CIS 3362 9/26/25

DES Cont

High Level

orig plain
$P_o = L_o R_o = IP(P)$

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

B is 48 bits
$B = B_1 B_2 B_3 \ldots B_8$ (subdivide into 6 bit blocks

2. for i from 1 to 8 → B_i is 6 bits, C_i is 4 bits

$C_i = S_i(B_i)$

$C = C_1 C_2 C_3 C_4 \ldots C_8$ (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 $= b_1 b_2 b_3 b_4$

$S_1(1\underline{0111}1\underline{0}) = 11$, row $= 10 = 2$ (0-based)

col $= 0111 = 7$

$S_3(\underline{0}1101\underline{1}) = 11$ row $= 01 = 1$

col $= 1101 = 13$

$S_6(\underline{0}00100\underline{0}) = 10$ row $= 00 = 0$

col $= 0010 = 2$

S-box criteria

P0 each row is a perm $\{0, 1, .. 15\}$

P1 no sbox 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 $e, f \in \{0,1\}$ $S(x) \neq S(x \oplus 11ef00)$

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. $C_0 D_0 = PC\text{-}1(K)$ → C_0 is 28 bits, D_0 is 28 bits

2. for i from 1 to 16:

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

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

$K_i = PC\text{-}2(C_i D_i)$

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

Left Cyclic Shift

10111001_2
01110011
11100110
11001101

D_0

C_0

57	49	41	33	25	...	36	63	55	47	39	..	4

Round 1 | 49 41 33 25 ... | 36 | 57 | 55 47 39 .. | 4 | 63

C_1 D_1

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

1st bit is 10th bit of C_1D_1 key
2nd bit is 51st bit of C_1D_1 key
3rd bit is 34th bit of C_1D_1 key