# DES function

```
$f(\overset{32\text{ bits}}{A}, \overset{48\text{ bits}}{J})$ {
    $\overset{48\text{ bits}}{A'} = E(A)$
    $B = A' \oplus J = b_1 b_2 \dots b_8$
    for (i=1; i<=8; i++)
only non-linear part ← *    $\underbrace{c_i}_{4\text{ bits}} = S_i(\underbrace{b_i}_{6\text{ bits}})$
    $C = c_1 c_2 \dots c_8$
    return $P(C)$
}
```

## High Level

```
$X_0 = IP(x) = L_0 R_0$
for(i=1; i<=16; i++){
    $L_i = R_{i-1}$
    $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$
}
return $IP^{-1}(R_{16} L_{16})$
```

## S-box Criteria

P0) each row is a perm of 0,1,..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.

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

---

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

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" (abs $|\#0s - \#1s| \leq 6$)

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 ← sum(1) = 5
$K_9\ K_{10}\ K_{11} \dots K_{16}$ 00011100 sum(1) = 3
⋮
$K_{57}\ K_{58}\ K_{59} \dots K_{64}$

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

10/4/19

# Key Schedule Algorithm (DES)

① Permute key bits according to PC-1.

$$PC\text{-}1(K) = \underset{\substack{28 \\ \text{bits}}}{C_0}\ \underset{\substack{28 \\ \text{bits}}}{D_0}$$

② 16 Rounds

```
for (i=1; i<=16; i++) {
        $C_i = LS_i(C_{i-1})$
        $D_i =$ ~~RS~~ $LS_i(D_{i-1})$
        $K_i = PC\text{-}2(C_i D_i)$
}
```

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

if $i = 1, 2, 9$ or $16$ $LS_i = 1$
else $LS_i = 2$

12 rounds × 2 bits + 4 round × 1 bit = 28 bits total

10/4/19 ④

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

LS 1 bit on 1st 28 values:

$C_1$ = (49 41 33 25 .... . 44 36 57

$D_1$ = 55 47 39 .... 12 4 63)

PC-2( ↗

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

↓ ↓ ↓ ↓ ↓

10 57 34 60 49 } location in the original key

| | | | | |
|---|---|---|---|---|
| 10 | 57 | 34 | 60 | 49 |
| 14th value listed above in C1 | 17th value listed above in C1 | 11th value listed | 24th ul | |