

D. E. S.

q e +
+ n q
q c n
y y j
+ q
i n
n j

Security of a system
shouldn't depend on
the secrecy of the
system. Assume the
algorithm is known +
there's only a shared
secret key. (Private key/
Symmetric)

Horst Feistel - IBM

Key ideas - confusion + diffusion
substitution moving things around

Block Cipher - breaks data into 64 bit blocks
(8 bytes)

Apply Algorithm to each block

DES High Level Design

1. $P_0 = L_0 R_0 \rightarrow IP(P_0)$ apply permutation

2. for $i = 1$ to 16 :

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

} Feistel
Structure

3. $C = IP^{-1} \text{ XOR } (R_{16} L_{16})$

↑ non-linear

Best attack anyone came up with

Choose 2^{48} plaintext receive all matching CIPHERTEXT then we could set up equations + solve for the key.

NOTE Key size only 56 bits.

Going through steps in detail!

IP(P_0) moving bits around

$P_0 =$

0101	1111
1010	1000
0000	1100
1101	0111
0111	0010
1011	1111
1001	0101
1111	0000

bits 1-8 IP = 58 50 42 ...
9-16
→ 5F A8 0C ...
57-64

IP(P_0) =

10011001
11111001

→ essentially reads 2nd col backwards
→ 4th col backwards
etc. read the IP matrix

For ~~be~~ brevity I'll refer to pieces of the input in HEX not binary
need to go back & forth btw HEX binary fast.

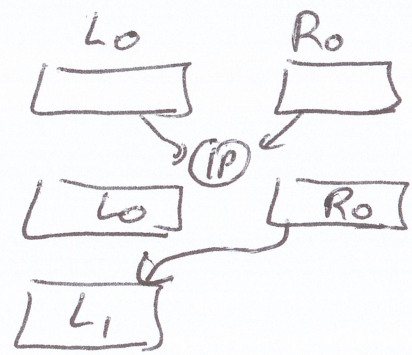
Key Steps

for $i = 1$ to $16 =$

$$L_i = R_{i-1} \quad // \text{easy}$$

$$R_i = f(R_{i-1}, K_i)$$

$$\oplus L_{i-1}$$



Function $f(R_{i-1}, K_i)$ ^{32bits 48bits} Round i key
Overall key K has 56 bits.

1. $E(R_{i-1}) \rightarrow 32 \text{ bits} \rightarrow 48 \text{ bits}$ split into

2. for i from 1 to 8: $\rightarrow 8$ 6 bit blocks $B_1, B_2, B_3, \dots, B_8$

$$C_i = S_i(B_i)$$

3. Return $P(C)$

Permutation $E(R_{i-1}) = B_1 \begin{matrix} 101110 \\ 011010 \\ 001111 \\ 101011 \\ 110010 \\ 011101 \\ 100100 \\ 001100 \end{matrix}$

$row = b_1 b_6 = 10 = 2$
 $col = b_2 b_3 b_4 b_5 = 0111 = 7$

$\rightarrow S_1[2][7] = 11$
 $\rightarrow S_2[0][13] = 0$
 $\rightarrow S_3[1][7] = 10$
 $\rightarrow S_4[3][5] = 1$
 $\rightarrow S_5[2][9] = 9$
 $\rightarrow S_6[1][14] = 3$
 $\rightarrow S_7[2][2] = 11$
 $\rightarrow S_8[0][6] = 11$

$$C(1+Ex) = 7B0A193BB$$

End 3. $C_{\text{ptor}} = 1P^{-1} (R_{16} L_{16})$