CIS 3362 10/7/22

DES Day 2

S-box review
review function
Key generation
Look @ Code

A single S-box input = 6 bits ⇒ output = 4 bits
8 boxes labels S_1 through S_8

S_1 (bits 1-6)
S_2 (bits 7-12)
⋮
S_8 (bits 43-48)

input = $b_1 b_2 b_3 b_4 b_5 b_6$
row = $b_1 b_6$ (0-3)
col = $b_2 b_3 b_4 b_5$ (0-15)

S_1 (101110) → row = 10 (2), col = 0111 (7) → 11
S_2 (010111) → row = 01 (1), col = 1011 (11) → 10
S_3 (111101) → row = 11 (3), col = 1110 (14) → 2
S_4 (000110) → row = 00 (0), col = 0011 (3) → 3

S-box Criteria (Cryptography Theory + Practice Stinson)

P0) each row permutation 0 to 15.
P1) No S-box linear or affine function of its input.
P2) Change 1 bit of input at least 2 bits of output change.
P3) For any S-box any input x, S(x) and S(x ⊕ 001100) differ in at least 2 bits.

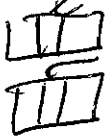
P4) For any S-box S, any input x and bits e,f, $S(x) \neq S(x \oplus 11ef00)$

P5) In any S-box, if we fix one input bit and look @ the distribution of a fixed output bit, the # of 0s + 1s will each be in between 13 and 19, inclusive

64 possible input

bit 4 = 1, input for x abclef.

Look @ output bit 2, look @ bit 2

$S(abclef) =$ 

≥ 13 zeros

≤ 19 zeros

↑ all 32 inputs

Round Review

$L_i = R_{i-1}$

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

$f(A, J)$

1. Calculate $E(A)$ 32 bits → 48 bits
2. $E(A) \oplus J$ Xor w/ key
3. Split in 8 groups of 6 bits: $B_1 \ldots B_8$
4. $S_i(B_i) \rightarrow C_i$ 48 bits → 32 bits
5. Return $P(C)$

DES Key Generation

1. $C_0 D_0 = PC\text{-}1(K)$ (permute key)

2. for $i = 1$ to 16:

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

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

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

C_0 | D_0

28 bits | 28 bits

LS = cyclic left shift (1 bit or 2 bits)

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

else $LS_i = 2$

LS 1 bit (1011010) = 0110101

LS 2 bits (1011010) = 1101010

Will show you How to get direct mappings for each round key.

PC-1 left 1/2

~~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)						

PC-2 starts 14, 17, 11, 24, 1, 5, 3, 28

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

10 51 34 60 49 17 33 57