CIS 3362 9/29/23

DES

- talk about the function f(A, J) that's in each round (S-box design)
- key schedule
- look at my code

$f(A = R_{i-1}$ 32 bits, $J = K_i$ 48 bits)

1. Calculate E(A) - expand A to 48 bits using table E (like a perm matrix)

A is HEX was 7CF63D28

0111 1100 1111 0110 0011 1101 0011 1000

E(A) = 32, 1, 2, 3, 4, 5, 4, 5

0 0 1 1 1 1 1 1 (3F is 1st byte output)

2. Calc $E(A) \oplus J$ (round key xor w/ round key

hex E(A) = 3F....

$\oplus$ J = 8C

B3

3. let Step 2 Output be $B = \underbrace{B_1}_{6 \text{ bits}} B_2 \dots B_8$

B_{hex} = B3CC0749CFD2

$B_1 = 101100$ $\qquad$ $B_5 = 010010$

$B_2 = 111100$ $\qquad$ $B_6 = 011100$

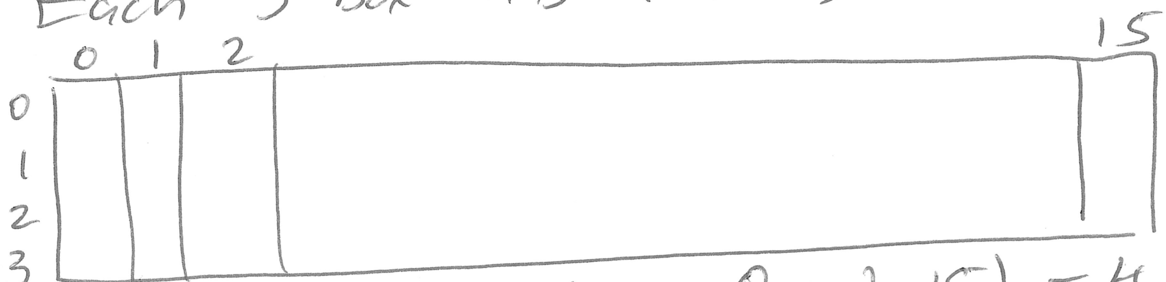
$B_3 = 110000$ $\qquad$ $B_7 = 111111$

$B_4 = 000111$ $\qquad$ $B_8 = 010010$

$C_i = \underbrace{S_i(B_i)}$

$S_1(B_1),\ S_2(B_2),\ \dots \quad S_8(B_8)$

Each S-box has 4 rows, 16 cols



outputs (values in box 0 and 15) – 4 bits

input = 6 bits $\qquad$ output = 4 bits (only non-linear component)

$B_i = b_1 b_2 b_3 b_4 b_5 b_6$ $\qquad$ $S_1(101100)$

row = $b_1 b_6$ $\qquad$ row = 10 (2)

col = $b_2 b_3 b_4 b_5$ $\qquad$ col = 0110 (6)

$S_1[2][6] = 2$ [0010]

$S_2(111100) = S_2[2][14] = 2$ [0010] $\qquad$ Output

$S_3(110000) = S_3[2][8] = 11$ [1011] $\qquad$ 15

$S_4(000111) = S_4[1][3] = 5$ [0101] $\qquad$ C

4. Return $P(C)$ {P is another perm matrix}

S-box Design

P0: each row is perm of $0, 1, 2, \ldots, 15$

P1: no s-box is a linear or affine function of its inputs.

P2: Changing one input bit to an S-box causes at least 2 output bits to change.

P3: For any Sbox and 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 $e, f \in \{0,1\}$
$$S(x) \neq S(x \oplus 11ef00)$$

P5: If we fix one input bit, and look at one output bit, there are 32 possibilities the #s of 0s and 1s in that output must be in between 13 and 19.

Alg

1. $IP(X) = L_0 R_0$
2. Run 16 rounds:

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

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

Will leave key schedule for Monday.