Name - Harsimran Singh Dhillon B-00983136

Introduction to Computer Security

CS 458/558

Assignment - 1

* Problem 1 :-

Given :- ciphertext :- QJKES REOGH GXXRF OXEO

Formula :- $c = (ap + b) \bmod 26$

where, a, p, c and b have range 0 to 25

a and b are constants

c → ciphertext

p → plaintext.

a	b	c	d	e	f	g	h	i	j
0	1	2	3	4	5	6	7	8	9

k	l	m	n	o	p	q	r	s	t
10	11	12	13	14	15	16	17	18	19

U	V	W	X	Y	Z
20	21	22	23	24	25

We are told that

plain text "t" encrypts to ciphertext "H"
and plain text "o" encrypts to ciphertext "E".

So, $p = t \ (19)$ and $p = o \ (14)$
$c = H \ (7)$ $c = E \ (4)$

Substituting these values in the formula.

$$c = (ap + b)$$
$$7 = a(19) + b \mod 26$$
$$7 = 19a + b \mod 26 \quad (1)$$

$$4 = 14a + b \mod 26 \quad (2)$$

~~Subtracting both the eq^n.~~

Subtracting both the eq^n

$$3 = (5a \ \text{[redacted]}) \mod 26$$

If we substitute $a = 11$ the eq^n will get satisfied.

$$3 = 55 \mod 26$$
$$3 = 3$$

$\therefore a = 11$

Substituting the value of a in eq. (1)

$$7 = (19 \times 11 + b) \mod 26$$

$$7 = (209 + b) \bmod 26$$

as we know that the value of b lies between 0 to 25
So adding what value of b to 209 when applied ~~to~~ modulus of 26 will give us 7.

$26 \times 8 = 208$ so we would need to add 7 to 208. to get answer as 7.

So $209 + 6 = 215$
and $215 \bmod 26 = 7$.

$\therefore b = 6$

Since we have got the values of a and b as 11 and 6 we can now use it in formula to get our plaintext.

$$C = (ap + b) \bmod 26$$

$$p = a^{-1}(C - b) \bmod 26.$$

We will use this formula to get the decrypted message.

a^{-1} for 11 mod 26 = 19. $\therefore a^{-1} = 19.$

for $C = 8$ (16) :-

$$p = 19(16 - b) \bmod 26$$
$$= 190 \bmod 26$$
$$p = 8 = I$$

lets solve for J(9)

$$p = 19(9-6) \bmod 26$$

$$= 19 \times 3 \bmod 26$$

$$= 57 \bmod 26$$

$$p = 5 = f$$

Similarly for k we will get $p = 24 = \boxed{Y}$

E, $p = 14 = \boxed{O}$

S, $p = 20 = \boxed{U}$

So the message

QIKES REOGH GXXRE OXEO

When decrypted turns out to be.

IFYOU BOWAT ALLBO WLOW

Ans "IF YOU BOW AT ALL BOW LOW".

This is the decrypted cipher message for $\boxed{a = 11}$ and $\boxed{b = 6}$.

Problem 2:-

A] $F(R_{i-1}, K_i) = 0$

Round 1:-

$L_1 = R_0$

$R_1 = L_0 \oplus 0 \neq L_0$

Round 2:-

$L_2 = R_1 = L_0 \oplus 0$

$L_2 = L_0 \oplus 0 \neq L_0$

$R_2 = L_1 \oplus 0 = R_0 \oplus 0$

$R_2 = R_0 \oplus 0 \neq R_0$

Round 3:-

$L_3 = R_2 = R_0 \oplus 0$

$L_3 = R_0 \oplus 0 = R_0$

$L_3 = R_0$

$R_3 = L_2 \oplus 0 = L_0 \oplus 0 = L_0$

$R_3 = L_0$

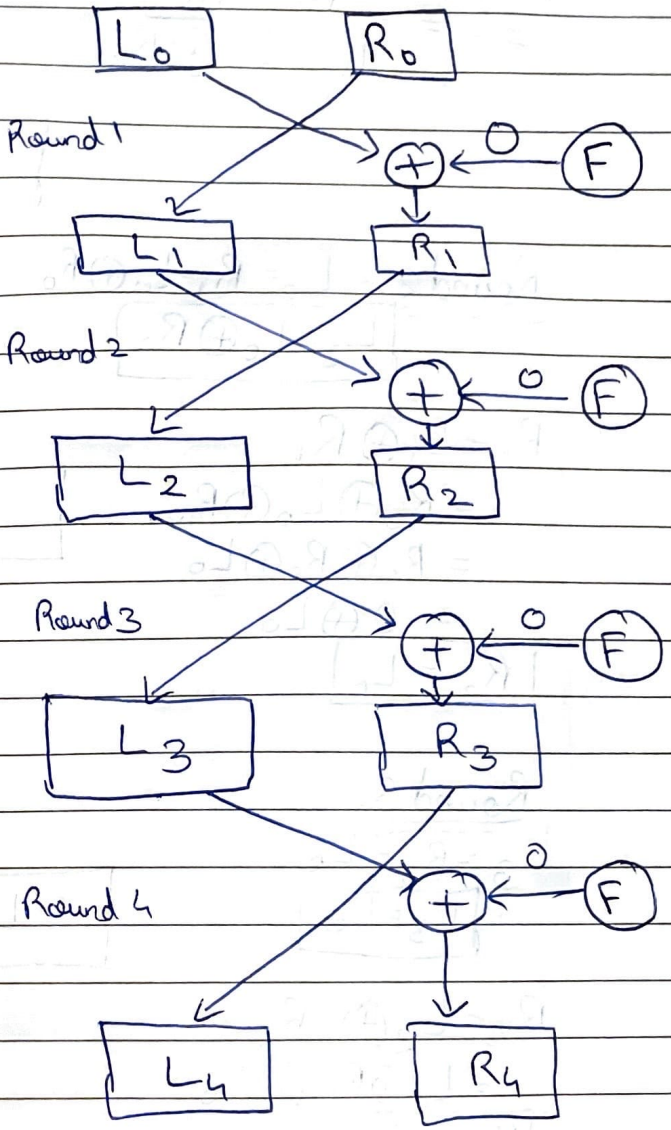
Round 4:-

$L_4 = R_3 = L_0$

$L_4 = L_0$

$R_4 = L_3 \oplus 0 = R_0$

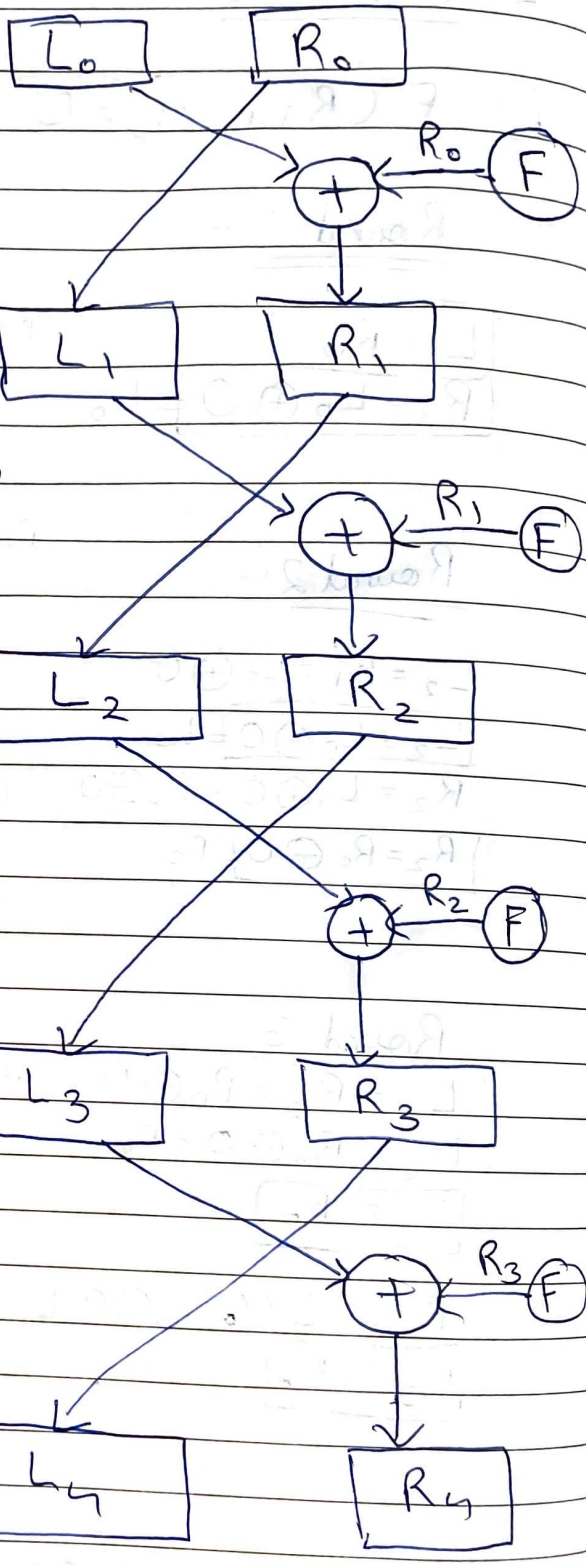
$R_4 = R_0$



We will swap L_4 & R_4

Ans After final swap $C = (R_0, L_0)$

B) $F(R_{i-1}, K_i) = R_{i-1}$



Round 1:- $\boxed{L_1 = R_0}$

$R_1 = L_0 \oplus R_0$

Round 2:- $L_2 = R_1 = L_0 \oplus R_0$

$\boxed{L_2 = L_0 \oplus R_0}$

$R_2 = L_1 \oplus R_1$

$= R_0 \oplus L_0 \oplus R_0$

$= R_0 \oplus R_0 \oplus L_0$

$= 0 \oplus L_0$

$\boxed{R_2 = L_0}$

Round 3:-

$L_3 = R_2 = L_0$

$\therefore \boxed{L_3 = L_0}$

$R_3 = L_2 \oplus R_2$

$= L_0 \oplus R_0 \oplus L_0$

$\boxed{R_3 = R_0}$

Round 4:-

$L_4 = R_3 = R_0$

$\therefore \boxed{L_4 = R_0}$

$R_4 = L_3 \oplus R_3$

$\therefore \boxed{R_4 = L_0 \oplus R_0}$

We will swap R_4 & L_4

Ans After final swap $C = (L_0 \oplus R_0, R_0)$

c) $F(R_{i-1}, K_i) = K_i$

Round 1:-

$L_1 = R_0$

$R_1 = L_0 \oplus K_1$

Round 2:-

$L_2 = R_1 = L_0 \oplus K_1$

$\boxed{L_2 = L_0 \oplus K_1}$

$R_2 = L_1 \oplus K_2 = R_0 \oplus K_2$

$\boxed{R_2 = R_0 \oplus K_2}$

Round 3:-

$L_3 = R_2 = R_0 \oplus K_2$

$R_3 = L_2 \oplus K_3 = L_0 \oplus K_1 \oplus K_3$

$\boxed{L_3 = R_0 \oplus K_2}$ $\boxed{R_3 = L_0 \oplus K_1 \oplus K_3}$

Round 4:-

$L_4 = R_3$

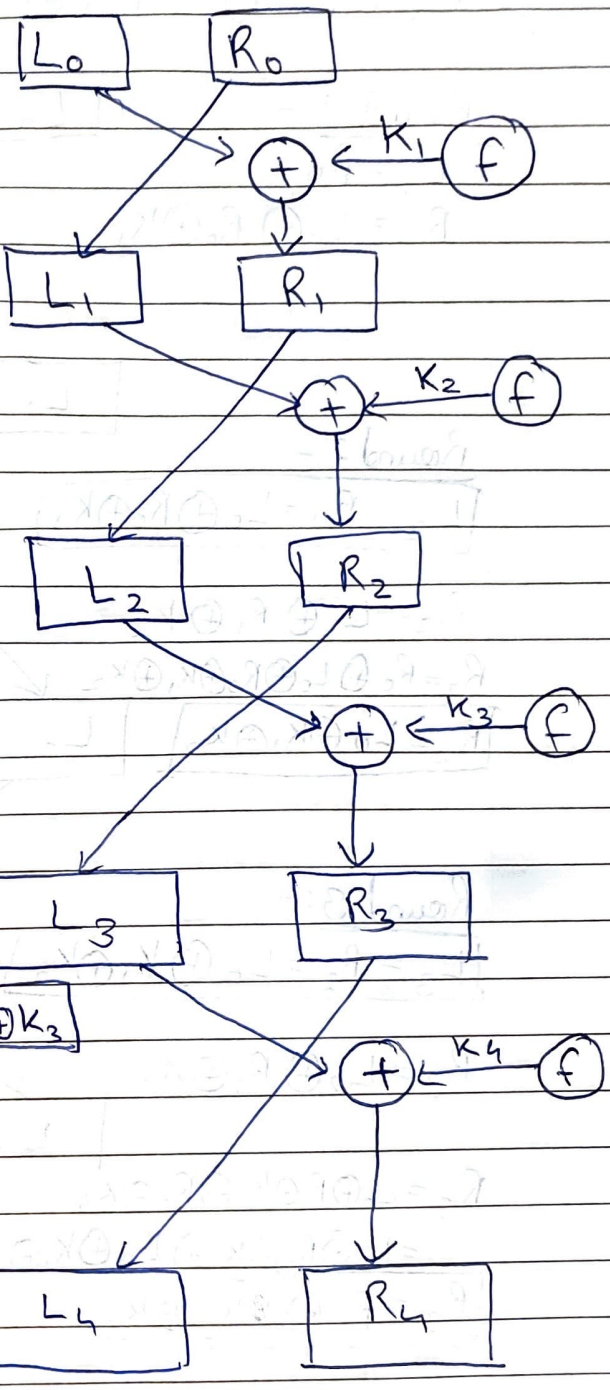
$\boxed{L_4 = L_0 \oplus K_1 \oplus K_3}$

$R_4 = L_3 \oplus K_4$

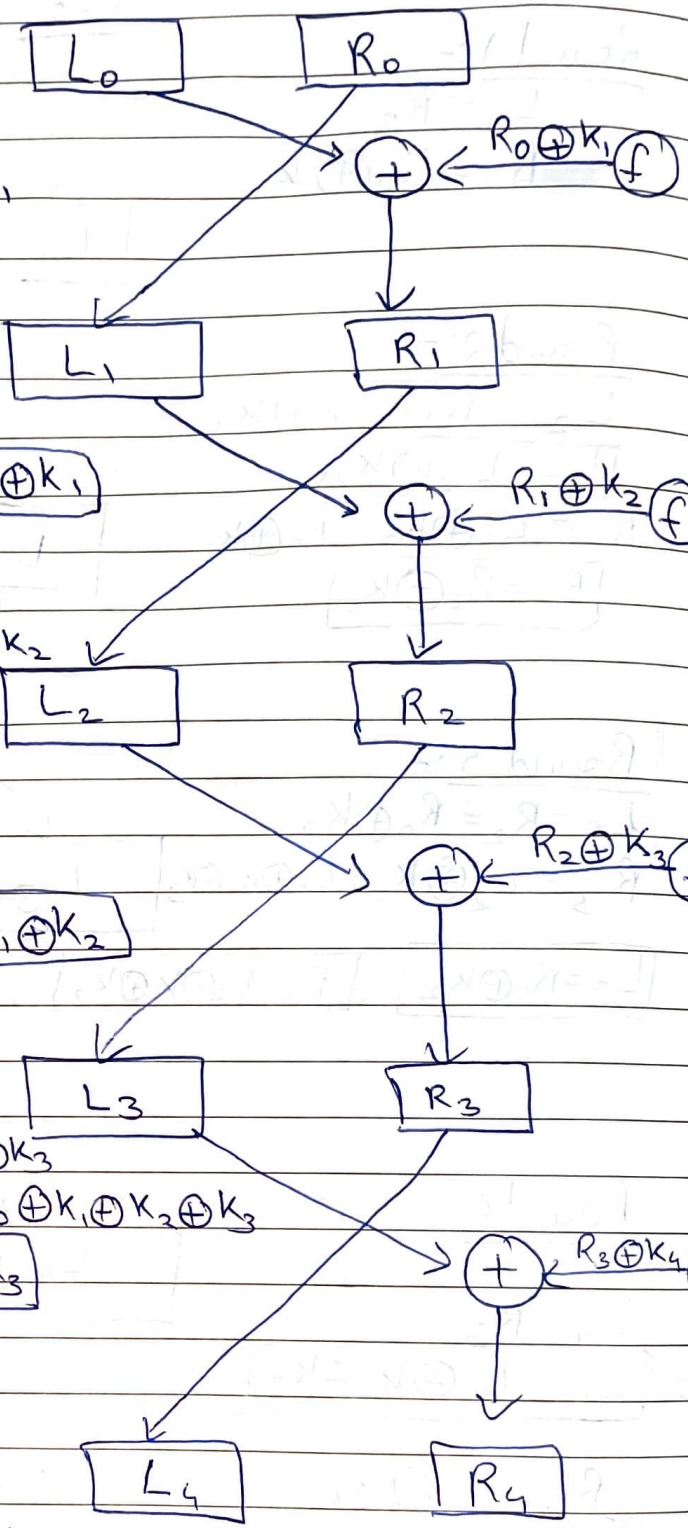
$\boxed{R_4 = R_0 \oplus K_2 \oplus K_4}$

We will swap L_4 & R_4

Ans After final swap $\boxed{C = (R_0 \oplus K_2 \oplus K_4, L_0 \oplus K_1 \oplus K_3)}$



D) $F(R_{i-1}, k_i) = R_{i-1} \oplus k_i$



Round 1:-

$L_1 = R_0$

$R_1 = L_0 \oplus R_0 \oplus K_1$

Round 2:-

$L_2 = R_1 = L_0 \oplus R_0 \oplus K_1$

$R_2 = L_1 \oplus R_1 \oplus k_2$

$R_2 = R_0 \oplus L_0 \oplus R_0 \oplus K_1 \oplus K_2$

$R_2 = L_0 \oplus K_1 \oplus K_2$

Round 3:-

$L_3 = R_2 = L_0 \oplus K_1 \oplus K_2$

$R_3 = L_2 \oplus R_2 \oplus K_3$

$R_3 = L_0 \oplus R_0 \oplus K_1 \oplus R_2 \oplus K_3$

$= L_0 \oplus R_0 \oplus K_1 \oplus L_0 \oplus K_1 \oplus K_2 \oplus K_3$

$R_3 = R_0 \oplus K_2 \oplus K_3$

Round 4:-

$L_4 = R_3 = R_0 \oplus K_2 \oplus K_3$

$L_4 = R_0 \oplus K_2 \oplus K_3$

$R_4 = L_3 \oplus R_3 \oplus K_4$

$= L_0 \oplus K_1 \oplus K_2 \oplus R_0 \oplus K_2 \oplus K_3 \oplus K_4$

$R_4 = L_0 \oplus K_1 \oplus R_0 \oplus K_3 \oplus K_4$

We will swap R_4 & L_4

Ans After final swap $C = (L_0 \oplus K_1 \oplus R_0 \oplus K_3 \oplus K_4 , R_0 \oplus K_2 \oplus K_3)$

* Problem 3:-

Given:- Encryption rule as

$$C_0 = IV \oplus E(P_0, K),$$
$$C_1 = C_0 \oplus E(P_1, K),$$
$$C_2 = C_1 \oplus E(P_2, K),$$
$$\ldots$$

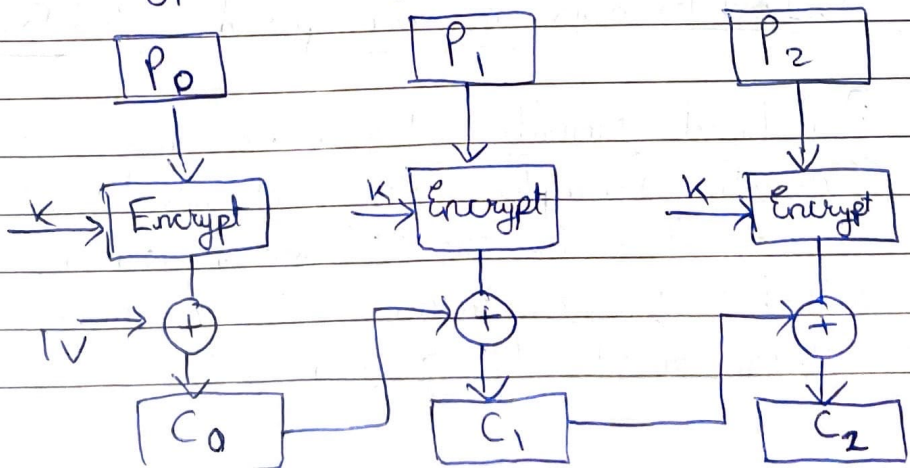
a) The corresponding decryption rule:-

The generalised encryption rule becomes.

$$C_i = C_{i-1} \oplus E(P_i, K)$$

Now solving in reverse order.

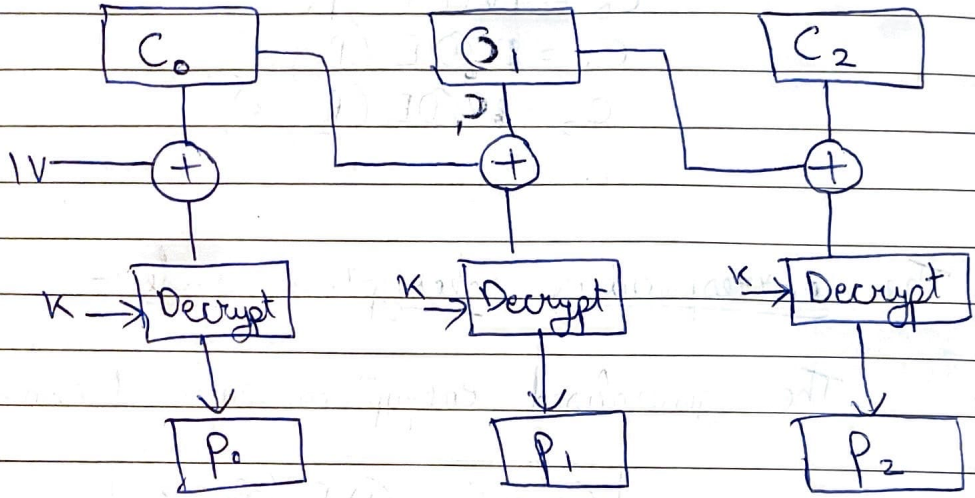
Our Encryption diagram will look like



$$C_i = C_{i-1} \oplus E(P_i, K)$$
$$C_i \oplus C_{i-1} = E(P_i, K)$$
$$\boxed{P_i = D(C_i \oplus C_{i-1}, K)}$$

Corresponding decryption diagram will be.

$$P_0 = D(C_0 \oplus IV, K)$$
$$P_1 = D(C_1 \oplus C_0, K)$$
$$P_2 = D(C_2 \oplus C_1, K)$$



$$\boxed{P_i = D(C_i \oplus C_{i-1}, K)}$$

b) Disadvantages as compared to CBC mode :-

i) Reduced security :- As over here we are directly encrypting the plain text with the key & and then we are ~~XOR~~ performing XOR operation. Which reduces the confusion and diffusion introduced by performing XOR operation first

then encryption. So we could say that CBC is more secure because it adds confusion and diffusion in the encryption process as it XOR's first then implements the encryption algorithm. Where as in the given algorithm we are directly encrypting the plain text.
This increases the probablity of plain text attacks.

ii) Easy decryption :-

As over here we are performing XOR operation first then we are applying the decryption algorithm which makes it easy for attackers to target as the algorithm both the cipher text prior and after decryption we directly get our plain text. Where as in CBC we had to perform XOR after getting the decryption message.