

CIS 3362 9/26/25

DES Cont

High Level

orig
plain

1. $P_0 = L_0 R_0 = \underline{IP}(P)$

2, for i from 1 to 16:

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

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

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

32 bit 48 bit

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

1. $B = E(\overset{R_{i-1}}{\cancel{R_i}}) \oplus K_i$ (expand R_{i-1} to 48 bits then XOR w/ key)

B is 48 bits

$$B = B_1 B_2 B_3 \dots B_8 \text{ (subdivide into 6 bits blocks)}$$

2. for i from 1 to 8

$$C_i = S_i(B_i)$$

B_i is 6 bits

C_i is 4 bits

$$C = C_1 C_2 C_3 C_4 \dots C_8 \text{ (32 bits)}$$

3. Return $P(C)$

Examples

$$S_i(b_0 b_1 b_2 b_3 b_4 b_5)$$

In S-box i , look at row = $b_0 b_5$
col = $b_1 b_2 b_3 b_4$

$$S_1(\underline{10} \underline{1110}) = 11 \quad \text{row} = 10 = 2 \text{ (0-based)}$$
$$\text{col} = \underline{0111} = 7$$

$$S_3(\underline{01} \underline{1011}) = 11 \quad \text{row} = 01 = 1$$
$$\text{col} = 1101 = 13$$

$$S_6(\underline{00} \underline{0100}) = 10 \quad \text{row} = 00 = 0$$
$$\text{col} = 0010 = 2$$

S-box criteria

- P0 each row is a perm $\{0, 1, \dots, 15\}$
- 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.
- P4 for any S-box, any input x , and for bits $e, f \in \{0, 1\}$ $S(x) \oplus S(x \oplus 011ef00) \neq 0$
- P5 if you fix 1 input bit look at 1 output bit

~~the~~ each output bit must occur in between 13 and ~~19~~ 19 times.

Key Schedule

Input: K , (64 bits of which 8 are parity bits)

1. $C_0 D_0 = PC-1(K)$ \rightarrow C_0 is 28 bits
 D_0 is 28 bits

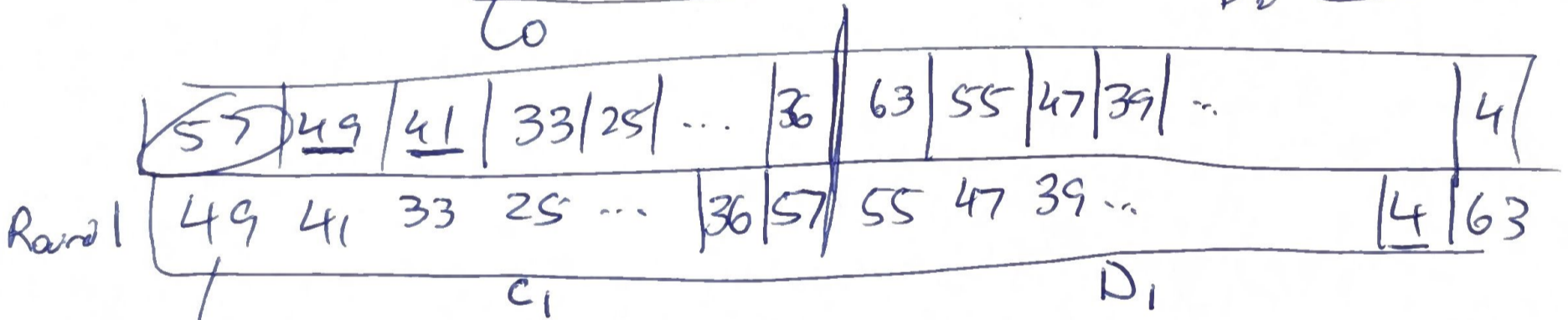
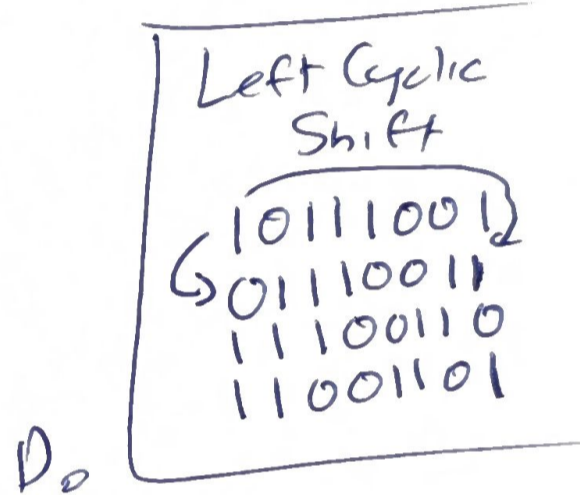
2. for i from 1 to 16:

$LS_i(B) =$
 1-bit shift
 if $i = 1, 2, 9, 12$
 else 2-bit shift

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

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

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



Round 1 key we'll grab 14th bit here, then 17th bit here, then 11th bit here

1st bit is 10th bit orig key
 2nd bit is 51st bit orig key
 3rd bit is 34th bit orig key