                                                                                                                                                                 0 \times f7
                                                                                                                                                                                                               0 \times f8
                                                                                                                                                                                                                             0 \times f9
                      0 \times fb
                                                   0 xfd
                SBox
                             1.1
         0x0b,
                      0 \times 0 c,
                                                                                                                                                       0 x 15,
                                     0 x 0d.
                                                   0 x 0 e .
                                                                 0 x 0 f.
                                                                               0 \times 10
                                                                                                            0 \times 12.
                                                                                                                          0 x 13.
                                                   0 x 1 e ,
        0x1b.
                      0 x1c.
                                    0 x 1 d .
                                                                 0 x 1 f.
                                                                               0x20.
                                                                                              0 \times 21
                                                                                                            0 x 2 2 .
                                                                                                                          0 x 2 3 .
                                                                                                                                        0 x 2 4 .
                                                                                                                                                      0 \times 25 .
                                                                                                                                                                    0 \times 26
                                                                                                                                                                                   0 \times 27 .
                                                                                                                                                                                                 0 \times 28
                                                                                                                                                                                                               0 \times 29
                                                                                                                                                                                                                             0 \times 2 a
                                                                 0 \times 2 f
                                     0 \times 2d
                                                   0 \times 2e,
                                                                                0 \times 30
                                                                                              0 \times 31
                                                                                                            0 \times 32,
                                                                                                                          0 \times 33
                                                                                                                                        0 \times 34
                                                                                                                                                       0 \times 35,
                                                                                                                                                                     0 \times 36
                                                                                                                                                                                   0 \times 37,
                                                                                                                                                                                                 0 \times 38
                                                                                                                                                                                                                0 \times 39
        0x3b,
                                                   0 x 3 e ,
                      0 \times 3c.
                                    0 \times 3 d
                                                                 0 \times 3 f
                                                                               0 \times 40
                                                                                              0 \times 41
                                                                                                            0 \times 42
                                                                                                                          0 \times 43
                                                                                                                                        0 \times 44
                                                                                                                                                       0 \times 45 .
                                                                                                                                                                    0 \times 46
                                                                                                                                                                                   0 \times 47
                                                                                                                                                                                                 0 \times 48
                                                                                                                                                                                                               0 \times 49
                                                                                                                                                                                                                              0 \times 4 a
                                                   0 \times 4 e ,
         0 x 4b ,
                                     0 x 4d
                                                                 0 x 4 f
                                                                                0 \times 50
                                                                                                            0 \times 52
                                                                                                                                                       0x55,
                                                                                                                                                                                                                0 x 5 9
        0x5b,
                                                   0х5е,
                                                                                                                                                      0x65,
                      0 \times 5 c
                                    0 \times 5 d
                                                                 0 \times 5 f
                                                                               0 \times 60
                                                                                              0 \times 61
                                                                                                            0 \times 62 .
                                                                                                                          0 \times 63
                                                                                                                                        0 \times 64.
                                                                                                                                                                    0 \times 66
                                                                                                                                                                                   0 \times 67
                                                                                                                                                                                                 0 \times 68
                                                                                                                                                                                                               0 \times 69
                                                                                                                                                                                                                             0 \times 6 a
                                                                                              0 x 7
                                                                                                            0 x 72,
                                                                                                                          0 x 7 3
                                                                                                                                        0 x 7 4
                                                                                                                                                       0x75,
                                                                                                                                                                     0 x 76
                                                                                                                                                                                                               0 x 7 9
                                                                               0 \times 70
        0x7b,
0x8b,
                                                   0 x 7 e ,
0 x 8 e ,
                                                                                                                                                      0 \times 85,
                      0 x7c.
                                    0 \times 7 d
                                                                 0 x 7 f.
                                                                               0x80.
                                                                                              0 \times 81
                                                                                                            0x82.
                                                                                                                          0x83.
                                                                                                                                        0 \times 84
                                                                                                                                                                    0 \times 86
                                                                                                                                                                                   0 \times 87
                                                                                                                                                                                                 0x88
                                                                                                                                                                                                               0 \times 89
                                                                                                                                                                                                                             0 x 8 a
                                                                                              0 \times 91
                                                                                                                                                      0\,\mathrm{x}\,9\,5 ,
                                                                                                                                                                    0 \ge 96
                                                                                                                                                                                                 0 \times 98
                                                                                                                                                                                                               0 \times 99
                                    0x8d
                                                                               0 \times 90
                                                                                                            0 \times 92
                                                                                                                          0 \times 93
                                                                                                                                        0 \times 94
                                                                                                                                                                                   0 \times 97
                                                                                                                                                                                                                              0 x 9 a
         0x9b,
                      0 x 9 c ,
                                    0 x 9d .
                                                   0х9е,
                                                                 0 x 9 f,
                                                                               0 \times a0.
                                                                                              0 \times a 1
                                                                                                            0 \times a2,
                                                                                                                          0 \times a3,
                                                                                                                                        0 \times a 4
                                                                                                                                                      0 \times a5,
                                                                                                                                                                    0 \times a6
                                                                                                                                                                                   0 \times a7
                                                                                                                                                                                                 0xa8
                                                                                                                                                                                                               0 \times a9
                                                                                                                                                                                                                             0 \, \mathrm{xaa}
                                     0 xad
                                                                 0 \times a f
                                                                                0 \times b 0
                                                                                              0 x b
                                                                                                            0 \times b2
                                                                                                                          0 \times b3
                                                                                                                                        0 \times b 4
                                                                                                                                                       0xb5,
                                                                                                                                                                                                 0 x b 8
                                                                                                                                                                                                                0 x b 9
         0xbb.
                      0xbc.
                                    0 \times b d
                                                   0xbe.
                                                                 0xbf.
                                                                               0 \times c 0
                                                                                              0 \times c1
                                                                                                            0 \times c2
                                                                                                                          0 \times c3
                                                                                                                                        0 \times c 4
                                                                                                                                                       0 \times c5.
                                                                                                                                                                    0 \times c6
                                                                                                                                                                                   0 \times c7
                                                                                                                                                                                                 0 \times c8
                                                                                                                                                                                                               0 \times c9
                                                                                                                                                                                                                              0 \times ca
                                                                                                            0\,x\,d\,2
                                                                                                                                                      0\,\mathrm{xd}\,5 ,
                                                                                                                                                                     0 \times d6
                                                                                                                                                                                                               0 \times d9
                                     0 \times c d
                                                                 0xcf,
                                                                               0 \times d0
                                                                                              0 \times d1
                                                                                                                          0 \times d3
                                                                                                                                        0 \times d4
                                                                                                                                                                                   0 \times d7
                                                                                                                                                                                                 0 \times d8
         0xdb,
                      0xdc,
                                    0xdd,
                                                   0xde,
                                                                 0xdf,
                                                                               0 \times e0,
                                                                                              0 \times e1
                                                                                                            0 \times e2,
                                                                                                                          0 \times e3,
                                                                                                                                        0 \times e 4
                                                                                                                                                      0 \times e5,
                                                                                                                                                                    0xe6,
                                                                                                                                                                                   0 \times e7
                                                                                                                                                                                                 0 x e 8
                                                                                                                                                                                                               0 \times e9
                                                                                                                                                                                                                             0 \, \mathrm{xea}
                                                                                                                                                      0 x f5,
                                                                                              0 x f1
                                                                                                                          0 x f3
                                                                                                                                        0 x f 4
                                                                                                                                                                                   0 x f 7
                      Охес
                                    0 \times ed
                                                   Охее
                                                                 0 \times e f
                                                                               0 \times f0
                                                                                                            0 \times f2
                                                                                                                                                                     0 \times f6
                                                                                                                                                                                                 0 \times f8
                                                                                                                                                                                                               0 \times f9
         0 \times eb
                                                                                                                                                                                                                             0 \times f_2
        0 \times fb
                      0 \times fc
                                    0xfd,
                                                   0 x fe,
                                                                 0 xff,
                                                                               0 \times 00,
                                                                                             0 \times 01
                                                                                                            0 \times 02,
                                                                                                                          0 \times 03,
                                                                                                                                        0 \times 04,
                                                                                                                                                      0 \times 05,
                                                                                                                                                                    0 \times 06
                                                                                                                                                                                   0 \times 07,
                                                                                                                                                                                                 0 \times 08,
                                                                                                                                                                                                               0 \times 09.
                                                                                                                                                                                                                             0 \times 0 a
                 SBox_12
, 0x0d,
        0х0с,
                                    0 x 0 e .
                                                   0 x 0 f .
                                                                 0 x 10.
                                                                               0 x 11.
                                                                                              0x12.
                                                                                                            0 x 13.
                                                                                                                          0x14.
                                                                                                                                                       0x16.
                                                                                                                                                                     0 \times 17
                                                                                                                                                                                   0x18.
                                                                                                                                                                                                 0 \times 19
                                                                                                                                                                                                                             0 \times 1 b
                                                                                                                                        0x15.
                                                                                                                                                                                                                0 x 1 a .
                                                                                                                                                      0 x 26
                                                                                                                                                                                   0 \times 28
                                                                                                                                                                                                               0 x 2 a
         0 x 1 c
                      0 \times 1 d
                                    0 x 1 e ,
                                                   0 x 1 f
                                                                 0 \times 20
                                                                               0 \times 21
                                                                                              0 \times 22
                                                                                                            0 \times 23
                                                                                                                          0 \times 24
                                                                                                                                        0 \times 25
                                                                                                                                                                     0 \times 27
                                                                                                                                                                                                 0 \times 29
                                                                                                                                                                                                                             0 \times 2 h
                                                   0 \times 2 f
                                                                 0 \times 30
                                                                               0 \times 31
                                                                                              0 \times 32
                                                                                                            0x33,
                                                                                                                          0 \times 34
                                                                                                                                        0 \times 35
                                                                                                                                                       0x36,
                                                                                                                                                                    0 \times 37
                                                                                                                                                                                   0 \times 38,
                                                                                                                                                                                                 0 \times 39
                                                                                                                                                                                                                              0 \times 3b
         0 x 2 c ,
                      0 x 2 d ,
                                    0 x 2 e ,
                                                                                                                                                                                                               0 \times 3a.
                                                                 0 \times 40
        0 \times 3c
                      0 \times 3d
                                    0х3е
                                                   0 \times 3 f
                                                                               0 \times 41
                                                                                              0 \times 42
                                                                                                            0 \times 43
                                                                                                                          0 \times 44
                                                                                                                                        0 \times 45
                                                                                                                                                       0 \times 46
                                                                                                                                                                     0 \times 47
                                                                                                                                                                                   0 \times 48
                                                                                                                                                                                                 0 \times 49
                                                                                                                                                                                                               0 \times 4 a
                                                                                                                                                                                                                              0 \times 4 h
                      0 \times 4d,
                                    0 x 4 e ,
                                                   0 \times 4f,
                                                                 0 \times 50,
                                                                               0x51,
                                                                                              0 \times 52,
                                                                                                            0 \times 53
                                                                                                                          0 x 54,
                                                                                                                                        0 \times 55,
                                                                                                                                                       0x56, 0x57
                                                                                                                                                                                                 0 \times 59,
         0 x 4 c ,
                                                                                                                                                                                   0x58,
                                                                                                                                                                                                               0 \times 5 a,
                                                                                                                                                                                                                             0 x 5 b
                                    0х5е,
                                                                                                                                                      0 \times 66,
                                                                                                                                                                                   0x68,
                                                                                                                                                                                                 0x69
                      0 \times 5d
                                                   0 \ge 5 \, \mathrm{f}
                                                                 0 \times 60
                                                                               0 \times 61
                                                                                              0 \times 62
                                                                                                            0 \times 63,
                                                                                                                          0 \times 64
                                                                                                                                        0 \times 65
                                                                                                                                                                    0 \times 67
                                                                                                                                                                                                               0 x 6 a
        0 \times 5 c
                                                                                                                                                                                                                             0 \times 6b
                      0 \times 6d,
                                                   0 \ge 6 \, \mathrm{f} ,
                                                                                             0 \times 72,
                                                                                                            0 \times 73,
                                                                 0 \times 70,
                                                                               0 \times 71,
                                                                                                                                        0x75,
                                                                                                                                                      0 \times 76, 0 \times 77,
                                                                                                                                                                                                 0 \times 79,
                                                                                                                                                                                                               0x7a,
                                                                                                                                                                                                                             0 x 7 b
         0x6c.
                                    0x6e,
                                                                                                                          0 \times 74,
                                                                                                                                                                                   0 \times 78,
```

```
0 \times 7 c ,
               0\,\mathrm{x7d} ,
                               0 \times 7 e
                                                                \begin{array}{c} 0 x 8 0 , \\ 0 x 9 0 , \end{array}
                                                                                 \begin{array}{c} 0 \times 81 \\ 0 \times 91 \end{array}
                                                                                                 \begin{array}{c} 0 \times 8 \, 2 \\ 0 \times 9 \, 2 \end{array}
                                                                                                                 \begin{array}{c} 0 \times 83 \ , \\ 0 \times 93 \ , \end{array}
                                                                                                                                 0 \times 84, 0 \times 94,
                                                                                                                                                  0 \times 85,
                                                                                                                                                                 0 \times 86,
0 \times 96,
                                                                                                                                                                                 0 \times 87
0 \times 97
                                                                                                                                                                                                                                   0x8a
               0 x 8 d
                                                0 x 8 f ,
                                                                                                                                                  0 \times 95
                                                                                                                                                                                                                  0 \times 99
0x8c,
                               0 x 8e,
                                                                                                                                                                                                   0x98,
                                                                                                                                                                                                                                   0 x 9 a .
                                                                                                                                                                                                                                                    0 x 9 b
0х9с,
                                                                                                                                                                  0xa6.
                                                                                                                                                                                                                                   Охаа
               0 x 9 d
                               0 x 9 e
                                                0 \times 9f,
                                                                0 \times a 0
                                                                                 0 \times a1
                                                                                                 0 \times a 2
                                                                                                                 0 \times a3
                                                                                                                                 0 \times a 4
                                                                                                                                                  0 \times a5
                                                                                                                                                                                  0 \times a7
                                                                                                                                                                                                   0xa8
                                                                                                                                                                                                                  0 \times a 9
                                                                                                                                                                                                                                                    0 vab
                                                                                                                                                                                                                   0 x b 9
                0\;x\,ad
                                0хае,
                                                 0 \times af
                                                                0\,\mathrm{ab}\,0
                                                                                 0 \times b 1
                                                                                                                 0xb3,
                                                                                                                                 0 \times b4,
                                                                                                                                                  0 \times b5
                                                                                                                                                                  0xb6,
0 xac,
                                                                                                  0 \times b 2
                                                                                                                                                                                                                                   0 \times ba
                                                                                                                                                                                                                                                    0 x b b
                                                                                                                                                                                  0 \times b7
                                                                                                                                                                                                   0xb8,
                                                                                                  0 x c 2
0 \times b c
               0 \times b d
                               0 \, \mathrm{xbe}
                                                0 \times b f
                                                                0 \times c 0
                                                                                 0 \times c 1
                                                                                                                 0 \times c3
                                                                                                                                 0 \times c 4
                                                                                                                                                  0 \times c5
                                                                                                                                                                  0 \times c6
                                                                                                                                                                                  0 x c 7
                                                                                                                                                                                                   0 \times c 8
                                                                                                                                                                                                                   0 \times c9
                                                                                                                                                                                                                                   0 \times ca
                                                                                                                                                                                                                                                    0 \times cb
                0 \ x \ c \ d
                                                                0 \times d0
                                                                                 0 \times d1
                                                                                                                 0xd3,
                                                                                                                                                                  0xd6,
                                                                                                                                                                                                   0xd8,
                                                                                                                                                                                                                                                    0xdb
0xcc,
                               0xce.
                                                 0 \times c f
                                                                                                  0 \times d2
                                                                                                                                 0 \times d4
                                                                                                                                                  0 \times d5
                                                                                                                                                                                  0 \times d7
                                                                                                                                                                                                                   0xd9
                                                                                                                                                                                                                                   0 \times da
0xdc,
               0xdd.
                               0 x d e
                                                0xdf,
                                                                0 \times e 0
                                                                                 0 \times e1
                                                                                                 0 \times e2
                                                                                                                 0 \times e3
                                                                                                                                 0 \times e4
                                                                                                                                                  0 \times e5
                                                                                                                                                                  0xe6.
                                                                                                                                                                                  0 \times e7
                                                                                                                                                                                                   0 \times e 8
                                                                                                                                                                                                                  0 \times e9
                                                                                                                                                                                                                                   0 \, \mathrm{xea}
                                                                                                                                                                                                                                                    0 xeb
                                                                                                  0 x f2
               0 \times ed
                               0 xee.
                                                 0 \times ef,
                                                                0 \times f0
                                                                                 0 \times f1
                                                                                                                 0 \times f3
                                                                                                                                 0 \times f4
                                                                                                                                                  0 \times f5
                                                                                                                                                                  0 x f6,
                                                                                                                                                                                  0 \times f7
                                                                                                                                                                                                   0xf8,
                                                                                                                                                                                                                  0 \times f9
                                                                                                                                                                                                                                   0 \times fa
0 xec,
0 \times fc
               0 \times fd
                               0 \times fe
                                                0 \times ff
                                                                0 \times 00
                                                                                 0 \times 01
                                                                                                  0 \times 02
                                                                                                                 0 \times 03
                                                                                                                                 0 \times 04
                                                                                                                                                  0 \times 05
                                                                                                                                                                  0 \times 0.6
                                                                                                                                                                                  0 \times 07
                                                                                                                                                                                                   0 \times 08
                                                                                                                                                                                                                  0 \times 09
                                                                                                                                                                                                                                   0 \times 0 a
                                                                                                                                                                                                                                                   0 \times 0 b
          SBox 13
0 \times 0 d,
               0 x 0 e ,
                                                                                                                                                                  \begin{array}{c} 0 \times 1.7 \\ 0 \times 2.7 \end{array}
                               0 \times 0 f
                                                 0 \times 10
                                                                0 \times 11
                                                                                 0 \times 12
                                                                                                  0 \times 13
                                                                                                                 0 \times 14,
                                                                                                                                 0 \times 15
                                                                                                                                                  0 \times 16
                                                                                                                                                                                  0 \times 18
                                                                                                                                                                                                   0 \times 19
                                                                                                                                                                                                                   0 \times 1 a
                                                                                                                                                                                                                                   0 \times 1 b
                                                                                                                                                                                                                                                    0 \times 1 c
                0\ge 1\ \mathrm{e}
                                                                0 \times 21
                                                                                 0 \times 22
                                                                                                                 0 \times 24,
                                                                                                                                  0 x 2 5
                                                                                                                                                                                                                   0 \times 2\,\mathrm{a} ,
                                                                                                                                                                                                                                   0 \times 2 \, \mathrm{b}
                                0 \times 1 f
                                                 0 \times 20
                                                                                                  0 \times 23
                                                                                                                                                  0 \times 26
                                                                                                                                                                                  0 \times 28
0 \times 2d
               0 \times 2e
                               0 \times 2f
                                                0 \times 30
                                                                0 \times 31
                                                                                 0 \times 32
                                                                                                 0 \times 3.3
                                                                                                                 0 \times 34
                                                                                                                                 0 \times 35
                                                                                                                                                  0 \times 36
                                                                                                                                                                  0 \times 37
                                                                                                                                                                                  0 \times 38
                                                                                                                                                                                                   0 \times 39
                                                                                                                                                                                                                  0 \times 3 a
                                                                                                                                                                                                                                   0 \times 3 b
                                                                                                                                                                                                                                                   0 \times 3c
                                                                0 x 4 1
                                                                                                                 0 x 4 4
                                                                                                                                                                                                   0 x 49
                                                                                                                                                                                                                   0 x 4 a ,
                                                                                 0 x 42
0 \times 4d, 0 \times 5d,
               0 \times 4 e
                               0 \times 4 f
                                                 0 \times 50
                                                                0 \times 51
                                                                                 0 \times 52
                                                                                                 0 \times 53
                                                                                                                 0 \times 54
                                                                                                                                 0 \times 55
                                                                                                                                                  0 \times 56
                                                                                                                                                                  0 \times 57
                                                                                                                                                                                  0 \times 58
                                                                                                                                                                                                   0 \times 59
                                                                                                                                                                                                                  0 x 5 a .
                                                                                                                                                                                                                                  0 \times 5 b
                                                                                                                                                                                                                                                    0 \times 5 c
                                                 0 \times 60
                                                                0 \times 61
                                                                                 0 \times 62
                                                                                                  0 \times 63
                                                                                                                 0 \times 64 ,
                                                                                                                                  0 \times 65
                                                                                                                                                  0 x 6 6
                                                                                                                                                                  0 \times 67
                                                                                                                                                                                  0 \times 68
                                                                                                                                                                                                   0 \times 69,
                                                                                                                                                                                                                   0х6а,
                                                                                                                                                                                                                                   0 x 6b
0x6d.
               0 x 6 e
                               0 \times 6 f
                                                0x70.
                                                                0 \times 71
                                                                                 0 \times 72
                                                                                                 0x73.
                                                                                                                 0 x 74.
                                                                                                                                 0 \times 75
                                                                                                                                                  0 \times 76
                                                                                                                                                                  0 \times 77
                                                                                                                                                                                  0 \times 78
                                                                                                                                                                                                   0x79.
                                                                                                                                                                                                                  0x7a.
                                                                                                                                                                                                                                  0 \times 7 b
                                                                                                                                                                                                                                                   0 \times 7 c
                                                                                 0 \times 82
0x8d,
               0 x 8 e
                               0 x 8 f
                                                 0 \times 90
                                                                0 \times 91
                                                                                 0 \times 92
                                                                                                  0 \times 93
                                                                                                                 0 \times 94
                                                                                                                                 0 \times 95
                                                                                                                                                  0 \times 96
                                                                                                                                                                  0 \times 97
                                                                                                                                                                                  0 \times 98
                                                                                                                                                                                                   0 \times 99
                                                                                                                                                                                                                   0x9a,
                                                                                                                                                                                                                                   0 \times 9 b
                                                                                                                                                                                                                                                    0х9с
                0х9е
                                0 \times 9 f
                                                 0 \times a 0
                                                                0 \times a 1
                                                                                 0 x a 2
                                                                                                                 0 \times a 4
                                                                                                                                  0 x a 5
                                                                                                                                                                  0 \times a7
                                                                                                                                                                                                   0 \times a9
                                                                                                                                                                                                                   Охаа,
               0 \times a.e
                               0 \times a f
                                                 0 \times b = 0
                                                                0 \times b 1
                                                                                 0 \times b 2
                                                                                                  0 \times b 3
                                                                                                                 0 \times b 4
                                                                                                                                 0 \times b5
                                                                                                                                                  0 \times b6
                                                                                                                                                                  0 \times b 7
                                                                                                                                                                                  0 \times b = 8
                                                                                                                                                                                                   0 \times b = 9
                                                                                                                                                                                                                  0xba.
                                                                                                                                                                                                                                   0 \times b b
                                                                                                                                                                                                                                                    0 \times b c
0xad.
                0 x b e
                                0 \times b f
                                                                                                                                                                                                   0 x c 9
0 xcd.
               Охсе
                               0 \times cf
                                                 0 \text{ xd} 0
                                                                0 \times d1
                                                                                 0 \times d2
                                                                                                  0 \times d3
                                                                                                                 0 \times d4
                                                                                                                                 0 \times d5
                                                                                                                                                  0 \times d6
                                                                                                                                                                  0 \times d7
                                                                                                                                                                                  0 \times d8
                                                                                                                                                                                                   0xd9.
                                                                                                                                                                                                                  0xda.
                                                                                                                                                                                                                                  0 \times db
                                                                                                                                                                                                                                                   0 \times dc
0xdd,
                                                                0 x e 1
                                                                                                                 0 x e 4
                                                                                                                                                                  0 x e 7
                0xde,
                                0 \times d f
                                                 0 \times e 0
                                                                                 0 \ge 2
                                                                                                 0 \ge 3
                                                                                                                                  0 x e 5
                                                                                                                                                                                                   0 \ge 9
                                                                                                                                                                                                                   0 \times ea,
0 xed,
               0 \, \mathrm{xee}
                               0 \times ef
                                                0 \times f0
                                                                0 \times f1
                                                                                 0 \times f2
                                                                                                  0 \times f3
                                                                                                                 0 \times f4
                                                                                                                                 0 \times f5
                                                                                                                                                  0 \times f6
                                                                                                                                                                  0 \times f7
                                                                                                                                                                                  0 \times f8
                                                                                                                                                                                                   0 \times f9
                                                                                                                                                                                                                  0xfa,
                                                                                                                                                                                                                                   0 \times fb
                                                                                                                                                                                                                                                    0 \times fc
               0 \times fe
                                                                                                  0 \times 03
                                                                                                                                                                  0 \times 07
                                                                                                                                                                                                   0 \times 09
                                                                                                                                                                                                                  0 \times 0 a,
         ŚBox
0 x 0 e ,
               0 \ge \overline{0} \ f
                                0 x 1 0
                                                                                                                                                                  0 \times 18
                                                                                                                                                                                                                   0 \times 1 b
0x1e.
                0 \times 1 f
                               0 \times 20
                                                0 \times 21
                                                                0 \times 22
                                                                                 0 \times 23
                                                                                                 0 \times 24
                                                                                                                 0 \times 25
                                                                                                                                 0 x 26.
                                                                                                                                                  0 \times 27
                                                                                                                                                                  0x28.
                                                                                                                                                                                  0 \times 29
                                                                                                                                                                                                   0 x 2a.
                                                                                                                                                                                                                  0x2b.
                                                                                                                                                                                                                                   0 \times 2 c
                                                                                                                                                                                                                                                    0 \times 2d
0 x 2 e
                0 \times 2 f
                               0 \times 30
                                                0 \times 31
                                                                0 \times 32
                                                                                 0 \times 33
                                                                                                  0 \times 34
                                                                                                                 0 \times 35
                                                                                                                                 0 \times 36
                                                                                                                                                  0 \times 37
                                                                                                                                                                  0 \times 38
                                                                                                                                                                                  0 \times 39
                                                                                                                                                                                                   0 \times 3 a
                                                                                                                                                                                                                   0 \times 3 b
                                                                                                                                                                                                                                   0 х 3 с
                                                                                                                                                                                                                                                    0 \times 3 d
0х3е,
               0 \times 3 f
                               0 \times 40
                                                 0 \times 41
                                                                0 \times 42
                                                                                 0 \times 43
                                                                                                 0 \times 44
                                                                                                                 0 \times 45
                                                                                                                                 0 \times 46
                                                                                                                                                  0 \times 47
                                                                                                                                                                  0 \times 48
                                                                                                                                                                                  0 \times 49
                                                                                                                                                                                                   0 x 4a,
                                                                                                                                                                                                                   0 \times 4 b
                                                                                                                                                                                                                                   0 \times 4 c
                                                                                                                                                                                                                                                    0 \times 4 d
                                                                                                                                                                                                   0x5a,
                                                                0 \times 52
                                                                                                                                                  0 x 5 7
                                0\ge 50
                                                 0 \times 51
                                                                                 0 \times 53
                                                                                                  0 \times 54
                                                                                                                 0 \times 55
                                                                                                                                 0 \times 56
                                                                                                                                                                  0 \times 58
                                                                                                                                                                                  0 \times 59
                                                                                                                                                                                                                   0 \times 5 b
                                                                                                                                                                                                                                   0 \times 5 c
               0 \times 5 f
                               0 \times 60
                                                0 \times 61
                                                                0 \times 62
                                                                                 0 \times 63
                                                                                                 0 \times 64
                                                                                                                 0 \times 65,
                                                                                                                                 0x66,
                                                                                                                                                  0 \times 67
                                                                                                                                                                  0x68,
                                                                                                                                                                                  0 \times 69
                                                                                                                                                                                                                  0x6b,
                                                                                                                                                                                                                                                   0 \times 6d
0 x 5 e ,
                                                                                                                                                                                                   0x6a,
                                                                                                                                                                                                                                  0 x 6 c
                                                 0 x 7 1
                                                                                                 0 x 7 4
0 x 8 4
                                                                                                                 0 x 7 5
0 x 8 5
                                                                                                                                 0\,\mathrm{x}\,7\,6
                                                                                                                                                 0 \times 77
0 \times 87
                                                                                                                                                                                  0 \times 79
                                                                                                                                                                                                                   0 \times 7 \, \mathrm{b}
                                                                                                                                                                                                                                   0 \times 7 c
0х6е,
                               0 \times 70
                                                                0 \times 72
                                                                                 0 \times 73
                                                                                                                                                                  0 \times 78
                                                                                                                                                                                                   0\,\mathrm{x}\,7\,\mathrm{a} ,
                                0 \times 80
                                                 0 \times 81
                                                                0 \times 82
                                                                                                                                                                                  0 \times 89
0x7e,
               0 \times 7 f
                                                                                 0 \times 83
                                                                                                                                 0 \times 86
                                                                                                                                                                  0x88,
                                                                                                                                                                                                   0x8a,
                                                                                                                                                                                                                   0x8b
                                                                                                                                                                                                                                   0 x 8 c
                                                                                                                                                                                                                                                    0x8d
0x8e,
               0 \times 81
                                0 \ge 90
                                                 0 \times 91
                                                                0 \times 92
                                                                                 0 \times 93
                                                                                                  0 x 9 4
                                                                                                                 0 \times 95
                                                                                                                                 0 \times 96
                                                                                                                                                  0 \times 97
                                                                                                                                                                  0 \times 98
                                                                                                                                                                                  0 \times 99
                                                                                                                                                                                                   0 x 9a ,
                                                                                                                                                                                                                   0 \times 9 b
                                                                                                                                                                                                                                   0х9с
                                                                                                                                                                                                                                                    0 \times 9 d
               0 \times 9 f
                                                0 \times a 1
                                                                0 \times a 2
                                                                                                                 0 \times a5
0 x 9 e ,
                               0 \times a 0
                                                                                 0 \times a3
                                                                                                 0 \times a 4
                                                                                                                                 0xa6,
                                                                                                                                                  0 \times a7
                                                                                                                                                                  0 xa8,
                                                                                                                                                                                  0 \times a9
                                                                                                                                                                                                   0 \times aa,
                                                                                                                                                                                                                   0xab,
                                                                                                                                                                                                                                   0 \, \mathrm{xac}
                                                                                                                                                                                                                                                    0 xad
               0 \times a f
                               0 \times b0
                                                0 \times b 1
                                                                0 \times b 2
                                                                                 0 \times b 3
                                                                                                 0 \times b 4
                                                                                                                 0 \times b5
                                                                                                                                 0\,\mathrm{x}\,\mathrm{b}\,6
                                                                                                                                                  0 \times b7
                                                                                                                                                                  0 \times b = 8
                                                                                                                                                                                  0 \times b 9
                                                                                                                                                                                                   0xba,
                                                                                                                                                                                                                   0 \times bb
                                                                                                                                                                                                                                   0 \, \mathrm{xbc}
                                                                                                                                                                                                                                                    0 \times b d
               0 \times b f
0xbe,
                                                                0 \times c 2
                                                                                                                 0 \times c5
                                                                                                                                                                  0xc8,
                                0 \times c0
                                                 0 \times c1
                                                                                 0 \times c3
                                                                                                  0 \times c 4
                                                                                                                                 0 \times c6
                                                                                                                                                  0 \times c7
                                                                                                                                                                                  0 \times c9
                                                                                                                                                                                                   0 xca,
                                                                                                                                                                                                                   0 \times cb
                                                                                                                                                                                                                                   0 \times cc
                                                                                                                                                                                                                                                    0 \times cd
               0 \times cf
                               0 \times d0
                                                 0 \times d1
                                                                0 \times d2
                                                                                 0 \times d3
                                                                                                  0 \times d4
                                                                                                                 0 \times d5
                                                                                                                                 0 \times d6
                                                                                                                                                  0 \times d7
                                                                                                                                                                  0xd8,
                                                                                                                                                                                  0 \times d9
                                                                                                                                                                                                   0xda.
                                                                                                                                                                                                                   0xdb
                                                                                                                                                                                                                                   0 \times dc
                                                                                                                                                                                                                                                    0 \times d d
               0 \times df
0xde,
                               0 \times e 0
                                                0 \times e1
                                                                0 \times e2
                                                                                 0 \times e3
                                                                                                                 0 \times e5,
                                                                                                                                 0 \times e6,
                                                                                                                                                  0 \times e7
                                                                                                                                                                  0 \times e8,
                                                                                                                                                                                  0 \times e9
                                                                                                                                                                                                                   0xeb,
                                                                                                                                                                                                                                   0 \, \mathrm{xec}
                                                                                                                                                                                                                                                   0 x e d
                                                                                                 0 x e 4
                                                                                                                                                                                                   0 xea,
               0 \times ef
                               0 \times f0
                                                0 \times f1
                                                                0 \times f2
                                                                                 0 \times f3
                                                                                                 0 \times f4
                                                                                                                 0 \times f5
                                                                                                                                 0 \times f6
                                                                                                                                                  0 \times f7
                                                                                                                                                                  0 x f8,
                                                                                                                                                                                  0 \times f9
                                                                                                                                                                                                   0 \times fa
                                                                                                                                                                                                                   0 \times fb
                                                                                                                                                                                                                                   0 \times fc
                                                                                                                                                                                                                                                   0 \times fd
0 \mathrm{\ x\ fe}
               0 \times ff
                                                                                                                                 0 \ge 0.6
                                                                                                                                                                  0 \times 08,
                                                                                                                                                                                  0 \times 09
                                                                                                                                                                                                                  0\,\mathrm{x}\,0\,\mathrm{b}
                                0 \ge 0
                                                0 \times 01
                                                                0 \ge 0.2
                                                                                 0 \times 03
                                                                                                 0 \times 04
                                                                                                                 0 \times 05
                                                                                                                                                  0 \times 07
                                                                                                                                                                                                   0 \times 0 a,
                                                                                                                                                                                                                                   0 \times 0 c
                                                                                                                                                                                                                                                   0 \times 0 \, d
          SBox_1
, 0x10
0 x 0 f ,
                                0 x 1 1
                                                 0 x 1 2
                                                                0 \times 13
                                                                                 0 \times 14
                                                                                                  0 \times 15
                                                                                                                                  0 \times 17
                                                                                                                                                  0 x 1 8
                                                                                                                                                                  0 x 19,
                                                                                                                                                                                  0 x 1a
                                                                                                                                                                                                   0x1b,
                                                                                                                                                                                                                   0 x 1 c
                                                                                                                                                                                                                                   0 \times 1 d
               0 \times 20
                               0 \times 21
                                                0 \times 22
                                                                0 \times 23
                                                                                 0 \times 24
                                                                                                 0 \times 25
                                                                                                                 0 \times 26
                                                                                                                                 0 \times 27
                                                                                                                                                  0 \times 28
                                                                                                                                                                  0 \times 29
                                                                                                                                                                                  0 \times 2a
                                                                                                                                                                                                   0 \times 2 h
                                                                                                                                                                                                                  0 \times 2c
                                                                                                                                                                                                                                   0 \times 2d
                                                                                                                                                                                                                                                    0 \times 2 e
                                                 0 \times 32
                                                                0 \times 33
                                                                                 0 \times 34
                                                                                                  0 \times 35
                                                                                                                 0 x 3 6
                                                                                                                                                  0 x 3 8
                                                                                                                                                                  0 x 3 9
                                                                                                                                                                                  0 x 3a
                                                                                                                                                                                                   0x3b,
                                                                                                                                                                                                                   0 x 3 c
                                0 \times 31
0 \times 3 f,
               0 \times 40
                               0 \times 41
                                                0 \times 42
                                                                0 \times 43
                                                                                 0 \times 44
                                                                                                 0 \times 45
                                                                                                                 0 \times 46
                                                                                                                                 0 \times 47
                                                                                                                                                  0 \times 48
                                                                                                                                                                  0 \times 49
                                                                                                                                                                                  0 \times 4 a
                                                                                                                                                                                                   0 \times 4 b.
                                                                                                                                                                                                                  0 \times 4 c
                                                                                                                                                                                                                                   0 \times 4 d
                                                                                                                                                                                                                                                   0 \times 4 e
                                                                                                                                                                                  0 x 5a,
0 x 5 f .
               0 \times 60
                               0 \times 61
                                                0 \times 62
                                                                0 \times 63
                                                                                 0 \times 64
                                                                                                 0 \times 65
                                                                                                                 0x66.
                                                                                                                                 0 \times 67
                                                                                                                                                  0 \times 68
                                                                                                                                                                  0x69.
                                                                                                                                                                                  0 \times 6a
                                                                                                                                                                                                   0x6b.
                                                                                                                                                                                                                  0 x 6 c
                                                                                                                                                                                                                                   0 \times 6 d
                                                                                                                                                                                                                                                   0 x 6 e
                                0 \ge 71
                                                                0~\mathrm{x}\,7\,3
                                                                                 0 \times 74
                                                                                                                 0 \times 76
                                                                                                                                                  0 \times 78
                                                                                                                                                                  0 \times 79
                                                                                                                                                                                  0 \times 7 a
                                                                                                                                                                                                   0x7b,
                                                                                                                                                                                                                   0 \times 7 c
                                                                                                                                                                                                                                   0 \times 7 d
               0 \times 80
                               0 \times 81
                                                 0 \times 82
                                                                0 \times 83
                                                                                 0 \times 84
                                                                                                  0 \times 85
                                                                                                                 0 \times 86
                                                                                                                                 0 \times 87
                                                                                                                                                  0 \times 88
                                                                                                                                                                  0 \times 89 .
                                                                                                                                                                                  0 x 8a
                                                                                                                                                                                                   0x8b.
                                                                                                                                                                                                                   0x8c
                                                                                                                                                                                                                                   0 \times 8d
                                                                                                                                                                  0 x 9 9
                0 \times 90
                               0 \times 91
                                                 0 x 9 2
                                                                0 \ge 93
                                                                                 0 \times 94
                                                                                                  0 x 9 5
                                                                                                                 0 x 9 6
                                                                                                                                 0 \times 97
                                                                                                                                                  0 x 9 8
                                                                                                                                                                                  0 x 9a,
                                                                                                                                                                                                   0x9b,
                                                                                                                                                                                                                   0х9с
                                                                                                                                                                                                                                   0 \times 9 d
0 \times 9 f.
               0 \times a \cdot 0
                               0 \times a.1
                                                 0 \times a.2
                                                                0 \times a.3
                                                                                 0 \times a.4
                                                                                                  0 \times a.5
                                                                                                                 0 \times a.6
                                                                                                                                 0 \times a.7
                                                                                                                                                  0xa8
                                                                                                                                                                  0 \times a.9
                                                                                                                                                                                  0 \times aa
                                                                                                                                                                                                   0 \times a \cdot b
                                                                                                                                                                                                                   0 \times ac
                                                                                                                                                                                                                                   0 \times ad
                0 \times b0
                                0 x b 1
                                                 0 x b 2
                                                                0 \times b3
                                                                                                                                                                                                   0xbb,
                                                                                                                                                                                                                   0 x b c
0xbf,
               0 \times c 0
                               0 \times c1
                                                 0 x c 2
                                                                0 \times c3
                                                                                 0 \times c4
                                                                                                  0 x c 5
                                                                                                                 0 \times c6
                                                                                                                                 0 \times c7
                                                                                                                                                  0 \times c 8
                                                                                                                                                                  0 x c 9
                                                                                                                                                                                  Охса
                                                                                                                                                                                                   0 \times cb
                                                                                                                                                                                                                   Охсс
                                                                                                                                                                                                                                   0 \times c d
                                                                                                                                                                                                                                                    0 хсе
                0 \times d0
                               0 \times d1
                                                 0 \times d2
                                                                0 \times d3
                                                                                 0\,x\,d\,4
                                                                                                  0 \times d5
                                                                                                                 0 \times d6
                                                                                                                                 0 \times d7
                                                                                                                                                  0 \times d8
                                                                                                                                                                  0 \times d9
                                                                                                                                                                                  0 \times da
                                                                                                                                                                                                   0 \times db
                                                                                                                                                                                                                   0 \, \mathrm{xdc}
                                                                                                                                                                                                                                   0 \times d d
0xdf,
               0 \times e 0
                               0 \times e1
                                                0 \times e2
                                                                0 \times e3
                                                                                 0 \times e4
                                                                                                 0 \times e5
                                                                                                                 0 xe6,
                                                                                                                                 0 \times e7
                                                                                                                                                  0 \times e 8
                                                                                                                                                                  0 \times e9,
                                                                                                                                                                                  0 \, \mathrm{xea}
                                                                                                                                                                                                   0xeb,
                                                                                                                                                                                                                  0 \, \mathrm{xec}
                                                                                                                                                                                                                                  0 \, \text{xed}.
                                                                                                                                                                                                                                                   0 \times ee
                                                                                                                                  0 x f7
                                                                                                                                                                  0 x f 9
                                0 \times f1
                                                 0 x f 2
                                                                0 \times f3
                                                                                 0 x f 4
                                                                                                  0 x f 5
                                                                                                                 0 \times f6
                                                                                                                                                                                                                   0 x fc
0 \times ff
               0 \times 00
                               0 \times 0.1
                                                0 \times 02
                                                                0 \times 03
                                                                                 0 \times 04
                                                                                                 0 \times 0.5
                                                                                                                 0 \times 06
                                                                                                                                 0 \times 0.7
                                                                                                                                                 0 \times 0.8
                                                                                                                                                                  0 \times 09.
                                                                                                                                                                                 0 \times 0 a
                                                                                                                                                                                                   0x0b.
                                                                                                                                                                                                                  0 \times 0 c
                                                                                                                                                                                                                                  0 \times 0 d.
                                                                                                                                                                                                                                                   0 \times 0 e

\begin{array}{ccc}
8 & t & \text{SI} \\
0 & x & 10 \\
0 & x & 20 \\
\end{array}

          SBox
                               0 \times 12
                                                 0 x 13.
                                                                                                  0x16.
                                                                                                                                                  0 \times 19
               0 \times 11
                                                                0 \times 14
                                                                                 0 \times 15
                                                                                                                 0 \times 17
                                                                                                                                 0 \times 18
                                                                                                                                                                  0 x 1 a .
                                                                                                                                                                                  0 x 1 b
                                                                                                                                                                                                   0 x 1 c .
                                                                                                                                                                                                                   0 \times 1 d
                                                                                                                                                                                                                                   0 \times 1 e
                                                                                                                                                                                                                                                    0 \times 1 f
               0 \times 21
                               0 \times 22
                                                0 \times 23
                                                                0 \ge 24
                                                                                 0 \ge 25
                                                                                                  0 \times 26
                                                                                                                 0 \times 27
                                                                                                                                 0 \times 28
                                                                                                                                                  0 \times 29
                                                                                                                                                                  0 x 2 a ,
                                                                                                                                                                                  0 \times 2 \, \mathrm{b}
                                                                                                                                                                                                   0 x 2 c ,
                                                                                                                                                                                                                   0\,\mathrm{x}\,2\,\mathrm{d}
                                                                                                                                                                                                                                   0 x 2 e
                                                                                                                                                                                                                                                   0 \times 2 f
                                                0 \times 33
                                                                0 \times 34
                                                                                 0 \times 35
                                                                                                                 0 \times 37
                                                                                                                                                  0 \times 39
0 \times 30,
               0 \times 31
                               0 \times 32
                                                                                                 0x36,
                                                                                                                                 0 \times 38
                                                                                                                                                                  0 x 3a,
                                                                                                                                                                                  0 \times 3 b
                                                                                                                                                                                                   0 x 3 c ,
                                                                                                                                                                                                                  0 \times 3 d
                                                                                                                                                                                                                                   0 \times 3 e
                                                                                                                                                                                                                                                   0 \times 3 f
                                                                                                                                  0 x 4 8
                                                                                                                                                  0 x 4 9
0 x 40 ,
                                0 \times 42
                                                 0 \times 43
                                                                0 \times 44
                                                                                 0 \times 45
                                                                                                                                                                                  0 \times 4 b
                                                                                                                                                                                                   0 x 4 c ,
                                                                                                                                                                                                                                   0 \times 4 e
0 \times 50 .
               0 \times 51
                               0 \times 52
                                                0 \times 53
                                                                0 \times 54
                                                                                 0 \times 55
                                                                                                 0 \times 56 .
                                                                                                                 0 \times 57
                                                                                                                                 0 \times 58
                                                                                                                                                  0 \times 59
                                                                                                                                                                  0 x 5 a .
                                                                                                                                                                                  0 \times 5 b
                                                                                                                                                                                                   0 x 5 c .
                                                                                                                                                                                                                   0x5d.
                                                                                                                                                                                                                                  0 x 5 e
                                                                                                                                                                                                                                                   0 \times 5 f
                                0 \times 62
                                                                0 \times 64
                                                                                 0 \times 65
                                                                                                  0 x 6 6
                                                                                                                                 0 \times 68
                                                                                                                                                  0 \times 69
                                                                                                                                                                                  0 \times 6 \, \mathrm{b}
                                                                                                                                                                                                                                   0 \times 6 e
0 \times 60
               0 x 6
                                                 0 \times 63
                                                                                                                 0 \times 67
                                                                                                                                                                  0х6а,
                                                                                                                                                                                                   0x6c,
                                                                                                                                                                                                                   0 \times 6 d
                                                 0 \times 73
                                                                0 \times 74
                                                                                                                 0 \times 77
0 \times 70,
               0 \times 71
                                0 \times 72
                                                                                 0 \times 75
                                                                                                  0x76,
                                                                                                                                 0 \times 78
                                                                                                                                                  0 \times 79
                                                                                                                                                                  0x7a,
                                                                                                                                                                                  0 \times 7 b
                                                                                                                                                                                                   0 x7c,
                                                                                                                                                                                                                   0 \times 7 d
                                                                                                                                                                                                                                   0 \times 7 e
                                                                                                                                                                                                                                                    0 \times 7 f
0x80,
                                                                                                                                                                                                                                   0 x 8 e
               0 \times 81
                                0 \times 82
                                                 0 \times 83
                                                                0 \times 84
                                                                                 0 \times 85
                                                                                                  0 \times 86
                                                                                                                 0 \times 87
                                                                                                                                 0x88
                                                                                                                                                  0 \times 89
                                                                                                                                                                  0 x 8 a ,
                                                                                                                                                                                  0 x 8 b
                                                                                                                                                                                                   0x8c,
                                                                                                                                                                                                                   0x8d
               0 \times 91
                                0 \ge 92
                                                                0 \ge 94
                                                                                                                                                                  0 x 9 a ,
                                                                                                                                                                                                                   0 \times 9 d
0x90,
                                                 0 \times 93
                                                                                 0 \times 95
                                                                                                  0x96,
                                                                                                                 0 \times 97
                                                                                                                                  0 \times 98
                                                                                                                                                  0 \times 99
                                                                                                                                                                                  0 x 9 b
                                                                                                                                                                                                   0x9c,
                                                                                                                                                                                                                                   0 x 9 e
                                                                                                                                                                                                                                                    0 \times 9 f
0 \times a 0
               0 x a 1
                                0 \times a 2
                                                                                 0 \times a5
                                                                                                  0 x a 6
                                                                                                                 0 \times a7
                                                                                                                                 0 x a 8
                                                                                                                                                  0 x a 9
                                                                                                                                                                  0 хаа
                                                                                                                                                                                  0 \, \mathrm{xab}
                                                                                                                                                                                                                                   0 x a e
                                                 0 \times a3
                                                                0 \times a \cdot 4
                                                                                                                                                                                                   0 \, \mathrm{xac}
                                                                                                                                                                                                                   0 x a d
                0 \times b1
                                0 \times b2
                                                                0 \times b 4
                                                                                 0 \times b 5
                                                                                                                 0 \times b7
                                                                                                                                                                  0xba,
                                                                                                                                                                                                                                                   0 \times b f
0xb0,
                                                 0 \times b3
                                                                                                  0xb6
                                                                                                                                  0 \times b8
                                                                                                                                                  0 \times b9
                                                                                                                                                                                  0 \times bb
                                                                                                                                                                                                   0 \times b c
                                                                                                                                                                                                                   0 \times bd
                                                                                                                                                                                                                                   0 \times be
0 \times c 0
                0 x c 1
                                                                                                                 0 x c 7
                                                                                                                                                                  0 x ca,
                                                                                                                                                                                                                                   Охсе
                                0 \times c2
                                                 0 \times c3
                                                                0 \times c4
                                                                                 0 \times c5
                                                                                                  0 x c 6
                                                                                                                                 0 \times c 8
                                                                                                                                                  0 \times c9
                                                                                                                                                                                  0 \times cb
                                                                                                                                                                                                   Охсс
                                                                                                                                                                                                                   0 \times c d
0xd0,
                0 \times d1
                                0 \times d2
                                                 0 \times d3
                                                                0 \times d4
                                                                                 0 \times d5
                                                                                                  0xd6
                                                                                                                 0 \times d7
                                                                                                                                  0 \times d8
                                                                                                                                                  0 \times d9
                                                                                                                                                                  0xda,
                                                                                                                                                                                  0 x d b
                                                                                                                                                                                                   0 \times dc
                                                                                                                                                                                                                   0 \times dd
                                                                                                                                                                                                                                   0 \times de
                                                                                                                                                                                                                                                    0 \times d f
                0 \times e^{1}
                                0 \times e^2
                                                 0 \times e3
                                                                0 \times e 4
                                                                                 0 \times e5
                                                                                                  0 \times e6
                                                                                                                 0 \times e^7
                                                                                                                                 0 xe8
                                                                                                                                                  0 \times e9
                                                                                                                                                                  0 \times ea
                                                                                                                                                                                  0 \, \mathrm{xeb}
                                                                                                                                                                                                                   0 \times e d
                                                                                                                                                                                                                                   0 \times ee
0 \times e 0
                                                                                                                                                                                                   0 \, \mathrm{xec}
                0 \times f1
                                                                0 \times f4
                                                                                                                                                                  0 x fa ,
                                0 \times f2
                                                 0 \times f3
                                                                                 0 \times f5
                                                                                                  0 \times f6
                                                                                                                 0 \times f7
                                                                                                                                  0 \times f8
                                                                                                                                                  0 \times f9
                                                                                                                                                                                                   0xfc.
                                                                                                                                                                                                                                   0 \times fe
                                                                                                                                                                                  0 \times fb
                                                                                                                                                                                                                   0xfd,
0 \times 0 = 0
               0 \times 0.1
                               0 \times 02
                                                0 \times 03
                                                                0 \times 04
                                                                                 0 \times 05
                                                                                                 0x06
                                                                                                                 0 \times 07
                                                                                                                                 0 \times 08
                                                                                                                                                  0 \times 09
                                                                                                                                                                  0 \times 0 a
                                                                                                                                                                                  0 \times 0 b
                                                                                                                                                                                                   0 \times 0 c
                                                                                                                                                                                                                  0x0d.
                                                                                                                                                                                                                                  0 \times 0 e
                                                                                                                                                                                                                                                   0 \ge 0 \ f
```

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	57	a1	1c	da	94	12	e4	77
00	01	00	00	00	00	00	00	9d	34	2f	27	24	04	c4	66
00	00	01	00	00	00	00	00	d2	43	05	ce	c4	18	1b	1c
00	00	00	01	00	00	00	00	8a	97	22	85	76	0d	61	26
00	00	00	00	01	00	00	00	c2	be	38	dc	11	48	1a	c8
00	00	00	00	00	01	00	00	ea	56	f4	71	70	51	fb	1f
00	00	00	00	00	00	01	00	26	94	65	c9	ca	27	b1	7e
00	00	00	00	00	00	00	01	a4	37	ab	19	f1	30	7f	2f

6 References

- $\bullet \ \ Data \ Encryption \ Standard, \ \texttt{https://en.wikipedia.org/wiki/Data_Encryption_Standard}$
- $\bullet \ \mathit{Feistel} \ \mathit{Cipher}, \ \mathtt{https://en.wikipedia.org/wiki/Feistel_cipher}$