1. DES

Expansion – ma trận mở rộng 32 bit thành 48 bit

E

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

8 hộp Sbox: đầu vào 6 bit:

* bit đầu và bít cuối xác định hàng từ 0 đến 3
* 4 bit 1, 2, 3, 4 xác định cột từ 0 đến 15

S0

14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7

0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8

4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0

15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13

S1

15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10

3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5

0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15

13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9

S2

10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8

13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1

13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7

1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12

S3

7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15

13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9

10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4

3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14

S4

2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9

14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6

4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14

11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3

S5

12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11

10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8

9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6

4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13

S6

4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1

13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6

1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2

6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12

S7

13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7

1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2

7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8

2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11

1. AES

SBOX = 0 1 2 3 4 5 6 7 8 9 a b c d e f

0 { 63 , 7c , 77 , 7b , f2 , 6b , 6f , c5 , 30 , 01 , 67 , 2b , fe , d7 , ab , 76

1 , ca , 82 , c9 , 7d , fa , 59 , 47 , f0 , ad , d4 , a2 , af , 9c , a4 , 72 , c0

2 , b7 , fd , 93 , 26 , 36 , 3f , f7 , cc , 34 , a5 , e5 , f1 , 71 , d8 , 31 , 15

3 , 04 , c7 , 23 , c3 , 18 , 96 , 05 , 9a , 07 , 12 , 80 , e2 , eb , 27 , b2 , 75

4 , 09 , 83 , 2c , 1a , 1b , 6e , 5a , a0 , 52 , 3b , d6 , b3 , 29 , e3 , 2f , 84

5 , 53 , d1 , 00 , ed , 20 , fc , b1 , 5b , 6a , cb , be , 39 , 4a , 4c , 58 , cf

6 , d0 , ef , aa , fb , 43 , 4d , 33 , 85 , 45 , f9 , 02 , 7f , 50 , 3c , 9f , a8

7 , 51 , a3 , 40 , 8f , 92 , 9d , 38 , f5 , bc , b6 , da , 21 , 10 , ff , f3 , d2

8 , cd , 0c , 13 , ec , 5f , 97 , 44 , 17 , c4 , a7 , 7e , 3d , 64 , 5d , 19 , 73

9 , 60 , 81 , 4f , dc , 22 , 2a , 90 , 88 , 46 , ee , b8 , 14 , de , 5e , 0b , db

a , e0 , 32 , 3a , 0a , 49 , 06 , 24 , 5c , c2 , d3 , ac , 62 , 91 , 95 , e4 , 79

b , e7 , c8 , 37 , 6d , 8d , d5 , 4e , a9 , 6c , 56 , f4 , ea , 65 , 7a , ae , 08

c , ba , 78 , 25 , 2e , 1c , a6 , b4 , c6 , e8 , dd , 74 , 1f , 4b , bd , 8b , 8a

d , 70 , 3e , b5 , 66 , 48 , 03 , f6 , 0e , 61 , 35 , 57 , b9 , 86 , c1 , 1d , 9e

e , e1 , f8 , 98 , 11 , 69 , d9 , 8e , 94 , 9b , 1e , 87 , e9 , ce , 55 , 28 , df

f , 8c , a1 , 89 , 0d , bf , e6 , 42 , 68 , 41 , 99 , 2d , 0f , b0 , 54 , bb , 16};

MIXCOL = { {2, 3, 1, 1},

{1, 2, 3, 1},

{1, 1, 2, 3},

{3, 1, 1, 2}};

RCON = {00, 01, 02, 04, 08, 10, 20, 40, 80, 1b, 36};

Tính từ khóa thứ i: w[i]

Temp = w[i-1], if (i%4 == 0)

{ rotWord(temp) dịch trái cả byte trong temp

temp = subBytes(temp) thế từng byte trong temp

temp = temp XOR RCON[i/4] };

w[i] = temp XOR w[i-4]