6. Symmetric Block Cipher
BLOWFISH

BLOWFISH belongs to the same class of conventional symmetric ciphers. The basic principles of BLOWFISH have been published in 1994 by Bruce Schneier, as an alternative to the Data encryption standard (DES) to satisfy the next requirements.

1. **Performance.** The ciphering and deciphering procedures require minimal CPU time. BLOWFISH ciphers 64 bit data block based on the 32 bit microprocessor during the 18 cycle per byte.

2. Memory space. BLOWFISH requires computer memory space less than 5 Kbytes.

3. Simplicity. The structure of BLOWFISH very simple for implementation, as well as for cryptographic strength evaluation.

4. **The length of the key.** The length of the key should be enough to eliminate so called direct attack by trying to apply all possible values of keys. At the same time should allow to high rate of enciphering and deciphering procedure. That is why BLOWFISH offers variable key length. It takes value in between 32 and 448 bits. **5. The length of the data block is 64.**

BLOWFISH operates with 64 plaintext blocks and corresponding 64 ciphertext blocks. At nowadays BLOWFISH have been implemented within the numerous product and have got excellent estimates.

6. Symmetric Block Cipher
BLOWFISH
Sub keys and S-matrixes calculation

Key. BLOWFISH allows to use the key with the length from one 32 bit word K_1 up to the fourteen 32 bit words

$$K_1, K_2, \ldots, K_j,\ 1 \le j \le 14.$$

Sub Keys. Sub keys store in the ***P***-array as

$$P_1, P_2, \ldots, P_{18}.$$

S-matrixes . There are four ***S***-matrixes. Each matrix consists of 256 32-bit words

$$S_{1,0}, S_{1,1}, \ldots, S_{1,255}$$

$$S_{2,0}, S_{2,1}, \ldots, S_{2,255}$$

$$S_{3,0}, S_{3,1}, \ldots, S_{3,255}$$

$$S_{4,0}, S_{4,1}, \ldots, S_{4,255}$$

6. Symmetric Block Cipher
BLOWFISH

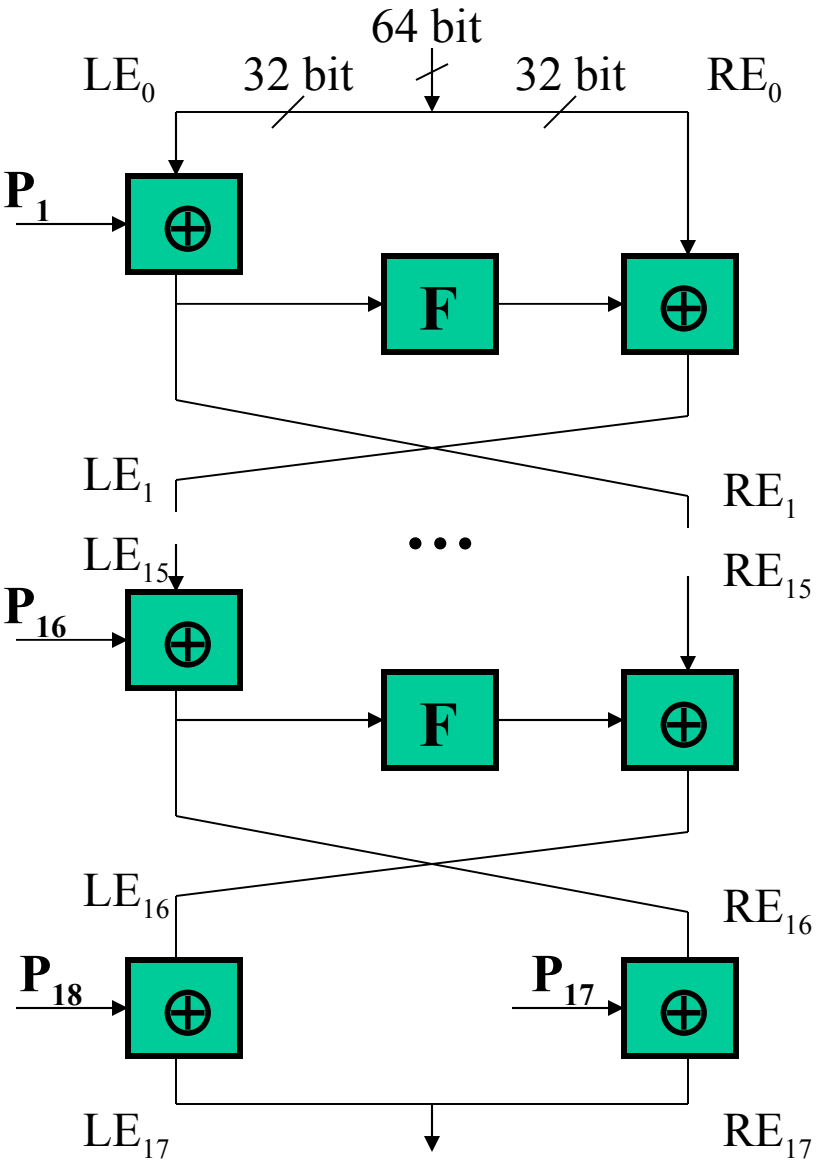
Sub keys and S-matrixes calculation Algorithm

1. For ***P***-array and ***S***-matrixes initialization the number π is used. Such a way that the P_1 equals to the first 32 bits of π the next 32 bits assigns to P_2 and so on. First of all initialization concerns the ***P***-array, then four ***S***-matrixes. For the hexadecimal notation there are P_1=243F6A88, P_2=85A308D3,…, $S_{4,254}$=57FDFE3, $S_{4,255}$=3AC372E6.

2. Bit wise XOR operation is perform between ***P***-array and ***K***-array, repeating the value of key words if necessary. For example, for the maximal length key $P_1=P_1 \oplus K_1$, $P_2=P_2 \oplus K_2,\ldots,P_{14}=P_{14} \oplus K_{14},P_{15}=P_{15} \oplus K_1,\ldots,P_{18}=P_{18} \oplus K_4$.

3. Based on the current value of ***P***- and ***K***-arrays 64 bits all zero data block is enciphering, then the 64 for ciphertext is used as a new values for P_1 and P_2, as well as plaintext data block for the next iteration. New value of ***P***- and ***K***-arrays is used for following enciphering iteration to get new values for P_3 and P_4. This procedure can be presented as $P_1,P_2=E_{P,S}[0]$, $P_3,P_4=E_{P,S}[P_1||P_2]$, $P_5,P_6=E_{P,S}[P_3||P_4],\ldots P_{17},P_{18}=E_{P,S}[P_{15}||P_{16}]$, $S_{1,0},S_{1,1}=E_{P,S}[P_{17}||P_{18}]$, $S_{1,2},S_{1,3}=E_{P,S}[S_{1,0}||S_{1,1}],\ldots,S_{4,254},S_{4,255}=E_{P,S}[S_{4,252}||S_{4,253}]$.

6. Symmetric Block Cipher
BLOWFISH



Enciphering

For i=1 ***to*** 16 ***do***

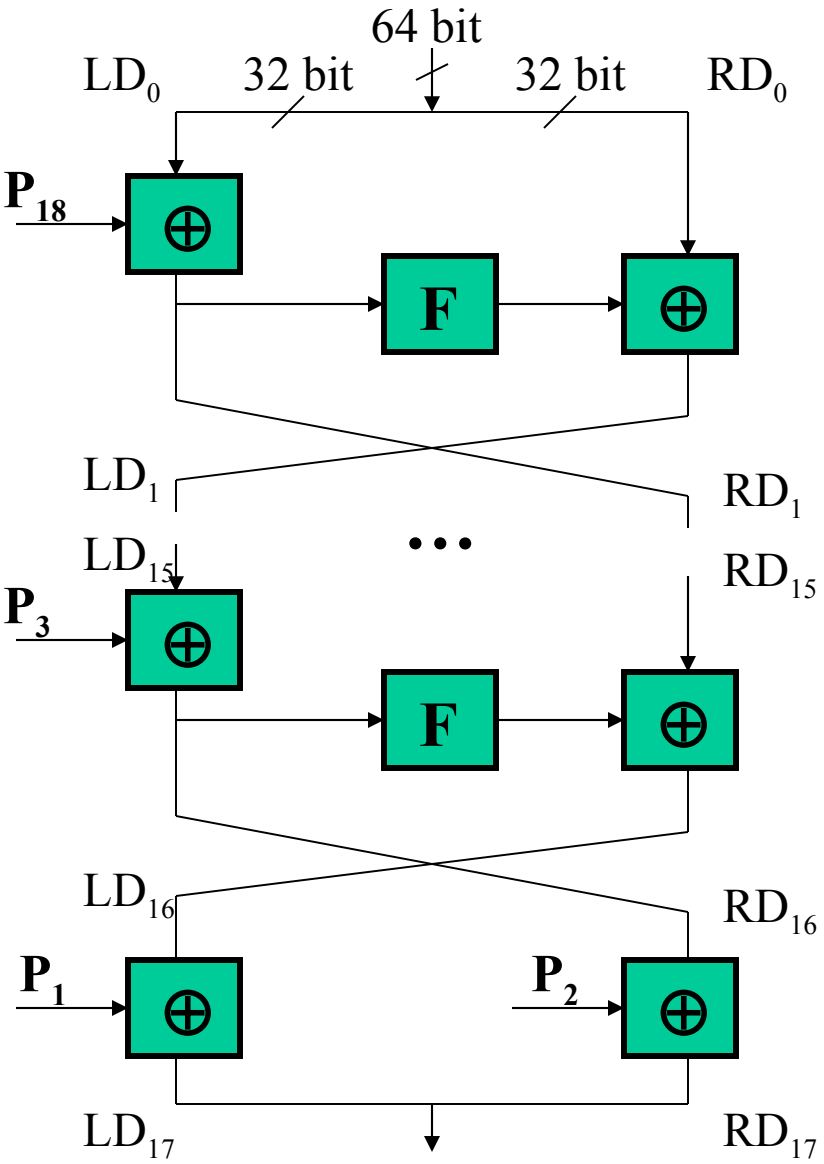
$RE_i = LE_{i-1} \oplus P_i$;

$LE_i = F[RE_i] \oplus RE_{i-1}$;

$LE_{17} = RE_{16} \oplus P_{18}$;

$RE_{17} = LE_{16} \oplus P_{17}$;

6. Symmetric Block Cipher
BLOWFISH



Deciphering

For i=1 ***to*** 16 ***do***

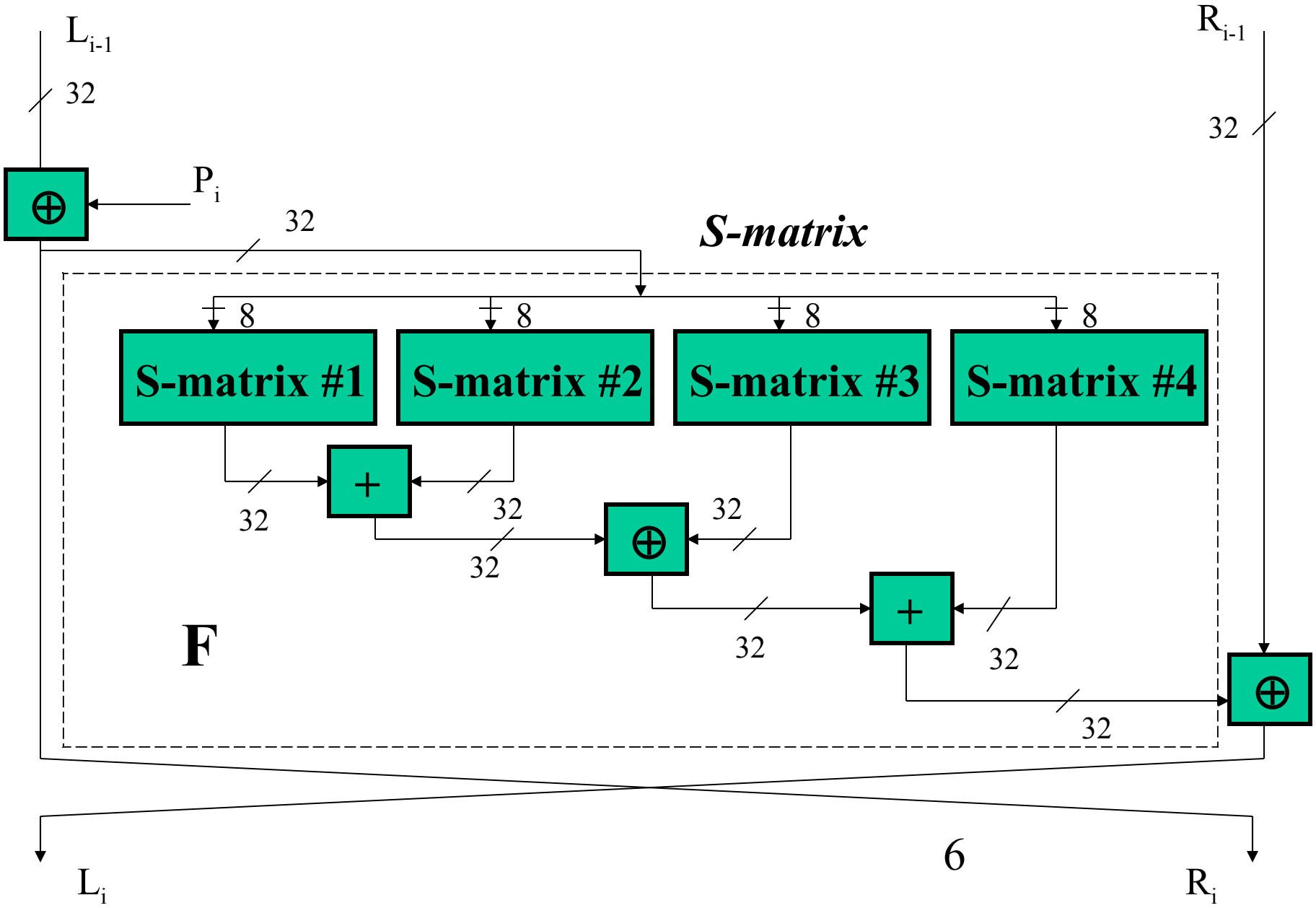
$RD_i = LD_{i-1} \oplus P_{19-i}$;

$LD_i = F[RD_i] \oplus RD_{i-1}$;

$LD_{17} = RD_{16} \oplus P_1$;

$RD_{17} = LD_{16} \oplus P_2$;

6. Symmetric Block Cipher
BLOWFISH



6. Symmetric Block Cipher BLOWFISH

There are two basic operation for BLOWFISH implementation:

+ addition by modulo 2^{16};

$\oplus$ bit wise Exclusive Or operation.

All iteration during ciphering and deciphering includes complex function ***F***, as well as substitutions defined by ***S***-matrixes.

First of all 32 bits input value is divided into four pieces ***a, b, c, d,*** 8 bits each. According to the 8 bits code and ***S***-matrix, new 32 value is generated as the output code. Four S-matrixes are generated operands for ***F*** function. General expression for this function is:

$$F(a, b, c, d)=(S_{1,a}+S_{2,b})\oplus S_{3,c}+S_{4,d}$$

6. Symmetric Block Cipher
BLOWFISH

BLOWFISH has next advantages:

1. Compare with DES algorithm ***S***-matrixes for BLOWFISH are depending on the key.

2. During each iteration there are data transformation for both part of the data block – left and right.

3. The enciphering and deciphering rate for BLOWFISH is the highest compare with classical symmetric algorithms.

Algorithm	Number of cycles for iteration	Number of iteration	Number of cycles for data block enciphering
BLOWFISH	9	16	18
DES	18	16	45
IDEA	50	8	50
Triple DES	18	48	108