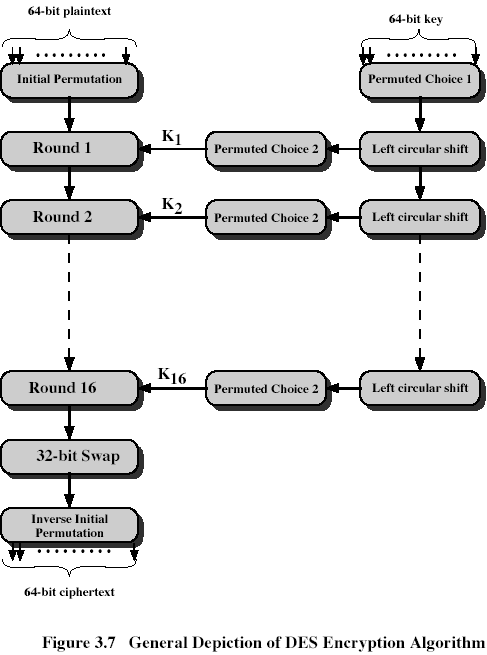
**DATA ENCRYPTION STANDARD**

It was adopted in 1977 by the National Bureau of Standards (NBS), now National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). In 1971, IBM’s team under Horst Feistel leadership developed algorithm LUCIFER, operating on 64-bit blocks with 128-bit key. Further, IBM’s team headed by Walter Tuchman and Carl Meyer revised LUCIFER to make it more resistant to cryptanalysis, but they reduced key size to 56 bits. In 1973, NBS issued a request for proposals for a national cipher standard. IBM submitted results of its Tuchman-Meyer project. This was by far the best algorithm proposed and was adopted in 1977 as Data Encryption Standard. In 1994, NIST reaffirmed DES for federal use for another 5 years. In 1999, NIST issued a new version of its standard (FIPS PUB 46-3) that indicated that DES should only be used for legacy systems and that triple DES be used. DES has Feistel structure.

**DES ENCRYPTION**



32-bit swap swaps left and 32-bit halves obtained after Round 16, we get pre-output. Finally, pre-output passes through a permutation IP-1, that is an inverse to initial permutation IP, to produce the 64-bit cipher-text. The right-hand portion of Fig. 3.7 shows the way in which 56-bit is used. For each of 16 rounds a sub-key Ki is produced by the combination of a left circular shift and a permutation. The permutation function is the same for each round.

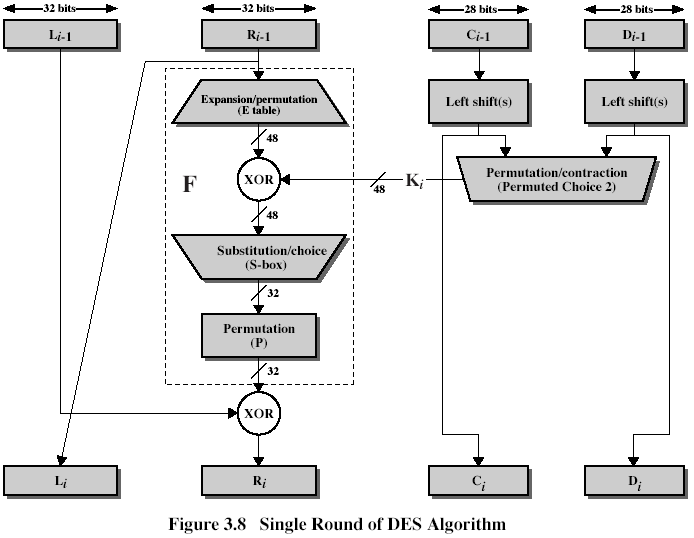
**INITIAL PERMUTATION AND ITS INVERSE**

It affects 64-bit input

|  |
| --- |
| IP |
| 58 50 42 34 26 18 10 2  60 52 44 36 28 20 12 4  62 54 46 38 30 22 14 6  64 56 48 40 32 24 16 8  57 49 41 33 25 17 9 1  59 51 43 35 27 19 11 3  61 53 45 37 29 21 13 5  63 55 47 39 31 23 15 7 |

|  |
| --- |
| IP-1 |
| 40 8 48 16 56 24 64 32  39 7 47 15 55 23 63 31  38 6 46 14 54 22 62 30  37 5 45 13 53 21 61 29  36 4 44 12 52 20 60 28  35 3 43 11 51 19 59 27  34 2 42 10 50 18 58 26  33 1 41 9 49 17 57 25 |

**DETAILS OF SINGLE ROUND**



The left and right halves of each 64-bit intermediate value are treated as separate 32-bit quantities, labeled L and R. As in the classic Feistel cipher, the overall process at each round is summarized as follows:



The round key Ki is 48 bits. The R input is 32 bits. This R input is first expanded to 48 bits by Expansion/Permutation (E table):

|  |  |  |
| --- | --- | --- |
| Expansion/Permutation (E table) | | |
| 32 | 1 2 3 4 | 5 |
| 4 | 5 6 7 8 | 9 |
| 8 | 9 10 11 12 | 13 |
| 12 | 13 14 15 16 | 17 |
| 16 | 17 18 19 20 | 21 |
| 20 | 21 22 23 24 | 25 |
| 24 | 25 26 27 28 | 29 |
| 28 | 29 30 31 32 | 1 |

**DETAILS OF SINGLE ROUND (CONT 1)**

The resulting 48 bits are XORed with Ki. This 48 bit result passes through a substitution function that produces 32-bit output, which is permuted by Permutation function (P):

|  |
| --- |
| Permutation function( P ) |
| 16 7 20 21 29 12 28 17  1 15 23 26 5 18 31 10  2 8 24 14 32 27 3 9  19 13 30 6 22 11 4 25 |

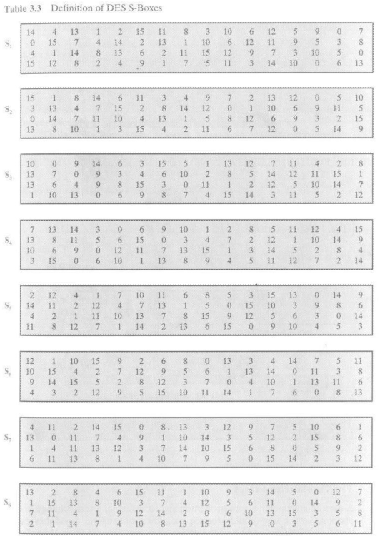
The role of S-boxes is illustrated in Fig. 3.9:



The substitution consists of a set of 8 S-boxes, each of which accepts 6 bits input and produces 4 bits as output.

**DETAILS OF SINGLE ROUND (CONT 2)**

These transformations are:



Each row of an S-box defines a general reversible substitution: middle 4 bits of each group of 6-bit input are substituted by S-box output, 1st and last 6th bits define what particular substitution out of four to use.

**KEY GENERATION**

Input key has 64 bits. But each 8th bit is not used: bits 8,16,24,32,40,48,56,64 are not further used. The 56-bit key is first subjected to permutation Permuted Choice 1:

|  |
| --- |
| Permuted Choice 1 (PC-1) |
| 57 49 41 33 25 17 9  1 58 50 42 34 26 18  10 2 59 51 43 35 27  19 11 3 60 52 44 36 |
| 63 55 47 39 31 23 15  7 62 54 46 38 30 22  14 6 61 53 45 37 29  21 13 5 28 20 12 4 |

The resulting 56-bit key is then treated as two 28-bit quantities, labeled C0 and D0. At each round, Ci-1 and Di-1 are separately subjected to a circular left shift, or rotation, of 1 or 2 bits as governed by the following:

|  |
| --- |
| Schedule of Left Shifts |
| Round number 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16  Bits rotated 1 1 2 2 2 2 2 2 1 2 2 2 2 2 2 1 |

These shifted values serve as input to the next round. They also serve as input to Permuted Choice 2, which produces a 48-bit output that serves as input to the function.

|  |
| --- |
| Permuted Choice 2 (PC-2) |
| 14 17 11 24 1 5 3 28  15 6 21 10 23 19 12 4  26 8 16 7 27 20 13 2  41 52 31 37 47 55 30 40  51 45 33 48 44 49 39 56  34 53 46 42 50 36 29 32 |

**DES DECRYPTION**

As with any Feistel cipher, decryption uses the same algorithm as encryption, except that the application of sub-keys is reversed.