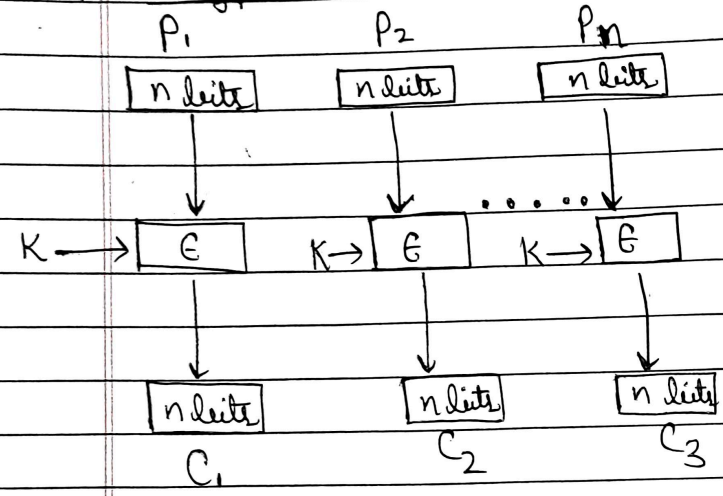
Name :- Aryan Raj Enrollment No :- 2020ITB012

Assignment -2

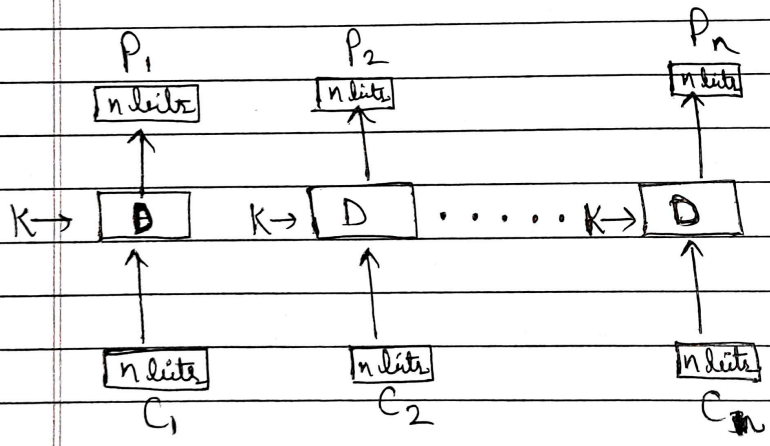
Q 1.) Electronic code block

a.) Encryption



$C_i = E_K(P_i)$

b.) Decryption

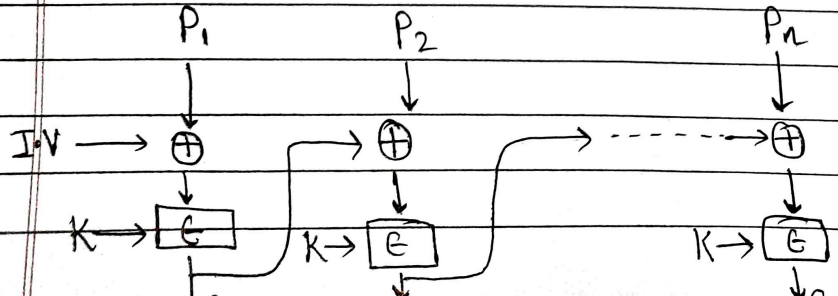


$P_i = D_K(C_i)$

2.) Cipher block chaining

I.V ⇒ Initialization vector (random)

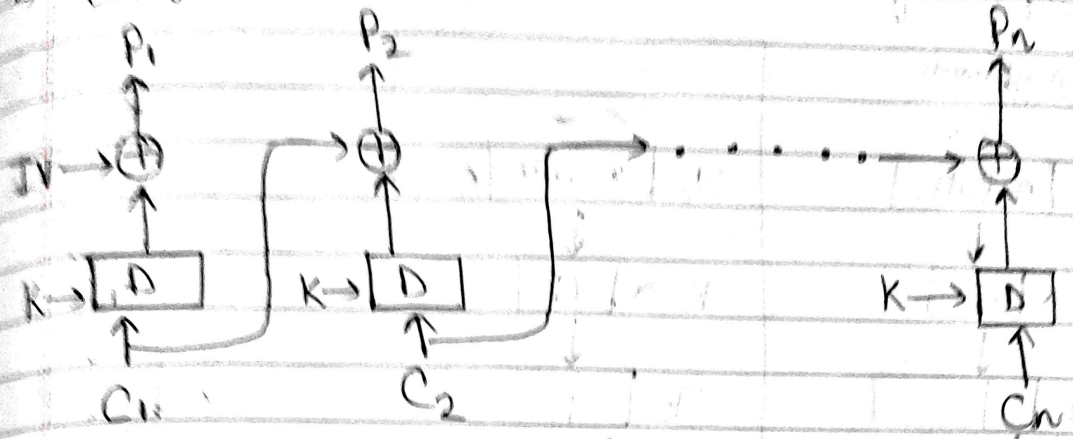
a.) Encryption



$C_0 = I.V$

$C_i = E_K(P_i \oplus C_i)$

b) Decryption

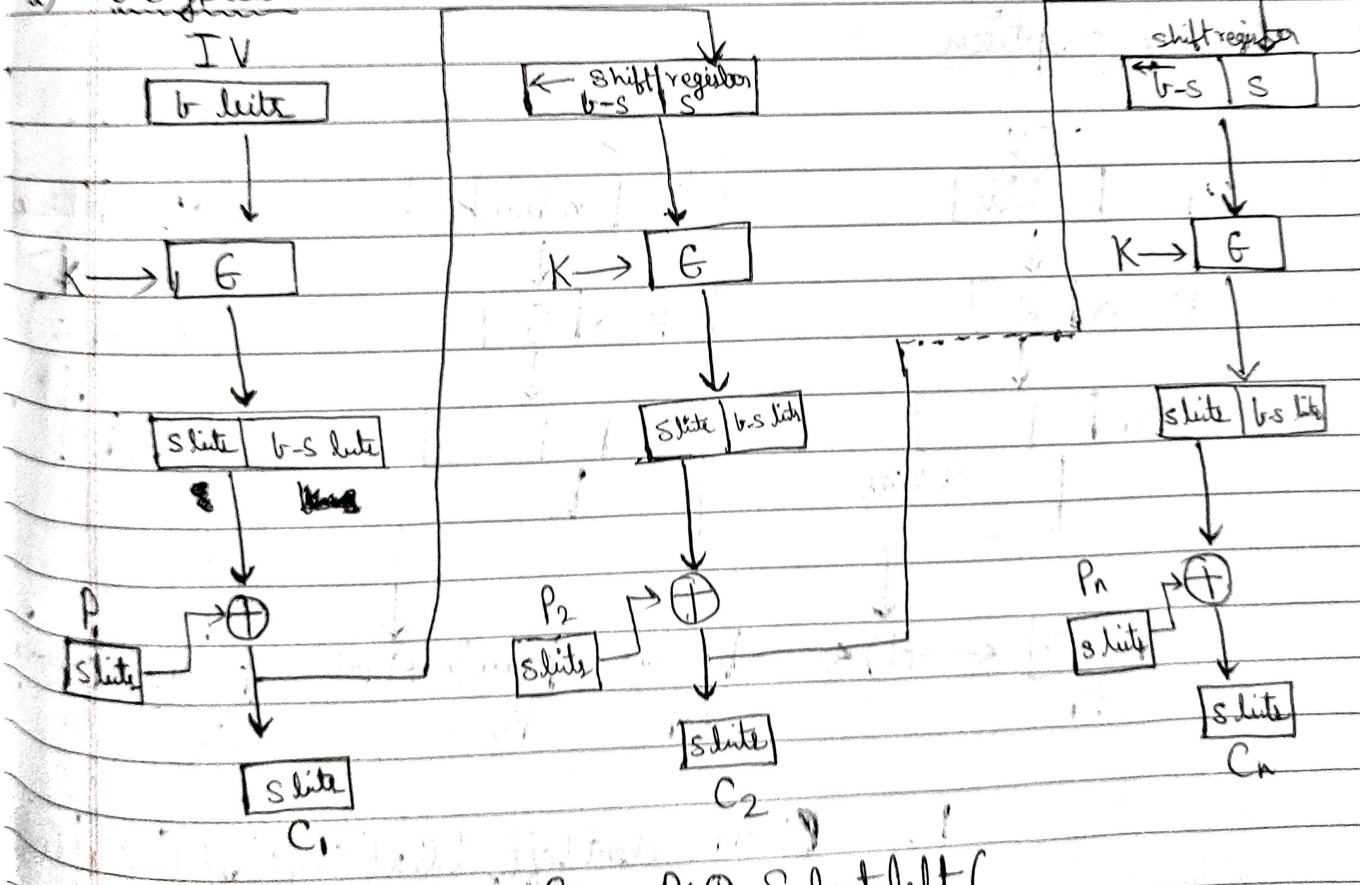


$C_0 = I \cdot V$

$P_i = C_{i-1} \oplus D_K(C_i)$

3.) Ciphier feedback mode

a) Encryption

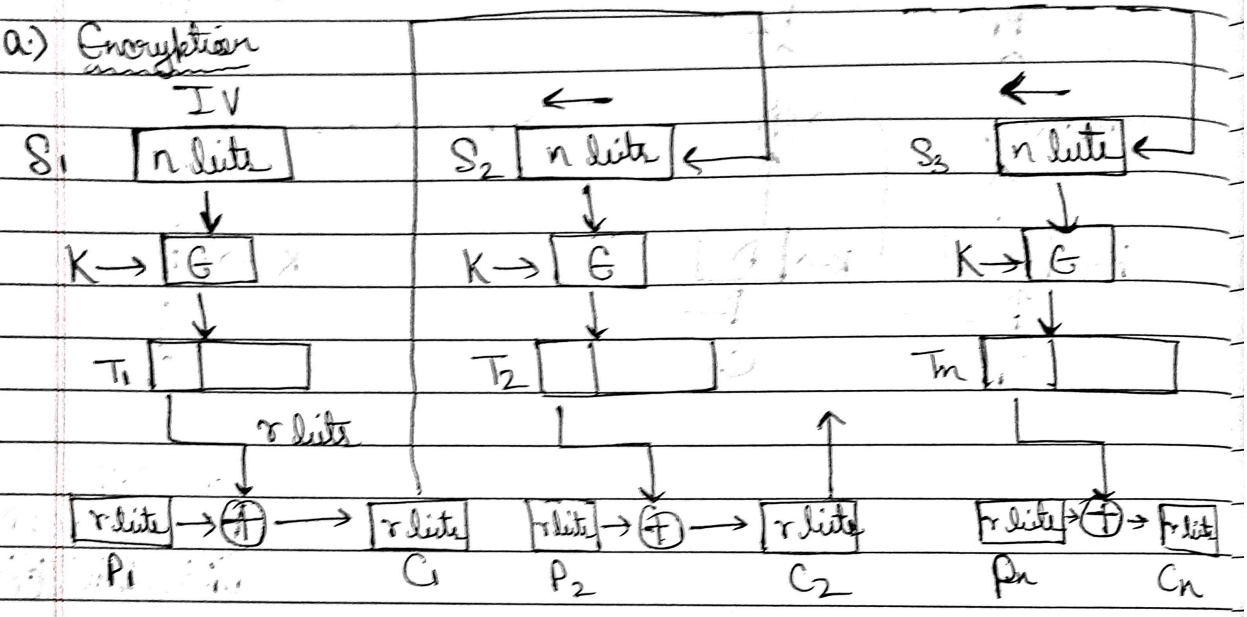


$C_0 = I \cdot V$

$C_i = P_i \oplus \text{Select left}_s(C$

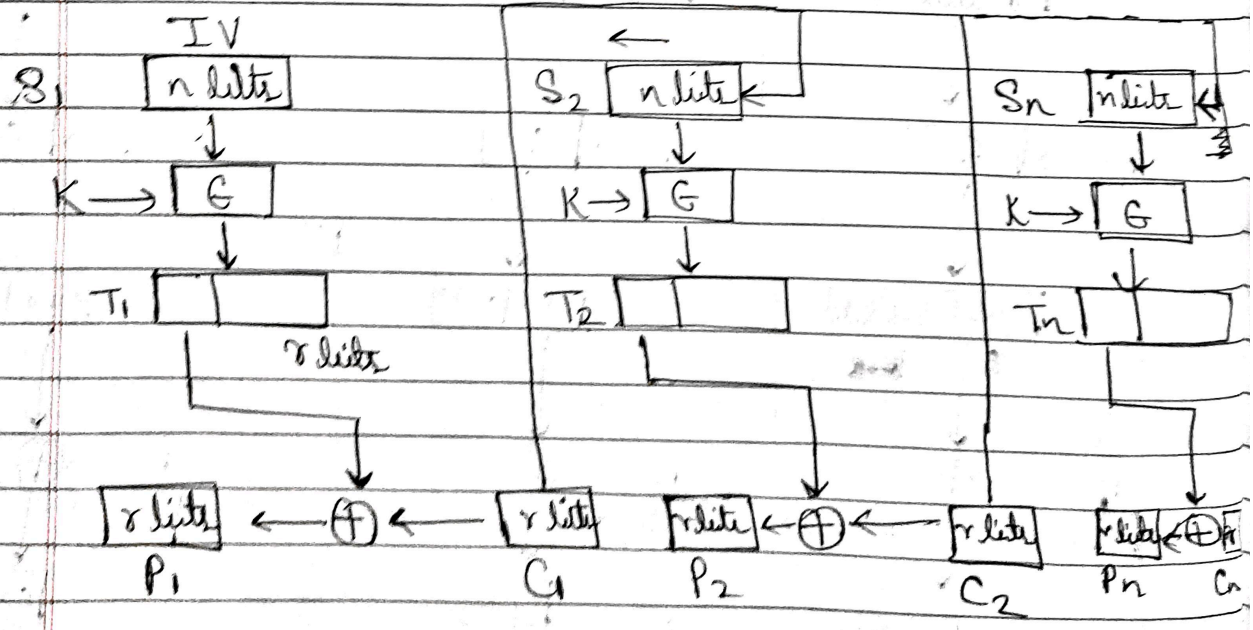
3.) Cipher feedback mode

a.) Encryption



$$C_i = P_i \oplus \text{SelectLeft}_{r,r}(G_K(\text{ShiftLeft}_r(S_{i-1}|C_{i-1})))$$

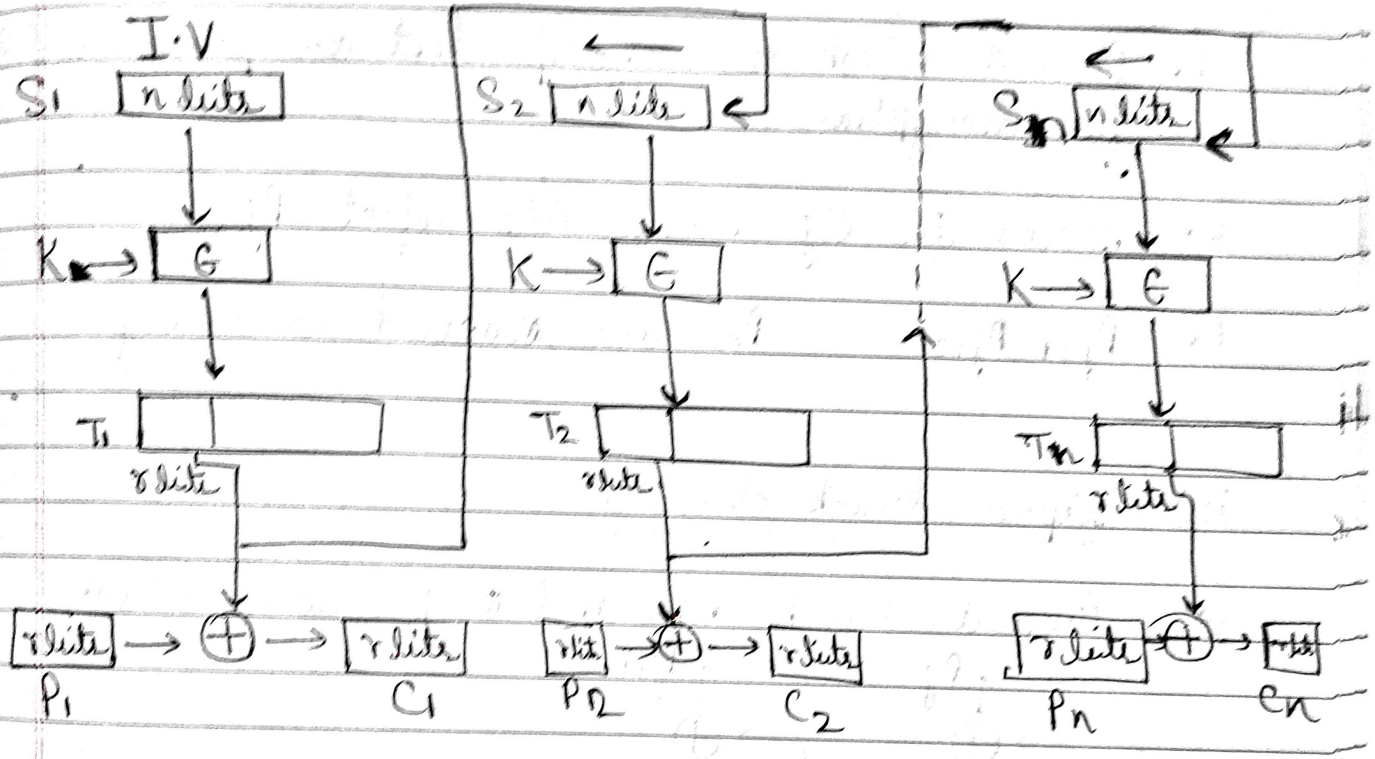
b.) Decryption



$$P_i = C_i \oplus \text{SelectLeft}_r(G_K(\text{ShiftLeft}(S_{i-1}|C_{i-1})))$$

4) Output feedback mode

a) Encryption

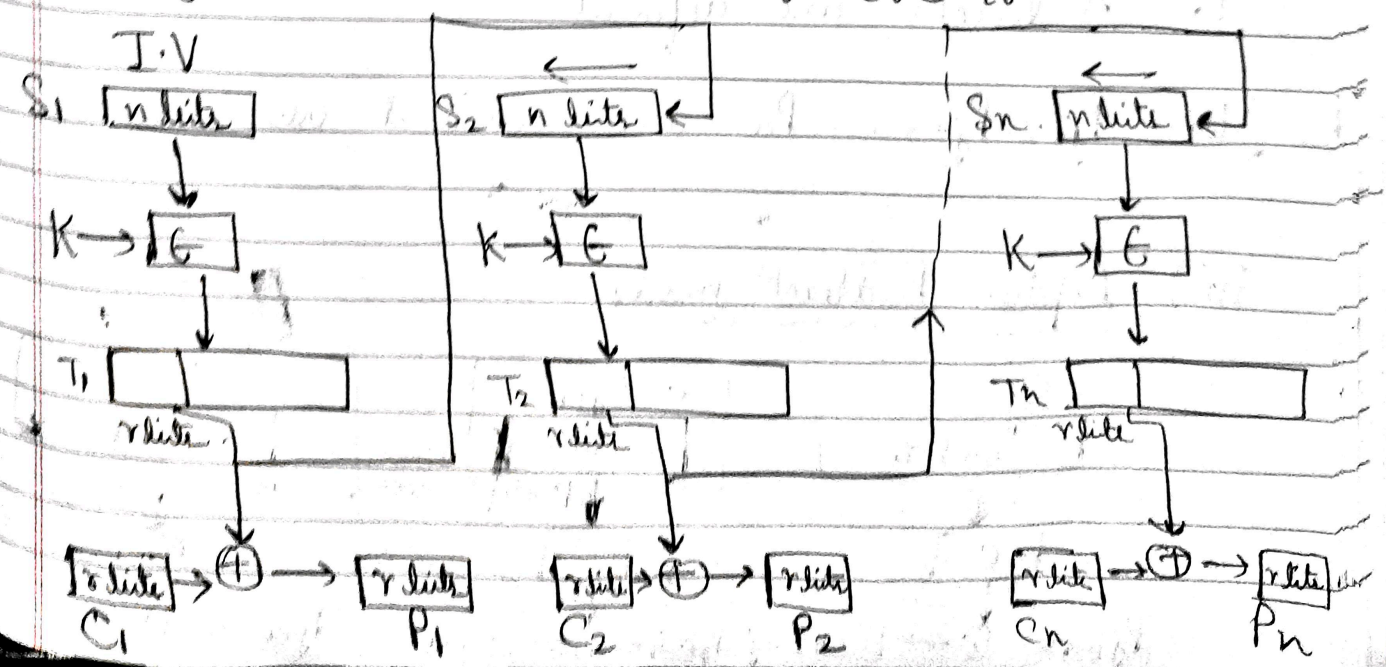


$$T_i = \text{Select Left}_r(E_K(\text{Shift Left}(S_{i-1} \mid T_{i-1})))$$

$$C_i = P_i \oplus T_i$$

b) Decryption

$$P_i = C_i \oplus T_i$$



Error propagation

i)

ii) Electronic code book

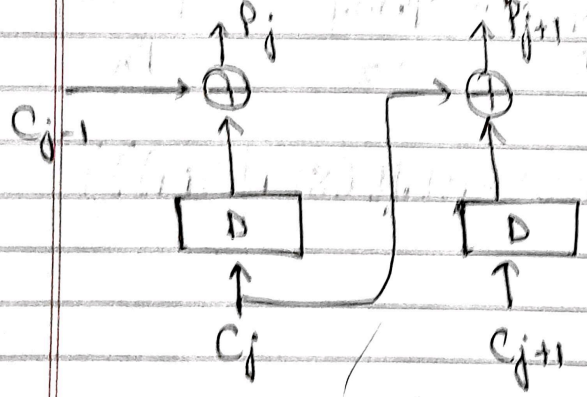
↳ Current block is not dependent on previous block for decryption.

↳ Error in C_j will only affect P_j.

↳ P_{j+1} P_{j+2} . . . . P_n are received correctly

iii) Cipher block chaining

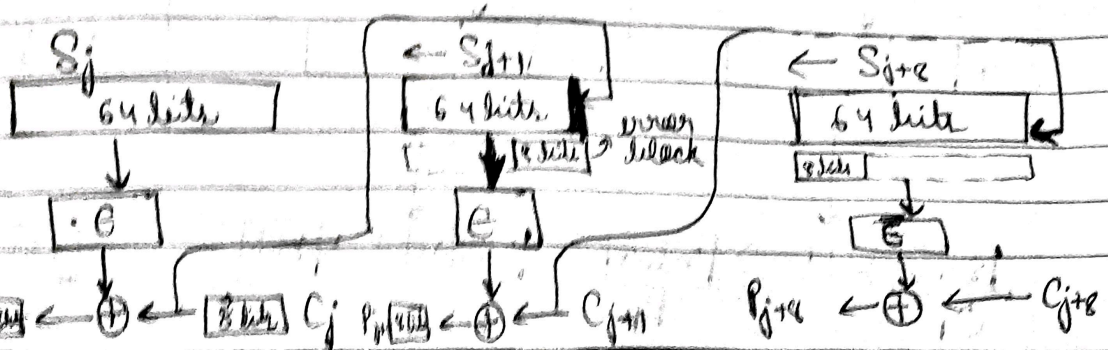
↳ Current block dependent on previous block



↳ 2 blocks are affected

↳ P_{j+2} P_{j+3} . . . P_n are received correctly

iii) Cipher Feedback mode



↳ Error transmitted in 64/8 = 8 blocks + 1 (starting P_j block)

↳ P_{j+1} ---- P_n are received correctly

iv) Output feedback mode

↳ Ciphertext is not used for chaining

↳ Error in only one block

↳ P_{j+1} P_{j+2} --- P_n are received correctly.

(2) In one time Pad

$P_1 P_2 P_3 \ldots P_n \oplus K_1 K_2 K_3 \ldots K_n = C_1 C_2 C_3 \ldots C_n$

(or)

$P \oplus K = C$

↳ 2 ciphertexts known = C, C'

$C = C_1 C_2 C_3 \ldots C_n$

$C' = C_1' C_2' C_3' \ldots C_n'$

$P \oplus K = C$
$P' \oplus K = C'$
} $P \oplus P' = C \oplus C' = X$ (let) $= X_1 X_2 \ldots X_n$

The attacker can use crib dragging for obtaining the plaintext. (Assuming a word that can appear in one of the two message and xoring it with X can give the second word and this can continue)

Justification using example

↳ "the" is the most common word and will be selected as our crib word.

↳ placing "the" at different indexes and Xoring with X until something meaningful is obtained.

↳ Let "the" = $b_1 b_2 b_3 \cdots b_K$

$X = C \oplus C' = X_1 X_2 X_3 \cdots X_n$

⇒ Xoring by placing "the" at the first index gives "KZM" which is gibberish, so we move it second index

$$\begin{array}{ll} & X_1 X_2 \cdots X_n \\ \oplus & \underline{b_1 b_2 \cdots b_K} \\ = & K_1 K_2 \cdots K_K \longleftrightarrow \text{"KZM" (gibberish)} \end{array}$$

move 1 index

$$\begin{array}{l} X_1 X_2 \cdots X_n \\ \underline{\quad b_1 \cdots b_K} \\ K_1' K_2' \cdots K_K' \longleftrightarrow \text{"hel" (meaningful)} \end{array}$$

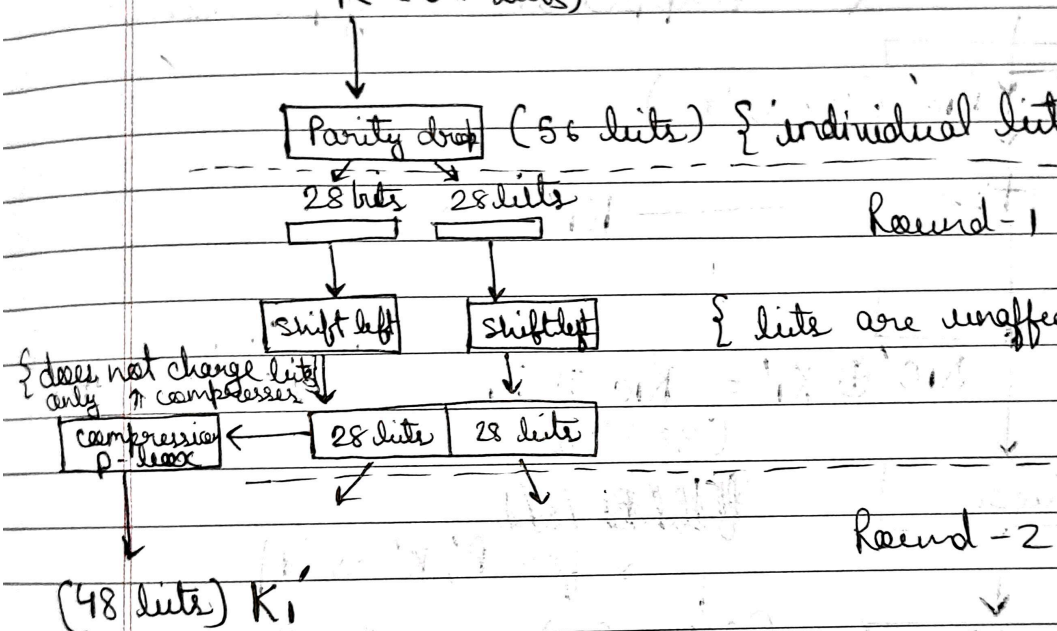
The attacker can look up for words starting with "hel", XOR with X and can continue the process until the entire text is decrypted.

{hello, help, helicopter}

Q3) Key complement Property of DES says

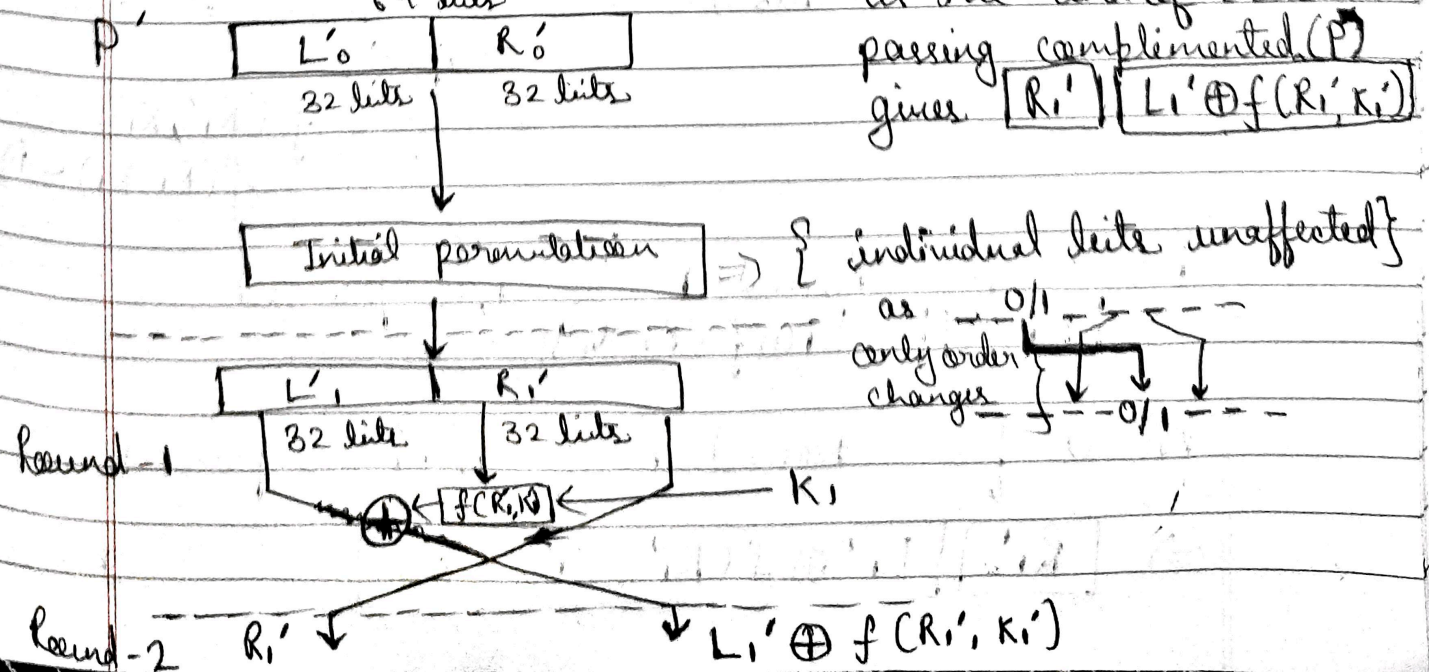
If $C = DES(P, K)$ then $C' = DES(P', K')$

i) For Key

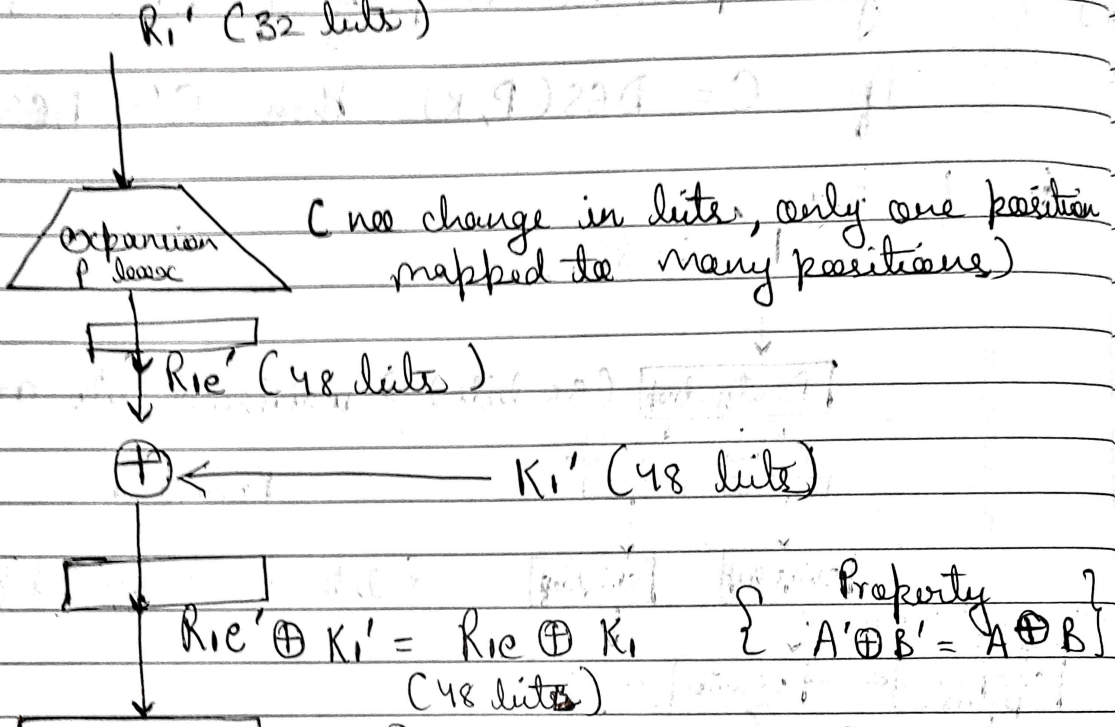


Since individual bits are not being changed, the compliment of the initial key (K') gives compliment of round keys (K_1', K_2', K_3' ...)

ii) For Plaintext



Inside Mangler Function $f(R_i', K_i')$



Result for Round-1 if P, K is passed

$\Rightarrow$ [R_1] [$L_1 \oplus f(R_1, K_1)$] – ii)

Result for Round-1 if P', K' is passed

$\Rightarrow$ [R_1'] [$L_1' \oplus f(R_1', K_1')$ – iii)]

From i) ii) and iii)

Result if P', K_2' is passed = $\boxed{R_1'}\boxed{L_1' \oplus f(R_1, K_1)}$

$= \boxed{R_1'}\boxed{(L_1 \oplus f(R_1, K_1))}$ { Property $A' \oplus B = (A \oplus B)'$ }

Thus for one round, the result gets complemented and this complemented result will be passed as input for the next round and so on. The final result we get is the complement of the ciphertext (C')

∴ If $C = DES(P, K)$ then $C' = DES(P', K')$

Q4.) A cryptographic hash function must satisfy

i) Preimage resistance { given $h(m)$ find m }

ii) Second Preimage resistance { given $h(m)$ and m find m' such that $m \neq m'$ and $h(m) = h(m')$ }

iii) Collision resistance

for $h(x) = x \bmod n$ { find m and m' such that $h(m) = h(m')$ and $m \neq m'$

Let us take true messages m and m' where $m' = m + n$

Clearly $m' \neq m$ — i.)

Also, $h(m) = m \bmod n = m \bmod n + n \bmod n$

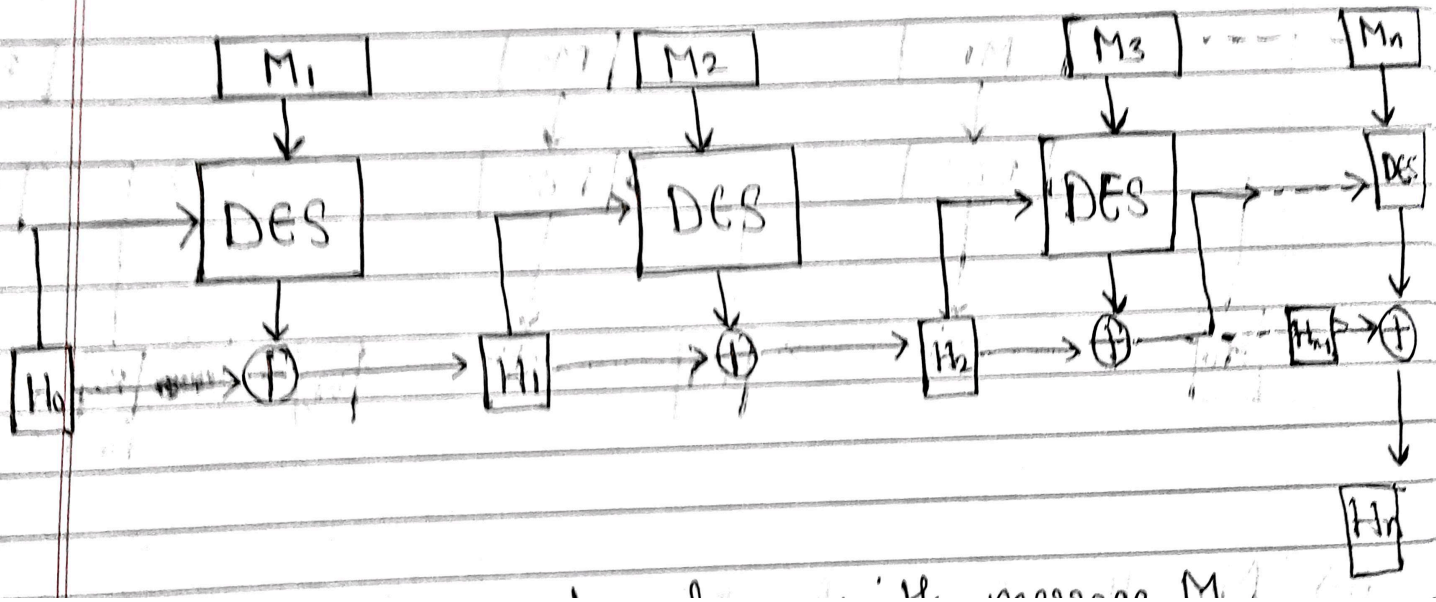
$= (m+n) \bmod n$

$= m' \bmod n = h(m')$ — ii.)

From i.) and ii.) we see that the function is not collision resistant.

Hence $h(x) = x \bmod n$ cannot be a cryptographic hash function.

(Q5) $H_i = H_{i-1} \oplus DES(M_i, H_{i-1})$



Q6) As H_0 is transmitted along with M, it can also be modified.

Let $M' = M_1' M_2 M_3 \cdots M_n$ and $M^2 = M_1' M_2 M_3 \cdots M_n$

where M_1' is the complement of M_1. Clearly $M' \neq M^2$ as $M_1 \neq M_1'$

Also let H_0' be the complement of H_0.

H_1 can be generated as $H_1 = H_0 + DES(M_1, H_0)$

Let $H_1' = H_0' + DES(M_1', H_0')$

↳ $H_1' = H_0' + (DES(M_1, H_0))'$ { Key complement property }

↳ $H_1' = H_0 + DES(M_1, H_0)$ { $A \oplus B = A' \oplus B'$ }

↳ $H_1' = H_1$

For two different (M, H_0) and (M', H_0'), we get the same hash

Hence the function is not collision resistant

Also $H_2' = H_1' + DES(M_2, H_1') = H_1 + DES(M_2, H_1)$

↳ $H_2' = H_2$ a similarly, $H_3' = H_3$ and so on

different inputs

Therefore for two (M', H_0) and (M^2, H_0'), we get the same hash.

So the function is not collision resistant.

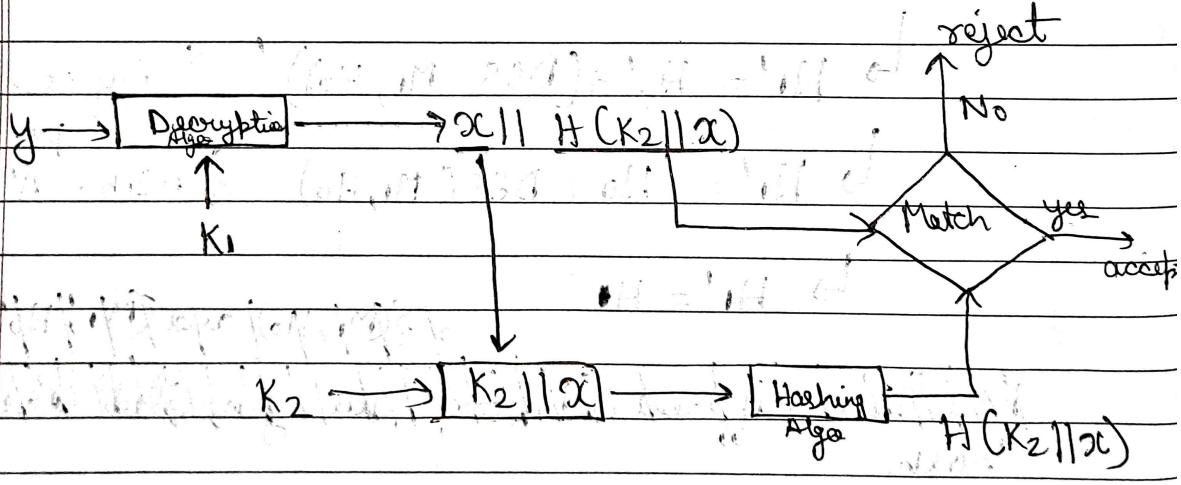
Q7) $y = E_{K_1}(x || H(K_2 || x))$

STEP-1 :- Decrypt message using K_1

↳ $x || H(K_2 || x) = D(y)$

STEP-2 :- Extract x and calculate hash of $K_2 || x$

STEP-3 :- Compare this calculated hash with the transmitted Hash. Accept if they match else reject.



Confidentiality is ensured as the entire transmitted message is encrypted using K_1.

Integrity is also ensured as hash is calculated for the message blocks.

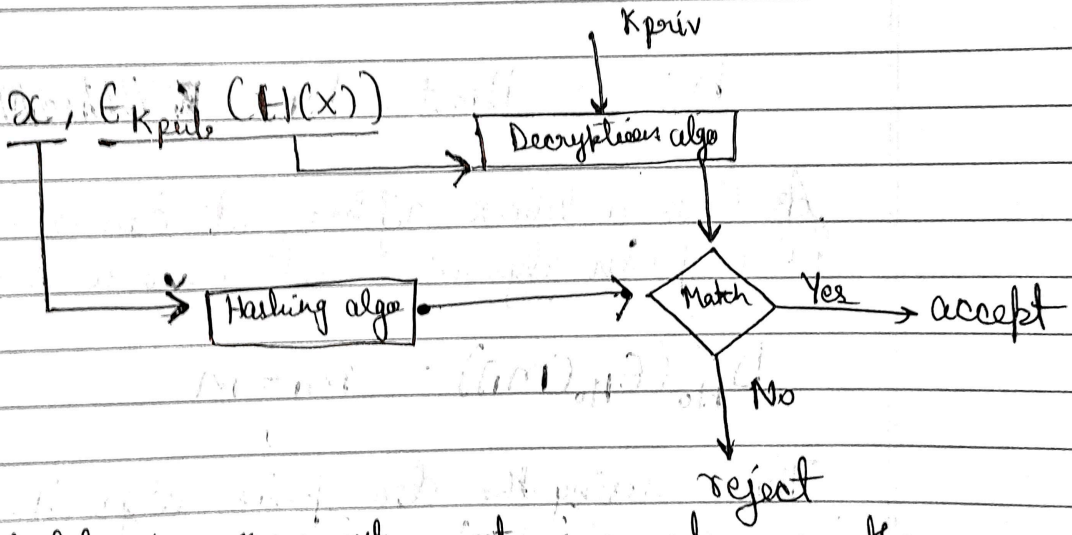
Non repudiation cannot be ensured as both the keys are present to both sender and receiver, and both can deny the message was sent by them. They can put the blame on each other. (same keys used)

Q8) $y = x, E_{K_{priv}}(H(x))$

STEP-1 :- Seperate x and encrypted Hash and decrypt the Hash using their private key.

STEP-2 :- Compute the hash for x

STEP-3 :- Compare the calculated hash. Accept if they match else reject.



Confidentiality is not ensured as the message is not encrypted.

Integrity is also not ensured as the attacker can modify the message, calculate hash and also encrypt it with receivers public key.

Non repudiation is also not ensured as anyone can send the message due to use of the public key of receiver during encryption instead of private key of sender.

Q9.) a) $H_0 = I.V$

$H_i = E(M_i, H_{i-1})$

$m = m_1 || m_2 || \cdots || m_{last}$

$h(m) = H_{last}$

For a preimage attack we know $h(m)$ and have to find m

Assuming m to be a single block message
$m = m_1$

We know $h(m)$, we also know the Initialization vector (I.V)

$h(m) = H_{last} = H_1 = E(M_1, H_0)$

As E is a block cipher, it can be inverted & Encryption algorithm will have a decryption algorithm

$D_{H_0}(E_{H_0}(m_1)) = m_1 = m$

Thus using the decryption algorithm and I.V we can find preimage of a hash and this preimage will have a single block.

Hence it is not resistant to preimage attack

b.) $M = M_1 || M_2$

$H_1 = E(M_1, H_0) = E(M_1, I.V)$

$H_2 = E(M_2, H_1)$

Let M_1' be a random message block and $M_2' = D(H_2, E(M_1', I.V))$

$h(M') = h(M_1' || M_2') = E(M_2', H_1') = E(M_2', E(M_1', I.V))$

$= E(\quad, E(D(H_2, E(M_1', I.V)), E(M_1', I.V))$

$= E_{E_{IV}(M_1')}(D_{E_{IV}(M_1')}(H_2)) = H_2$

$= h(M_1 || M_2)$

$= h(M)$

$\therefore h(M') = h(M)$

$\therefore$ M and M' are collision pairs

(Q10) CMAC

$M_i \Rightarrow$ message block i