**DES ( Data encryption standard )**

1.Encryption

64 bit key

Round 2

Left circular shift

Left circular shift

Left circular shift

Permuted choice 2

Permuted choice 2

Initial Permutation

64 bit plan text

Permuted choice 1

56 bit

56 bit

Round 1

48 bit

Key 1

Key 2

……………………………… ……………………………………..

Permuted choice 2

32 bit Swap

Inverse IP

Round 16

Key 16

1.1 IP, Inverse IP,E,P

+) 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 |

+) Inverse IP :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

+)Expansion Permutation:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 |

+) Permutation function :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

1.2) Detail of single round

32 bit 32 bit 28 bit 28bit

L

Di-1

Ci-1

R

R

S - Box

Permutation

L

32 bit

Left shift

Left shift

Expansion permutation 48 bit

Di

Ci

Permuted choice 2

Key

+) S box : 6 bit input and 4 bit output:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit | 6 bit |
| S1 | S2 | S3 | S4 | S5 | S6 | S7 | S8 |
| 4 bit | 4 bit | 4 bit | 4 bit | 4 bit | 4 bit | 4 bit | 4 bit |

6 bit input :

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 |

Bit 1 & 6 : define of the four rows in the table for Si

Bit 2 3 4 5: sixteen columns

1.3) Key generation

56 bit key input -> PC1 -> C0 & D0 : 28 bit -> cicurlar left shift ( input for the next round) -> pc2 \_> 48 bit key

+) 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 |

+)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 |

+) schedule of left shift

For round number = 1,2,9,16 : 1 bits rotated

Other : 2 bits

**AES ( Advance encryption standard )**

1.Encryption

128 bit plain text :

Overall :

128 bit plaintext-> 4x4 matrix (16 bytes)

Round 1 (4 tranformation)

Key expansion

Round N (3 tranformation)

Round 2

Pre tranformation

128 bit plain text

* 1. Detail structure

+) four stages :

Add round key

Mix columns

Shift rows

Sub bytes

Key = 16 byte – 10 rounds

24 byte – 12 rounds

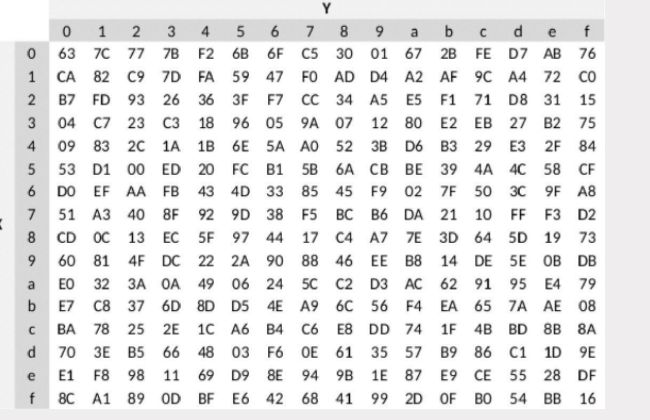
32 byte – 14 rounds

Ki

* 1. Tranformation function :

+) substitute bytes transformation

AES defines a 16 x 16 matrix of byte values called an Sbox



For 8 bit values :

* 4 bit left are used as a row value
* 4 bit right are used as a colums value

+) Shiftrows Tranformation

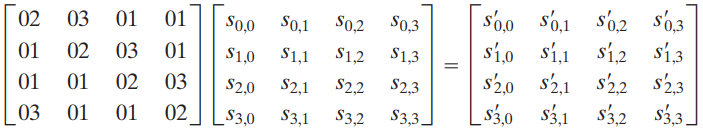
First row of state is not altered.

For second row : 1byte cicular left

For third row : 2 byte cicular left

For fourth row : 3 byte cicular left

+) MixColums Transformation



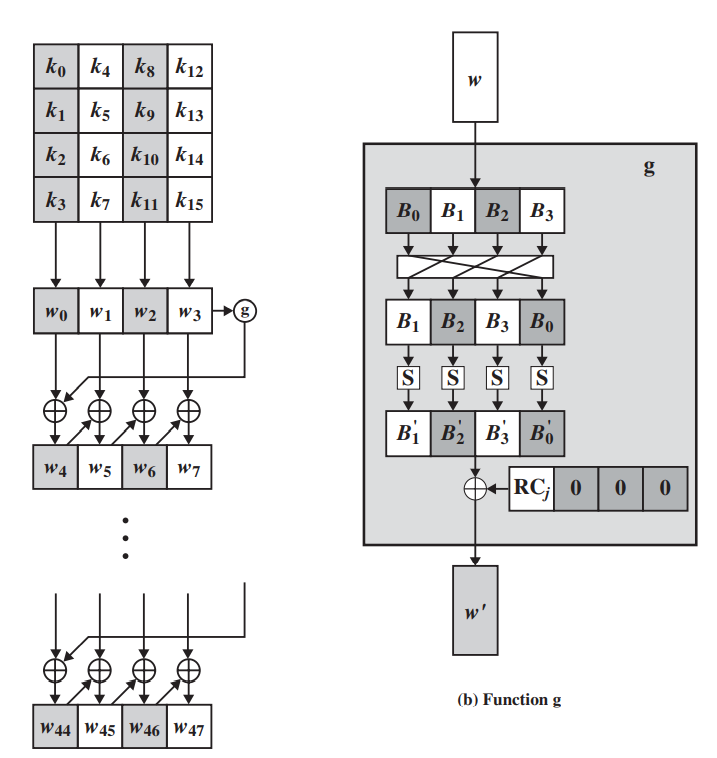
Each element in the product matrix is the sum of products of elements of one row and one column. In this case, the individual additions and multiplications5 are performed in GF(2^8 ).

Ảnh có chứa văn bản

Mô tả được tạo tự động

+) AddroundKey Transformation

* 128 bits of state are bitwise XOR with the 128 bits of the roundkey
  1. AES key expansion
* Take input 4 word ( 16 byte ) and produce linear array of 44 words ( 176 bytes)



+) RotWord : [B0,B1,B2,B3] -> [B1,B2,B3,B0]

+)Subword : using Sbox

+) Xor with a round constant Rcon[j] with Rc[1] =1 , RC[j] = 2 . RC[j-1]

Ảnh có chứa bàn

Mô tả được tạo tự động