CIS 3362 9/27/24

DES cont

Begin

$P_0 = L_0 R_0 = IP(P)$

Rounds

for $i = 1$ to 16

$L_i = R_{i-1}$

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

End

Round 16 $L_{16} R_{16}$

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

f (Input A (text), Input J (key round))

---

1. $E(A)$ → 32 bits to 48 bits
2. $B = E(A) \oplus J$ (xor w/ round key)
3. $B = B_1 B_2 \ldots B_8$ (split into 6 bit blocks)
4. for $i = 1$ to 8

$$C_i = S_i(B_i)$$

(C_i: 4 bits; B_i: 6 bits)

$B_i = b_1 b_2 b_3 b_4 b_5 b_6$

row $= b_1 b_6$

col $= b_2 b_3 b_4 b_5$

$S_i(B_i)$ is the entry in row $b_1 b_6$ col $b_2 b_3 b_4 b_5$

5. return $P(C)$.

$S_1(\underline{1}0101\underline{1})$ – row = 11 → 3, col = 0101 → 5, $S_1[3][5] = 9\ (1001)$

$S_4(\underline{0}1110\underline{1})$ – row = 01 → 1, col = 1110 → 14, $S_4[1][14] = 14\ (1110)$

$S_6(\underline{0}0011\underline{0})$ – row = 00 → 0, col = 0011 → 3, $S_6[0][3] = 15\ (1111)$

$S_8(\underline{1}0110\underline{0})$ – row = 10 → 2, col = 0110 → 6, $S_8[2][6] = 14\ (1110)$

S box criteria

1. Each row is a permutation of 0 to 15.
2. No s-box is a linear or affine function of its inputs.
3. Changing 1 bit in input forces at least 2 output bits to change.
4. For all x, $S(x)$ and $S(x \oplus 001100)$ differ in at least 2 bits
5. $S(x) \neq S(x \oplus 11ef00)$ for all e, f.
6. If you fix a single input bit and analyze a fixed output bit there should be "no worse than" a 13-19 split btw 0s + 1s.

Verify #5 for S_2, $x = 101100$

$x \oplus 11ef00$

$S_2(011100)$: r=0, c=14 → 5 → 0101

$S_2(011000)$: r=0, c=12 → 12 → 1100

$S_2(010100)$: r=0, c=10 → 2 → 0010

$S_2(010000)$ → r=0, c=8 → 3 → 0011

flipped 4 pos | same

$S_2(101100) = 13$ → 1101

row = 2

col = 6

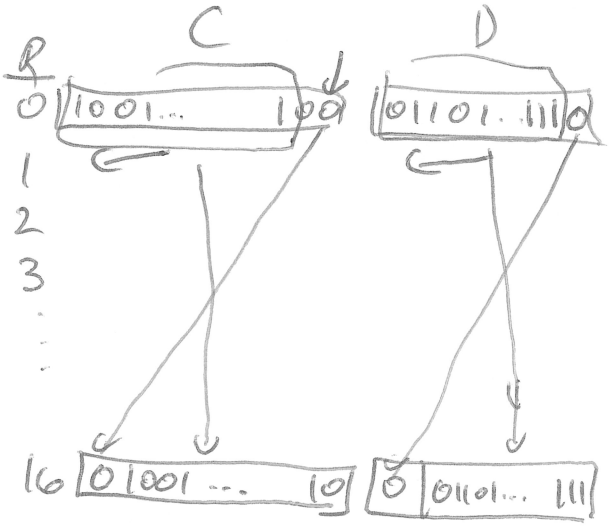
Key Schedule

Given K (56 bits w/ 8 parity bits) calculate $K_1, K_2, K_3 \ldots K_{16}$ the 16 round keys each which use 48 bits.

1. $C_0 D_0 = PC\text{-}1(K)$ → 56 bits (won't "have" bits 8, 16, 24, ...)
   - C_0: 28 bits
   - D_0: 28 bits

2. for i from 1 to 16:

$$C_i = LS_i(C_{i-1})$$
$$D_i = LS_i(D_{i-1})$$
$$K_i = PC\text{-}2(C_i D_i)$$



PC-1:

C_ϕ	~~57~~	49	41	33	25	17	9	1
	58	50	42	34	26	18	(10)	2
	59	51	43	35	27	19	11	3
	60	52	44	36	[57]	~~63~~	55	47	39
D_ϕ	31	23	15	7	62	54	46	38
	30	22	14	6	61	53	45	37
	29	21	13	5	28	20	12	4

63

PC-2: 14, 17, 11, 24, 1, 5, 3, 28, 15, 6, 21, 10, 23, 19, 12, 4

10 51 34 60 49 17 33 57 2 9 19 42 3 35 26 25