DES

Key schedule round 1

10 51 34 60 49 17 33 57 2 9 19 42

3 35 26 25 44 58 59 1 36 27 18 41

22 28 39 54 37 4 47 30 5 53 23 29

61 21 38 63 15 20 45 14 13 62 55 31

Key schedule round 2

2 43 26 52 41 9 25 49 59 1 11 34

60 27 18 17 36 50 51 58 57 19 10 33

14 20 31 46 29 63 39 22 28 45 15 21

53 13 30 55 7 12 37 6 5 54 47 23

S1 (hex)

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

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

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

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

S2 (hex)

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

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

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

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

S3 (hex)

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

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

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

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

S4 (hex)

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

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

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

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

S5 (hex)

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

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

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

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

S6 (hex)

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

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

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

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

S7 (hex)

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

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

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

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

S8 (hex)

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

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

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

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

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

**P**

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

16 7 20 21 29 12 28 17 1 15 23 26 5 18 31 10

17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

1. 8 24 14 32 27 3 9 19 13 30 6 22 11 4 25

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Bx | Sbox Equation | W | h(w) | Prob | Round Equation |
| A | 5 | X[2]⨁Y[1,2,3,4]= K[2]⨁1 | 408 | 40 | 12/64 | X[17]⨁Y[3,8,14,25]=K[26] |
| B | 1 | X[2,3,5,6]⨁Y[2]= K[2,3,5,6]⨁1 | 278 | 20 | 22/64 | X[1,2,4,5]⨁Y[17]=K[2,3,5,6] |
| C | 1 | X[4]⨁Y[2]= K[4]⨁1 | 48 | 4 | 30/64 | X[3]⨁Y[17]=K[4] |
| D | 5 | X[2]⨁Y[1,2,3]= K[2] | 108 | 20 | 42/64 | X[17]⨁Y[8,14,25]=K[26] |
| E | 5 | X[1, 5]⨁Y[1,2,3]= K[1,5]⨁1 | 228 | 32 | 16/64 | X[16,20]⨁Y[8,14,25]=K[25,29] |

Note on applying permutations: For permutations of bit positions, like P above, the table entries consisting of two rows, the top row of which is “in order” means the following. If t is above b, the bit at b is moved into position t in the permuted bit string. For example, after applying P, above, the most significant bit of the output string was at position 16 of the input string.

15R: E-DCA-ACD-DCA-A

8R: E-DAC-AB

S-Box output bit use

S[1]: 9 17 23 31

S[2]: 13 28 2 18

S[3]: 24 16 30 6

S[4]: 26 20 10 1

S[5]: 8 14 25 3

S[6]: 4 29 11 19

S[7]: 32 12 22 7

S[8]: 5 27 15 21

FEAL

G0(a,b) = (a+b (mod 256))<<< 2

G1(a,b) = (a+b+1 (mod 256))<<< 2, where “<<<” is left cyclic shift (rotation)

F(x0,x1,x2,x3) = (y0,y1,y2,y3) where

y1 = G1(x0⨁x1, x2⨁x3)

y0 = G0(x0, y1)

y2 = G0(y1, x2⨁x3)

y3 = G1(y2, x3)

X = X[0], …, X[31]), Y=F(X). Notation: X[i,j]= X[i]⨁X[j]

(a⨁b)[7] = (a+b(mod 256))[7], so G0(a,b)[5] = (a⨁b)[7]

(a⨁b⨁1)[7] = (a+b+1(mod 256))[7], so G1(a,b)[5] = (a⨁b⨁1)[7]

Since y1= G1(x0⨁x1, x2⨁x3), Y[13]=y1[5]=x0[7]⨁x1[7]⨁x2[7]⨁x3[7]⨁1=X[7,15,23,31]⨁1

Since y0=G0(x0, y1), Y[5]=y0[5]=y1[7]⨁x0[7] =Y[15]⨁X[7]

Since y2=G0(y1, x2⨁x3), Y[21]=y2[5]=y1[7]⨁x2[7]⨁x3[7] = Y[15]⨁X[23,31]

Since y3=G1(y2,x3), Y[29]=y3[5]=y2[7]⨁x3[7]⨁1= Y[23]⨁X[31]⨁1

L0= PL, R0= PL⨁PR

Y0= F(R0⨁K0), R1= L0⨁Y0, L1= R0

Y1= F(R1⨁K1), R2= L1⨁Y1, L2= R1

Y2= F(R2⨁K2), R3= L2⨁Y2, L3= R2

Y3= F(R3⨁K3)

CL= L3⨁Y3⨁K4, CR= CL⨁R3⨁K5, CL= L1⨁Y1⨁Y3⨁K4= PL⨁PR⨁Y1⨁Y3⨁K4

So CL⨁PL⨁PR⨁K4= Y1⨁Y3, CL⨁PL⨁PR⨁K4 =F(R1⨁K1)⨁F(R3⨁K3)

CL⨁PL⨁PR⨁K4 =F(L0⨁Y0⨁K1)⨁F(R3⨁K3)

Since R3 = CL⨁CR⨁K5, and L0= PL, CL⨁PL⨁PR⨁K4 = F(PL⨁Y0⨁K1)⨁F(CL⨁CR⨁K5⨁K3)

We’ve show:CL⨁PL⨁PR⨁K4 = F(PL⨁Y0⨁K1)⨁F(CL⨁CR⨁K5⨁K3),

Y0= F(R0⨁K0)=F(PL⨁PR⨁K0) , Y[13]=X[7,15,23,31]⨁1, Y[5] =Y[15]⨁X[7]

Y[21]=Y[15]⨁X[23,31], Y[29]⨁Y[23] = X[31]⨁1

From 1, (CL⨁PL⨁PR⨁K4)[23,29]= F(PL⨁Y0⨁K1)[23,29]⨁F(CL⨁CR⨁K5⨁K3)[23,29]

From 6, F(PL⨁Y0⨁K1)[23,29]= (PL⨁Y0⨁K1)[31]⨁1, F(CL⨁CR⨁K5⨁K3)[23,29]= (CL⨁CR⨁K5⨁K3)[31]⨁1

Adding 8 and 9, (CL⨁PL⨁PR⨁K4)[23,29]= (PL⨁Y0⨁K1)[31]⨁(CL⨁CR⨁K5⨁K3)[31]

(CL⨁PL⨁PR⨁K4)[23,29]= (PL⨁Y0⨁K1)[31]⨁(CL⨁CR⨁K5⨁K3)[31], so

K4[23,29]⨁(K1⨁K5⨁K3)[31]=(CL⨁PL⨁PR)[23,29]⨁PL[31]⨁Y0[31]⨁(CL⨁CR)[31]=

(CL⨁PL⨁PR)[23,29]⨁PL[31]⨁(CL⨁CR)[31]⨁ F(PL⨁PR⨁K0)[31]

The left hand side is a constant for fixed key.

The attack consists of guessing K0 and computing

h(P,C)= (CL⨁PL⨁PR)[23,29]⨁PL[31]⨁(CL⨁CR)[31]⨁F(PL⨁PR⨁K0)[31]

for a number of corresponding (PL,PR), (CL,CR). If the guessed K0 is right, h(P,C) will have the same value for each corresponding pair of plain-text and cipher-text.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| #  Rounds | # Pairs  needed | # Pairs  used | # bits  found | #  chrtstcs | P | S/N |
| 4 | 23 | 23 | 24 | 1 | 1 | 16 |
| 6 | 27 | 27 | 30 | 3 | 1/16 | 216 |
| 8 | 215 | 213 | 30 | 5 | 1/104656 | 15.6 |
| 8 | 217 | 213 | 30 | 5 | 1/104656 | 1.2 |
| 8 | 220 | 219 | 30 | 5 | 1/55000 | 1.5 |
| 9 | 225 | 224 | 30 | 6 | 10-6 | 1.0 |
| 9 | 226 | 28 | 48 | 7 | 10-24 | 223 |