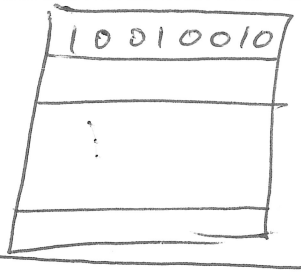
9/29/21

CIS 3362 DES

(1) Input 64 bits (Block Cipher)

typically visualized in 8×8 grid



bit #s are 1 2 3 ... 8
9 10 11 ... 16
...
57 58 ... 64

(2) Key 56 bits specified using 64 bits
8×8 grid

bits 8, 16, 24, ... 64
odd parity bit.

1 0 1 1 0 1 1 [0]
1 0 0 1 0 1 1 [1]
0 0 1 0 0 0 0 [0]
0 1 0 0 1 0 0 [1] etc.

Input $x \rightarrow IP(x) = L_0 R_0$ (32 bits, 32 bits) } run Round 1

$L_1 R_1$ } Run Round 2

$L_2 R_2$

$\downarrow$ ⋮

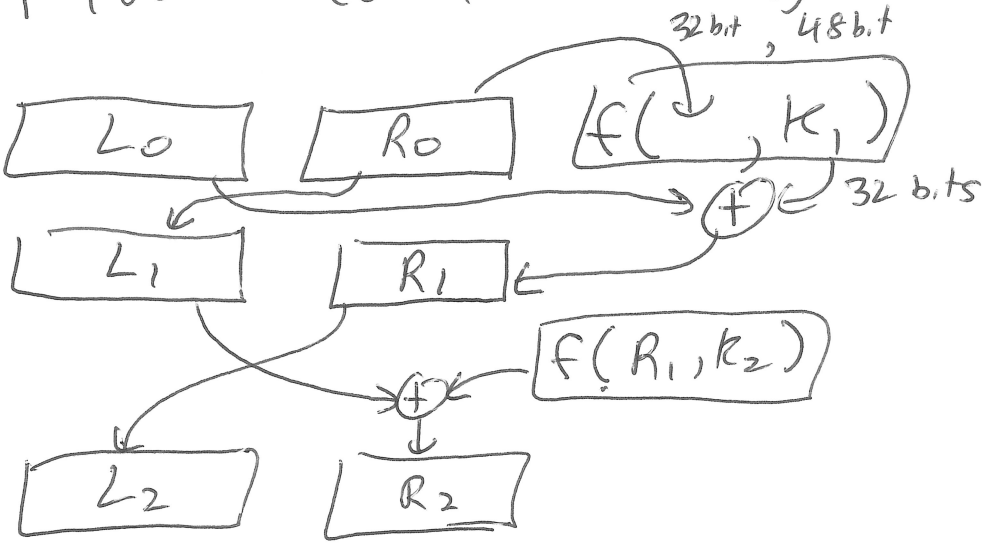
$L_{16} R_{16}$ Run 16 Rounds total

$IP^{-1}(R_{16} L_{16}) \rightarrow$ Cipher text

$X =$

1	0	1	0	1	1	1	1
0	1	1	0	1	0	0	1
0	0	0	0	1	1	1	1
1	1	1	1	0	0	0	0
0	1	1	1	0	1	1	0
1	0	1	1	1	0	1	1
1	1	0	0	0	1	0	1
1	1	0	1	1	1	1	1

$IP(x) =$ 1101 1010 (col 2 backwards)
1011 1000 (col 4 backwards)



Function (R_{i-1}, K_i)

1. $E(R_{i-1})$ to be 48 bits
2. $B = B_1 B_2 B_3 \cdots B_8 = E(R_{i-1}) \oplus K_i$ (6 bits, 6 bits, 6 bits)
3. $C = S_1(B_1) S_2(B_2) S_3(B_3) \cdots S_8(B_8)$ (4 bits)

how to calculate Sbox

$S_i(b_1 b_2 b_3 b_4 b_5 b_6)$

$= S_i[b_1 b_6][b_2 b_3 b_4 b_5]$

$S_i(101100) = S_i[10][0110]$ → 2, 6

→ In s-box i go to row 2, column 6

$S_1(101100) = 0010$ → (2) S_1 entry row 2 col 6

$S_2(110111) = 1100$, row 3, col 11

11 | 1011 → entry is S_2 row 3 col 11 (12)