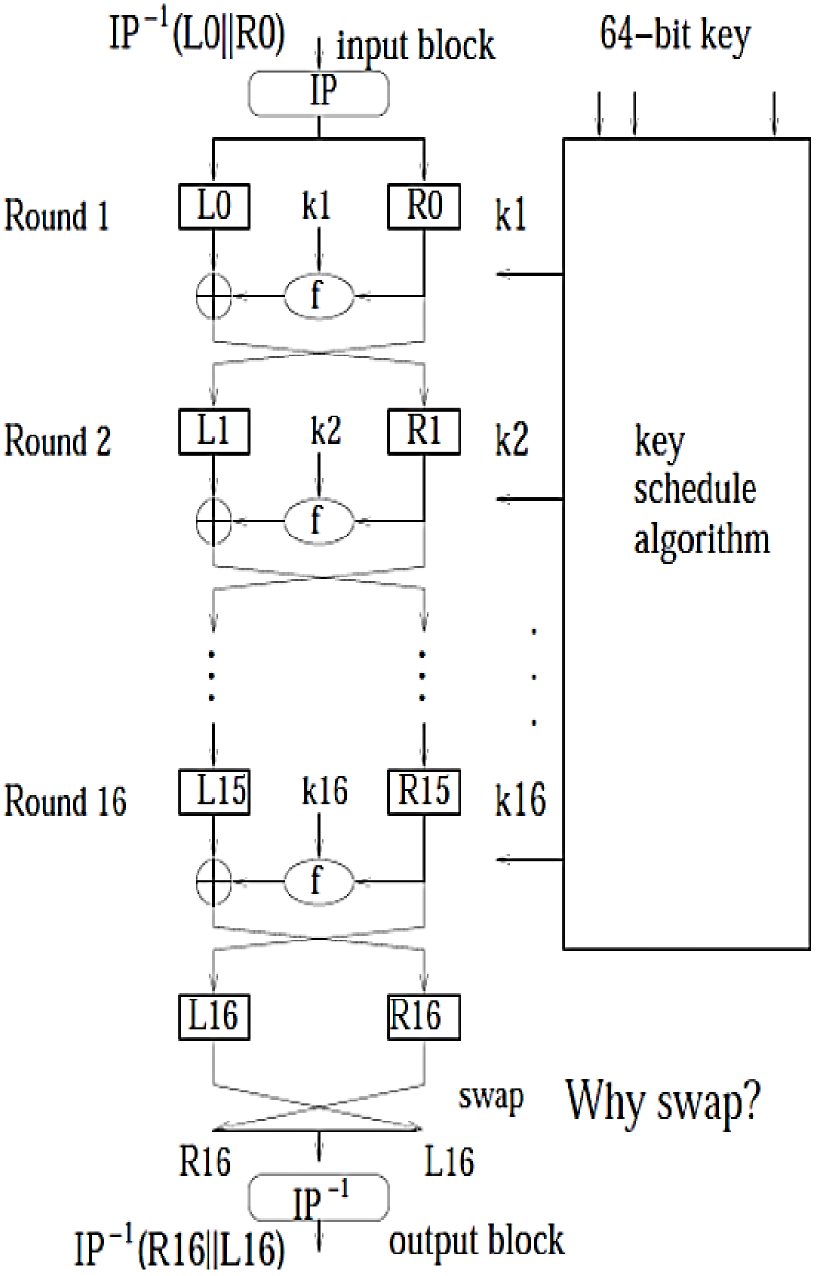
Data Encryption Standard (DES)

- A 16-round Feistel cipher with block size of 64 bits.
- Published in 1977, standardized in 1979.
- Key: 64 bit quantity = 8-bit parity+56-bit key
  - every eighth bit is used for parity checking and is ignored.
- It encrypts 64-bit data, and uses 56-bit key with 16 48-bit sub-keys.
- DES is a symmetric algorithm: The same algorithm and key are used for both encryption and decryption (except for minor differences in the key schedule).
- DES is a single combination of these techniques (a substitution followed by a permutation) on the text, based on the key.
- All security rests within the key.
- The algorithm is nothing more than a combination of the two basic techniques of encryption: **confusion** and diffusion.
  - **Diffusion** – dissipates statistical structure of plaintext over bulk of ciphertext(spreading of the effect of a change in the plaintext to many parts of the ciphertext).
  - **Confusion** – makes relationship between ciphertext and key as complex as possible (difficulty in determining how a change in the plaintext will affect the ciphertext).

DES Algorithm



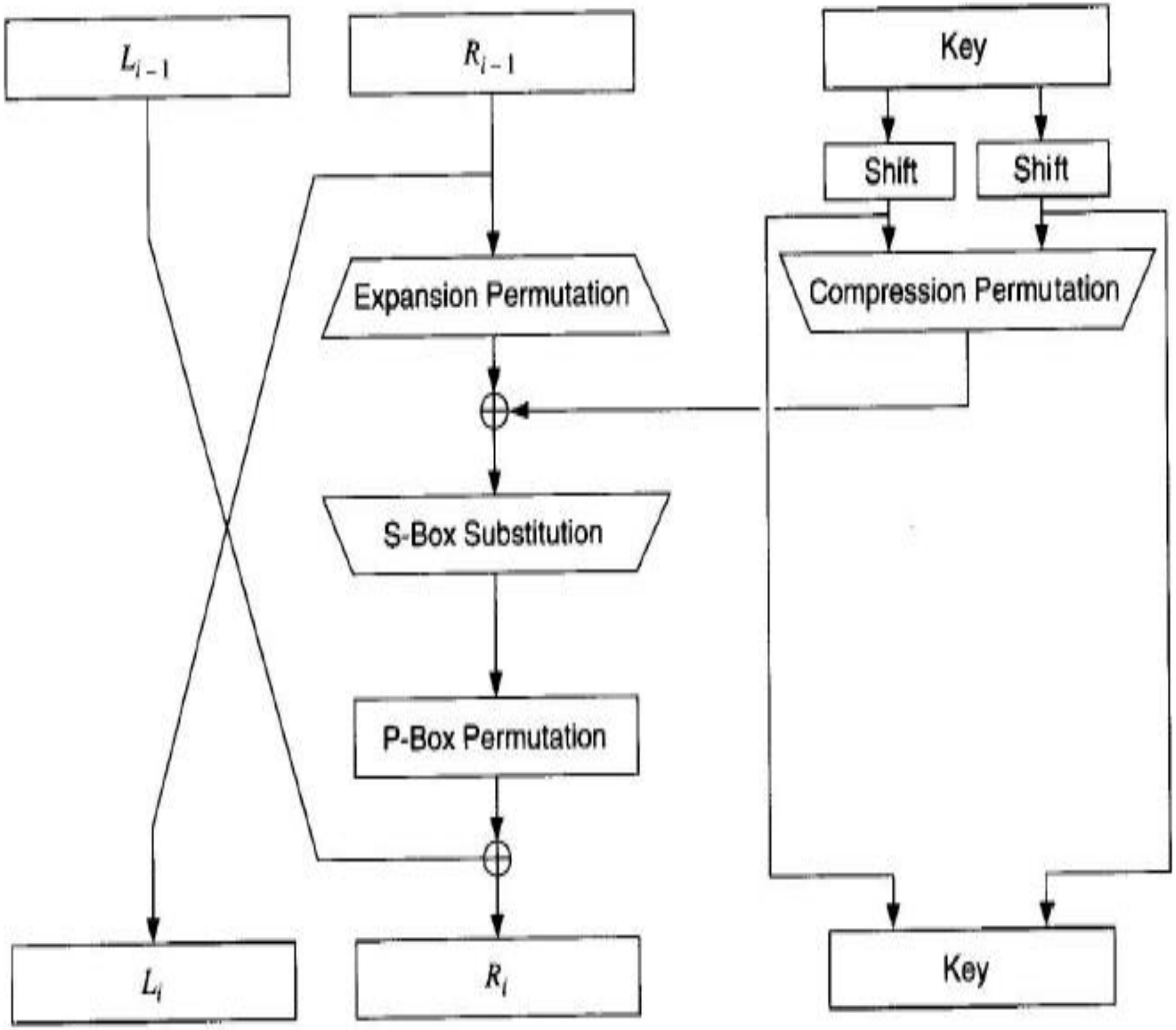
Outline of the Encryption Algorithm

- The basic process in enciphering a 64-bit data block using the DES consists of:
  - an initial permutation (IP)
  - 16 rounds of a complex key dependent calculation f
  - final permutation, being the inverse of IP
- In each round : -
  - the key bits are shifted, and then 48 bits are selected from the 56 bits of the key.
  - The right half of the data is expanded to 48 bits via an **expansion permutation**, combined with 48 bits of a shifted and permuted key via **an XOR**, sent through **8 S-boxes** producing 32 new bits, and **permuted** again.
  - These four operations make up **Function F**.
  - The output of Function F is then combined with the left half via another XOR.
  - The result of these operations becomes the new right half; the old right half becomes the new left half.
  - If Bi is the result of the ith iteration, Li and Ri are the left and right halves of Bi, Ki is the 48-bit key for round i, and F is the function that does all the substituting and permuting and XORing with the key, then a round looks like:

$$Li = R_{j-1}$$

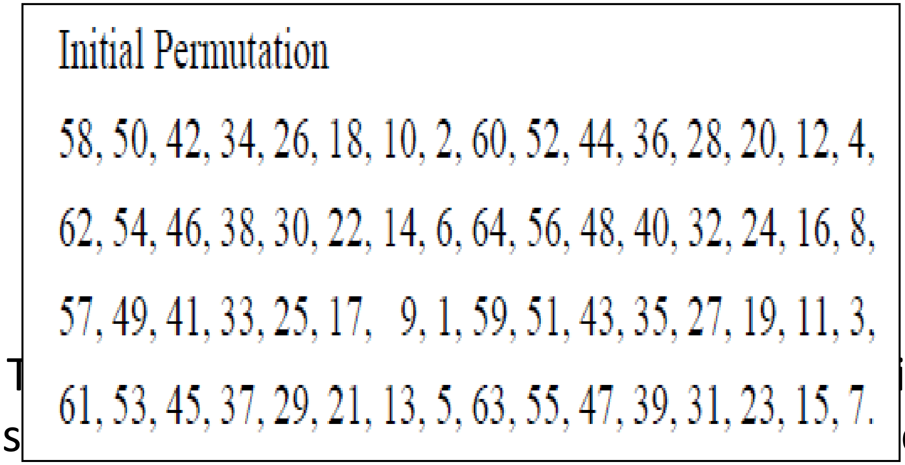
$$Ri = L_{i-1} \text{ Xor } f(R_{i-1}, K_i)$$

One round of DES



The Initial Permutation

- The initial permutation occurs before round 1.
- it transposes the input block as described in this Table



Initial Permutation

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,

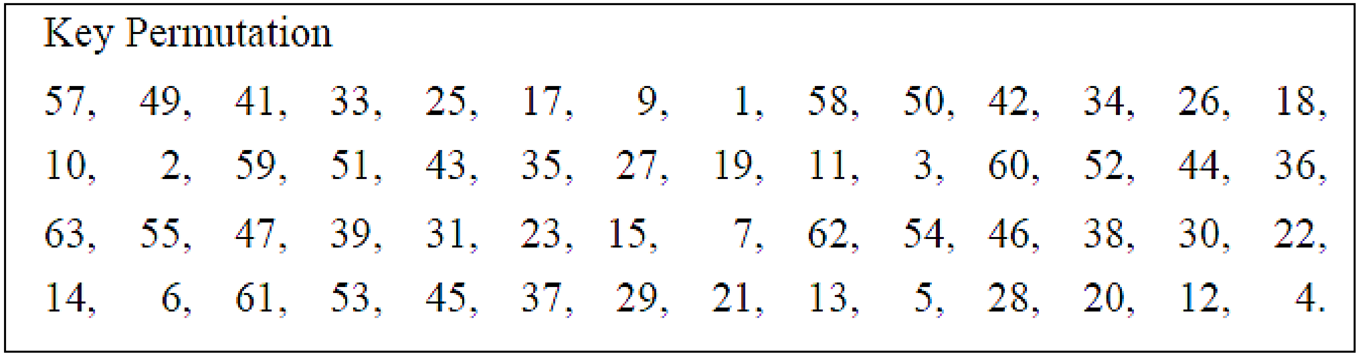
57, 49, 41, 33, 25, 17, 9, 1, 59, 51, 43, 35, 27, 19, 11, 3,

61, 53, 45, 37, 29, 21, 13, 5, 63, 55, 47, 39, 31, 23, 15, 7.

- This table T ing final permutation do not improve DES's s d be read left to right, top to bottom.
- For example, the initial permutation moves bit 58 of the plaintext to bit position 1, bit 50 to bit position 2, bit 42 to bit position 3, and so forth.
- Example: IP(675a6967 5e5a6b5a) = (ffb2194d 004df6fb)
-

The Key Transformation: -

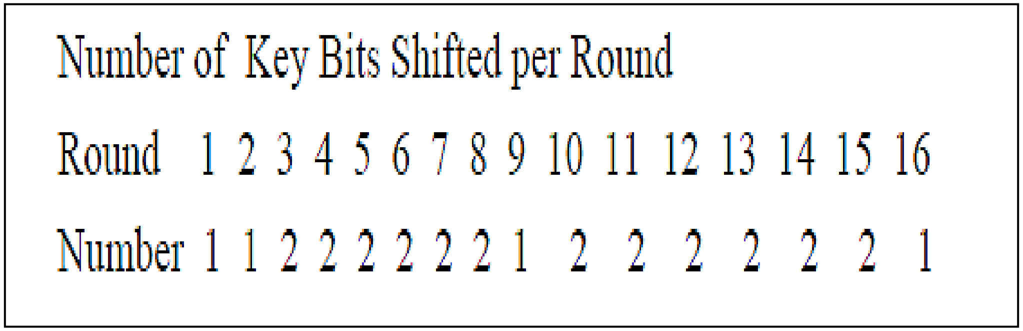
- Initially, the 64-bit DES key is reduced to a 56-bit key by ignoring every eighth bit using this table: -



Key Permutation

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.

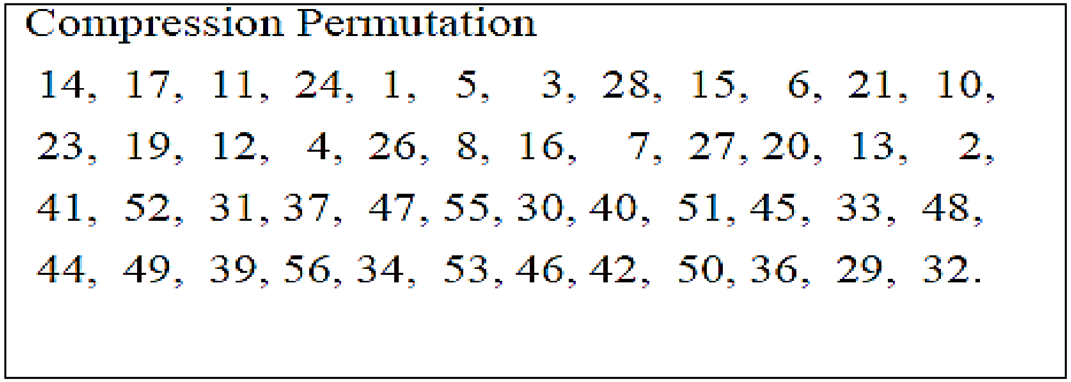
- Next the 56-bits key is reduced to a 48-bits subkey for each of the 16 rounds of DES. These subkeys, Ki, are determined in the following manner: -
  - splits the 56-bits key bits into 2 halves (C and D), each 28-bits
  - The halves C and D are circularly shifted left by either one or two bits, depending on the round. This shift is given in this table



Number of Key Bits Shifted per Round

Round	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Number	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

- After being shifted, 48 out of the 56 bits are selected. This is done by an operation called **compression permutation**, it permutes the order of the bits as well as selects a subsets of bits.



Compression Permutation

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.

- Example: keyinit(5b5a5767, 6a56676e)