**Block Ciphers and the Data Encryption Standard**

**Data Encryption Standard (DES)**

* The DES (Data Encryption Standard) algorithm is the most widely used encryption algorithm in the world.
* adopted in 1977 by NBS (now NIST)
* It is a block cipher algorithm
* DES algorithm is a variant of the Feistel algorithm

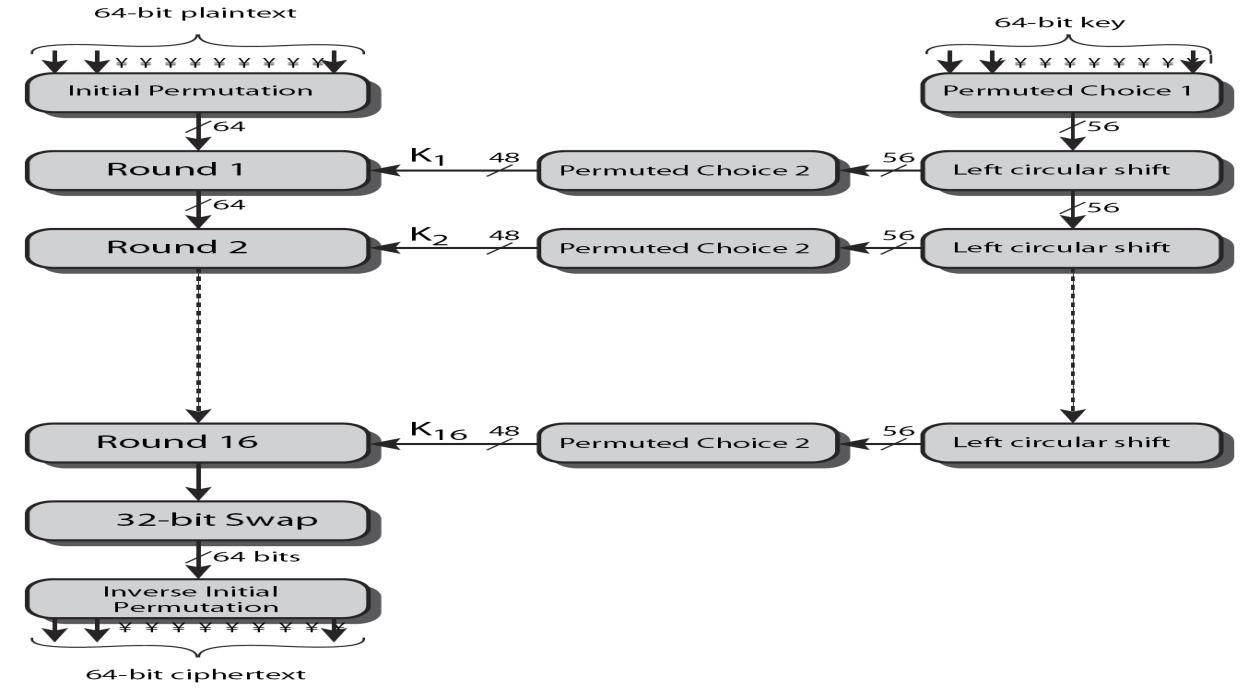
**DES History**

* IBM developed Lucifer cipher
  + by team led by Feistel in late 60’s
  + used 64-bit data blocks with 128-bit key
* then redeveloped as a commercial cipher with input from NSA and others
* in 1973 NBS issued request for proposals for a national cipher standard
* IBM submitted their revised Lucifer which was eventually accepted as the DES

**DES Features**

* encrypts 64-bit data using 56-bit key
* 16 rounds
* 16 sub-keys generated, one used in each round
* Each round performs some substitution and transformation

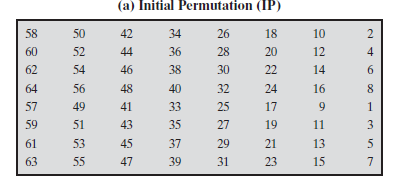
**DES Encryption Overview**

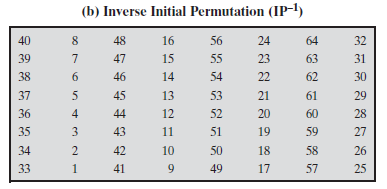


3 phases.

1. First, the 64-bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.
2. Second, a phase consisting of sixteen rounds of the same function, which involves both permutation and substitution functions.The output of the last(sixteenth) round consists of 64 bits. The left and right halves of the output are swapped to produce the preoutput.

3. Finally, the preoutput is passed through a permutation that is the inverse of the initial permutation function, to produce the 64-bit ciphertext





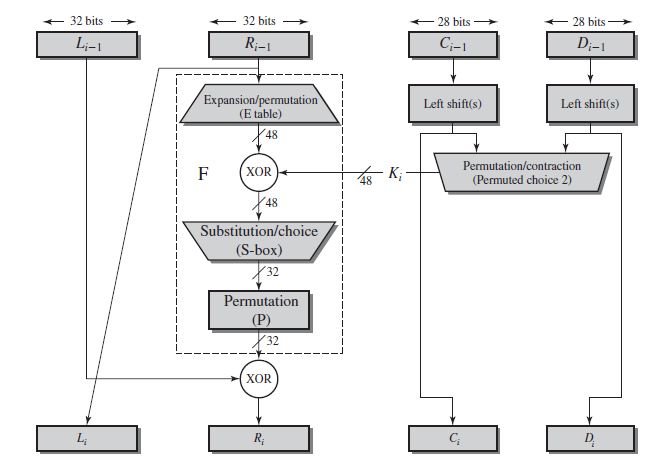
**DES Round Structure**

* uses two 32-bit L & R halves
* as for any Feistel cipher can describe as:

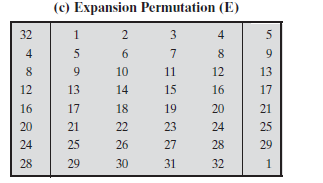
Li = Ri–1

Ri = Li–1 ⊕ F(Ri–1, Ki)

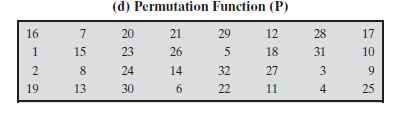
* F takes 32-bit R half and 48-bit subkey:
  + expands R to 48-bits using E-table
  + adds to subkey Ki of 48-bits using XOR
  + 48 bit output passes through 8 S-boxes to get 32-bit result
  + permutes using 32-bit P-Table
  + The The permuted output XORed with Li–1



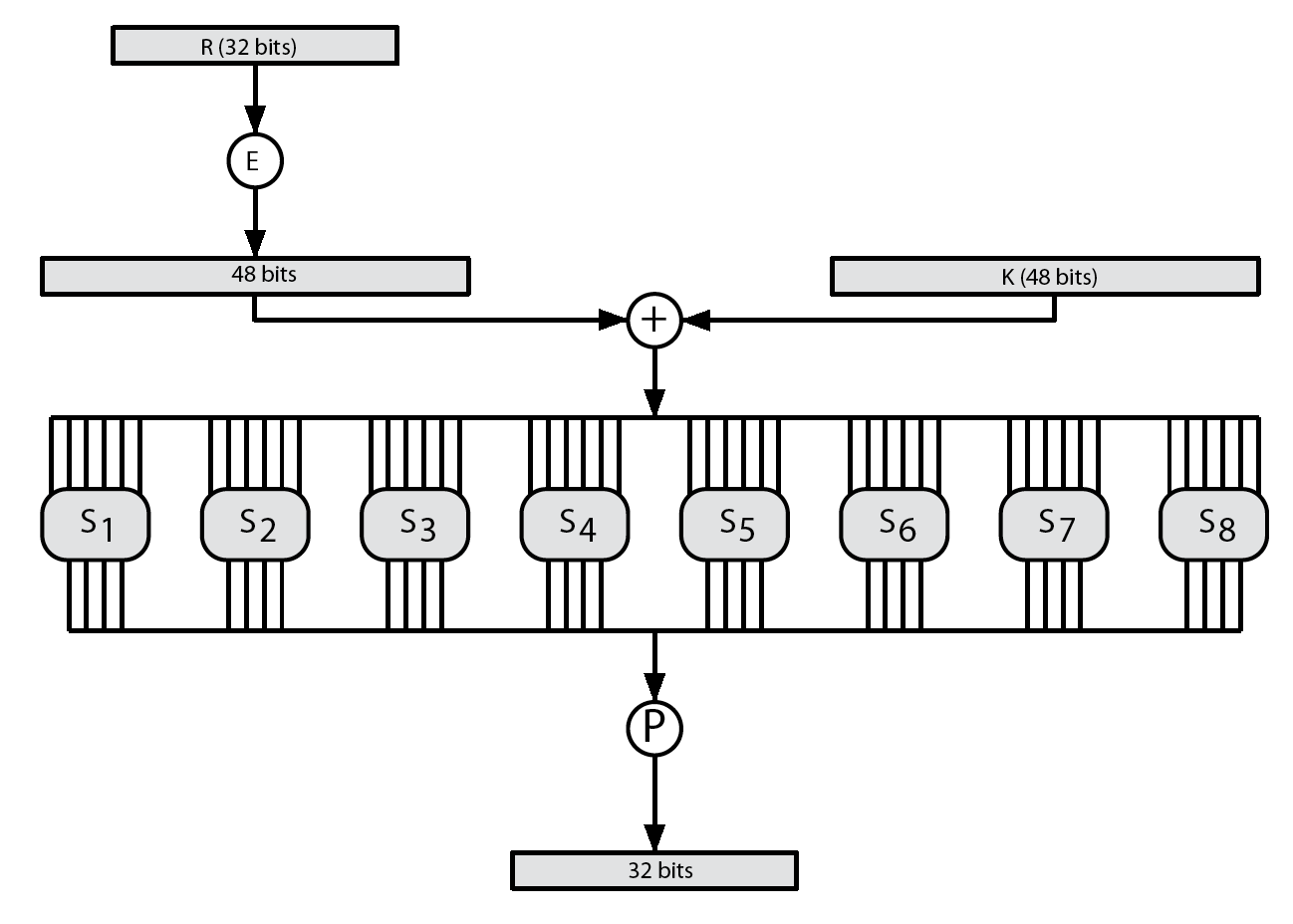
**E-Table**



**P-Table**

****

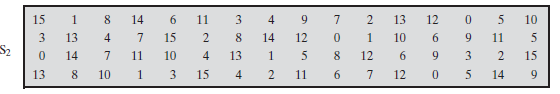
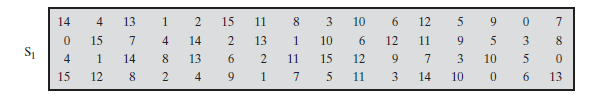
**Calculation of F(R,K)**

****

**Substitution Boxes S**

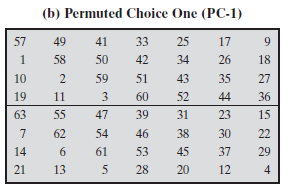
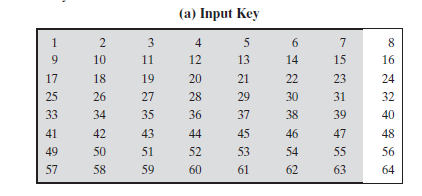
* **have eight S-boxes which map 6 to 4 bits**
* **each S-box is actually 4 little 4 bit boxes** 
  + **outer bits 1 & 6 (row bits) select one row of 4**
  + **inner bits 2-5 (col bits) are substituted**
  + **result is 8 lots of 4 bits, or 32 bits**
* **row selection depends on both data & key**
  + **feature known as autoclaving (autokeying)**

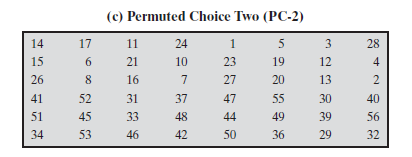
**DES S-Box**

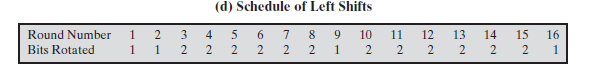
****

**DES Key Schedule**

* forms subkeys used in each round
  + initial permutation of the key (PC1) which selects 56-bits in two 28-bit halves
  + 16 stages consisting of:
    - rotating each half separately either 1 or 2 places depending on the key rotation schedule K
    - selecting 24-bits from each half & permuting them by PC2 for use in round function F







**DES Decryption**

* with Feistel design, do encryption steps again using subkeys in reverse order (SK16 … SK1)

**Avalanche Effect**

* key desirable property of encryption alg
* where a change of **one** input or key bit results in changing approx **half** output bits
* DES exhibits strong avalanche