

DES function

$$f(A, J) \approx$$

$$A' = E(A)$$

$$B = A' \oplus J = b_1 b_2 \dots b_8$$

for ($i=1; i \leq 8; i++$)

$$c_i = S_i(b_i)$$

$$C = c_1 c_2 \dots c_8$$

return $P(C)$

only
non-linear
part *

⋮

S-box Criteria

P0) each row is a perm of $0, 1, \dots, 15$

P1) no S-box is a linear or affine function of its inputs.

P2) Changing 1 input bit to an S-box causes at least 2 output bits to change.

P3) For any S-box any input x , $S(x)$ and $S(x \oplus 001100)$ differ in at least 2 bits.

High Level

$$X_0 = IP(x) = L_0 R_0$$

for ($i=1; i \leq 16; i++$) {

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

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

}
return $IP^{-1}(R_{16} L_{16})$

10/4/19 (2)

P4) For any S-box, any input x ,
 and for $e, f \in \{0, 1\}$
 $S(x) \neq S(\text{~~the~~ } x \oplus 11ef00)$

$S(x) \neq S(x \oplus 110000)$
 $S(x) \neq S(x \oplus 110100)$
 $S(x) \neq S(x \oplus 111000)$
 $S(x) \neq S(x \oplus 111100)$



P5) For any S-box, if 1 input bit is fixed, and we look at one output bit, the # of 0s and 1s needs to be "pretty close" ($qbs | \#0s - \#1s | \leq 6$)

There are 32 inputs with 1 bit fixed. Consider looking at the 32 outputs of 4 bits + choosing a specific bit to look at (say bit 3), then we must have in between 13 0s and 19 0s in those 32 outputs at that position.

Key Schedule

Key is 56 bits expressed in 64 bits w/parity bits $k_8, k_{16}, k_{24}, \dots, k_{64}$ (odd parity)

k_1	k_2	k_3	\dots	k_8	11011001	$\leftarrow \text{sum}(1) = 5$
k_9	k_{10}	k_{11}	\dots	k_{16}	00011100	$\text{sum}(1) = 3$

We use the 56 bits to create 16 Round keys, K_1, K_2, \dots, K_{16} each of which are 48 bits.

$k_{57} k_{58} k_{59} \dots k_{64}$

Key Schedule Algorithm (DES) 10/4/19 (3)

(1) Permute key bits according to PC-1.

$$PC-1(K) = \begin{matrix} C_0 & D_0 \\ 28 & 28 \\ \text{bits} & \text{bits} \end{matrix}$$

(2) 16 Rounds

for $(i=1; i \leq 16; i++)$ }

$$C_i = LS_i(C_{i-1})$$

$$D_i = ~~RS~~ LS_i(D_{i-1})$$

$$K_i = PC-2(C_i D_i)$$

⋮

LS_i is a cyclic left shift of either 1 or 2 bits.

$$\text{if } i=1, 2, 9 \text{ or } 16 \quad LS_i = 1$$

$$\text{else} \quad LS_i = 2$$

$$12 \text{ rounds} \times 2 \text{ bits} + 4 \text{ rounds} \times 1 \text{ bit} = 28 \text{ bits} \quad \{K_1$$

57, 49, 41, 33, 25 ... (After Step 1)

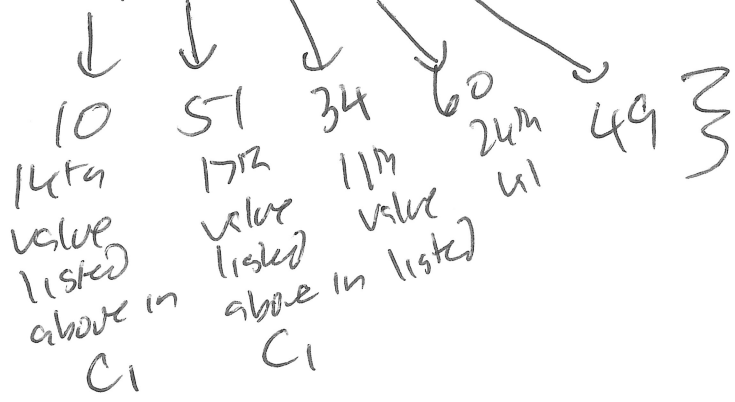
LS 1 bit on 1st 28 values :

C₁ = (49 41 33 25 44 36 57

D₁ = 55 47 39 ... (2 4 63)

PC-2 (↗)

14, 17, 11, 24, 1, 5, 3, 28



} location in the original key