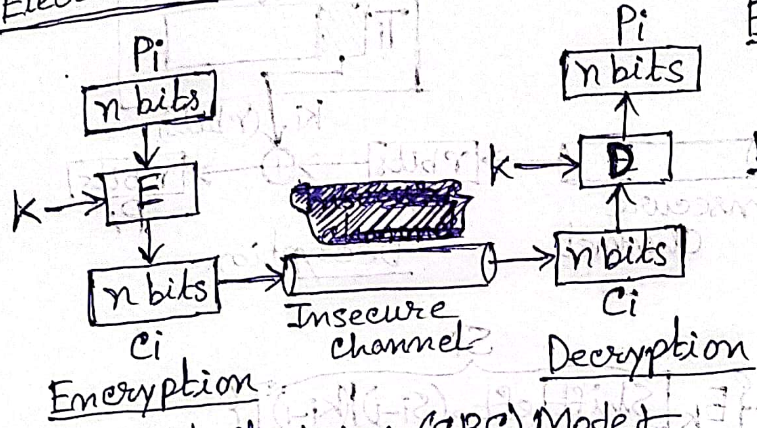
ISS-Assignment-2

1) E: Encryption, D: Decryption, K: Secret key, IV: Initial Vector (S_1) (C_0)
S_i: Shift Register, C_i: Ciphertext block i, P_i: Plaintext block i,
T_i: Temporary Register, k_i: ~~Register~~ Generated key, where $i = 1, 2, 3, \ldots, N$. ($r \leq n$)

→ Electronic Coodbook (ECB) Model



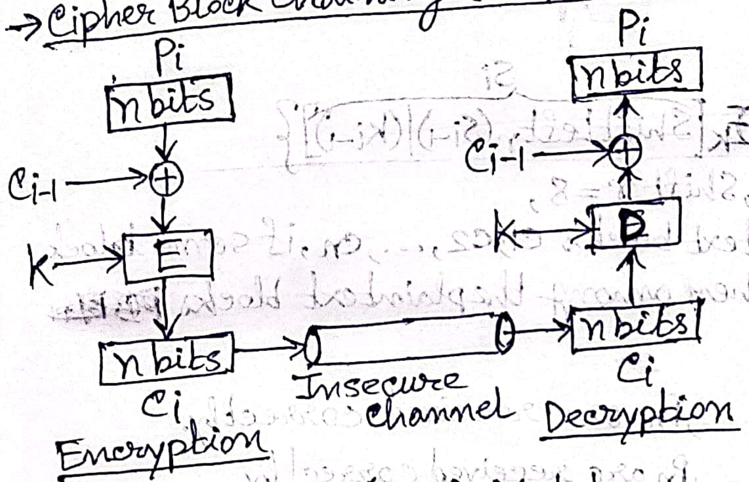
Encryption:

$C_i = E_K(P_i)$

Decryption:

$P_i = D_K(C_i)$

→ Cipher Block Chaining (CBC) Model



Encryption:

$C_0 = IV$

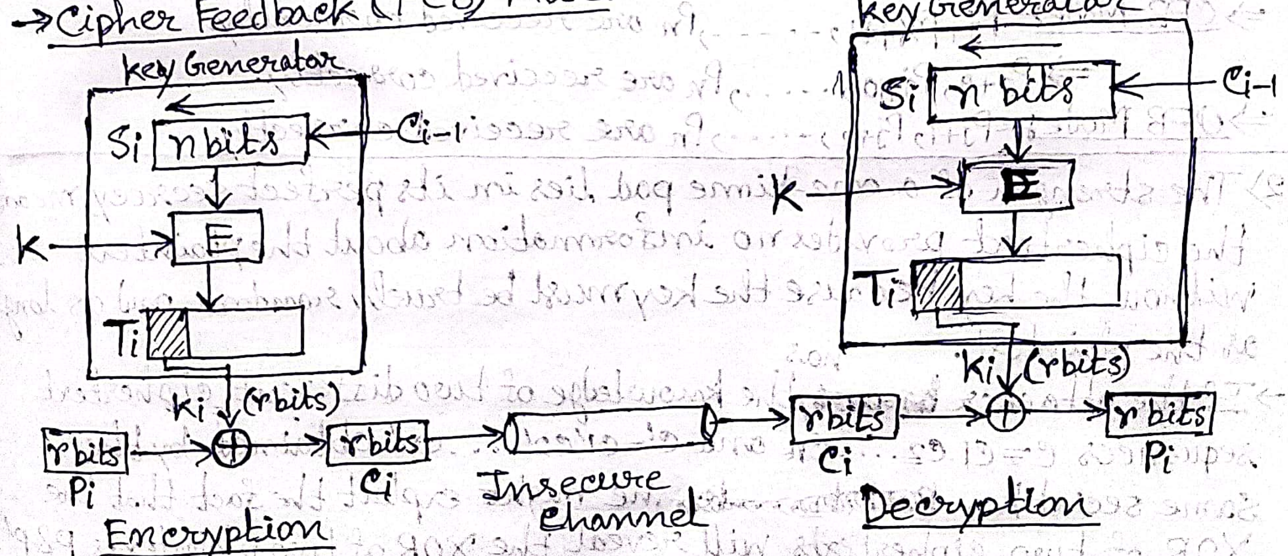
$C_i = E_K(P_i \oplus C_{i-1})$

Decryption:

$C_0 = IV$

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

→ Cipher Feedback (FCB) Model



Encryption:

$S_1 = IV$, C_0 not exist.

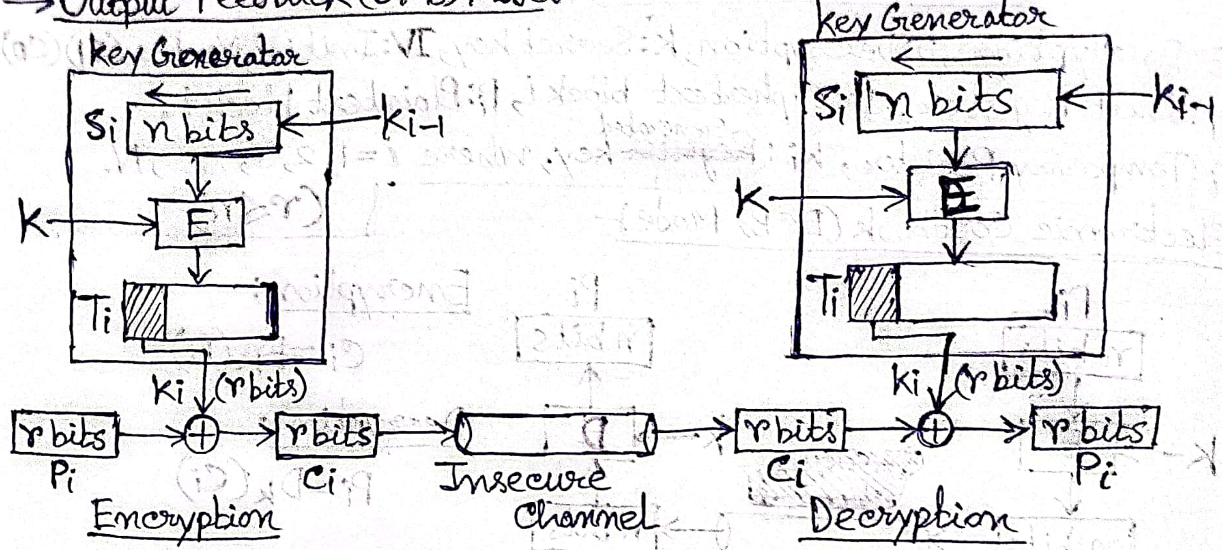
$C_i = P_i \oplus \text{SelectLeft}_r\{E_K[\underbrace{\text{ShiftLeft}_r(S_{i-1}) | (C_{i-1})}_{S_i}]\}$

Decryption:

$S_1 = IV$, C_0 not exist.

$P_i = C_i \oplus \text{SelectLeft}_r\{E_K[\underbrace{\text{ShiftLeft}_r(S_{i-1}) | (C_{i-1})}_{S_i}]\}$

→ **Output Feedback (OFB) Mode:-**



Encryption:-

$S_1 = IV$

$C_i = P_i \oplus SelectLeft_r\{E_K[\overbrace{ShiftLeft_r(S_{i-1}) | (k_{i-1})}^{S_i}]\}$

Decryption:-

$S_1 = IV$

$P_i = C_i \oplus SelectLeft_r\{E_K[\overbrace{ShiftLeft_r(S_{i-1}) | (k_{i-1})}^{S_i}]\}$

•• For given, block size $n = 64$, Shift $r = 8$,
If in a sequence of ciphertext blocks $c_1, c_2, \ldots, c_n$, if some block c_j is erroneous, $1 \le j \le n$, then among the plaintext blocks $P_j, P_{j+1}, \ldots, P_n$,

⇒ ECB Mode:- $P_{j+1}, P_{j+2}, \ldots, P_n$ are received correctly.

⇒ CBC Mode:- $P_{j+2}, P_{j+3}, \ldots, P_n$ are received correctly.

⇒ CFB Mode:- $P_{j+\lceil n/r \rceil + 1}, \ldots, P_n$ are received correctly.

⇒ $P_{j+9}, P_{j+10}, \ldots, P_n$ are received correctly.

⇒ OFB Mode:- $P_{j+1}, P_{j+2}, \ldots, P_n$ are received correctly.

---

2) The strength of a one-time pad lies in its perfect secrecy, means the ciphertext provides no information about the plaintext without the key because the key must be truely random and as long as the plaintext.

→ If the attacker has the knowledge of two different ciphertext sequences $c = c_1 c_2 \ldots c_n$ and $c' = c_1' c_2' \ldots c_n'$ obtained by the same secret key, he might exploit the fact that the XOR of two ciphertexts will reveal the XOR of two plaintexts P & P'

⇒ $C \oplus C' = (P \oplus K) \oplus (P' \oplus K) = P \oplus P'$ [let, the same key be K]

→ With Statistical analysis or other cryptographic attacks, the Attacker can guess K, subject to constraint:-

1. $P \oplus C = P' \oplus C' = K$, 2. $P \oplus P' = C \oplus C'$.

And this is how, the security of one-time pad starts to degrade and the strength of one time pad reduces.

---

3) Key Complement Property:- For any plaintext P and key k, if $C = DES(P, k)$, then $C' = DES(P', k')$, where, C is the ciphertext.

Proof:-

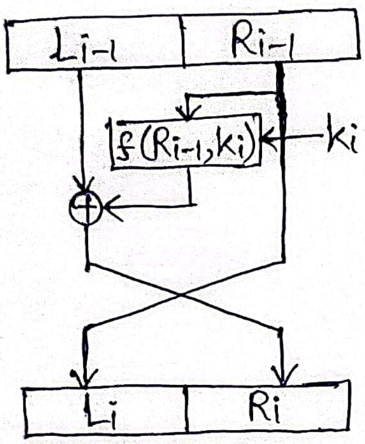
We know the basic properties of XOR operation:-

(i) $A \oplus B = A' \oplus B'$, (ii) $(A \oplus B)' = A' \oplus B$, (iii) $(A \oplus B)' = A \oplus B'$

→ As Initial and Final Permutations in DES are inverses of each other, they have no significance on key Complement Property.

→ For each Round i of total 16 Rounds (16 Feistel Ciphers), Round key Generator provides k_i' because it involves mainly shift operations.

→ If for each Round i, $L_i = R_{i-1}$, $R_i = L_{i-1} \oplus f(R_{i-1}, k_i)$, where



Round i in DES

$f(R_{i-1}, k_i)$ involves mainly XOR operation of R_{i-1} and k_i.

So, if L_{i-1}' & R_{i-1}' is provided in place of L_i & R_{i-1}, then,

$L_i = R_{i-1}'$,

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

$= L_{i-1}' \oplus f(R_{i-1}, k_i)$ [Applying Property (i)]

$= [L_{i-1} \oplus f(R_{i-1}, k_i)]'$ [Applying Property (ii) or (iii)]

So, for each Round i, if we input complement of L_{i-1} & R_{i-1} & k_i, the the output is the complement of what we would get if inputs are L_{i-1} & R_{i-1} & k_i.

→ Hence, proved that if $C = DES(P, K)$ then $C' = DES(P', K')$.

---

4) A Cryptographic Hash function must satisfy three Criteria,

~~1) Given, Y=h(M), difficult to find M such~~

i) Preimage Resistance:-

Given $Y = h(M)$, difficult to find M' such that $Y = h(M')$.

ii) Second Preimage Resistance:-

Given M and $h(M)$, difficult to find $M' \neq M$ such that $h(M) = h(M')$

iii) Collision Resistance:-

Given nothing, difficult to find $M' \neq M$ such that $h(M) = h(M')$

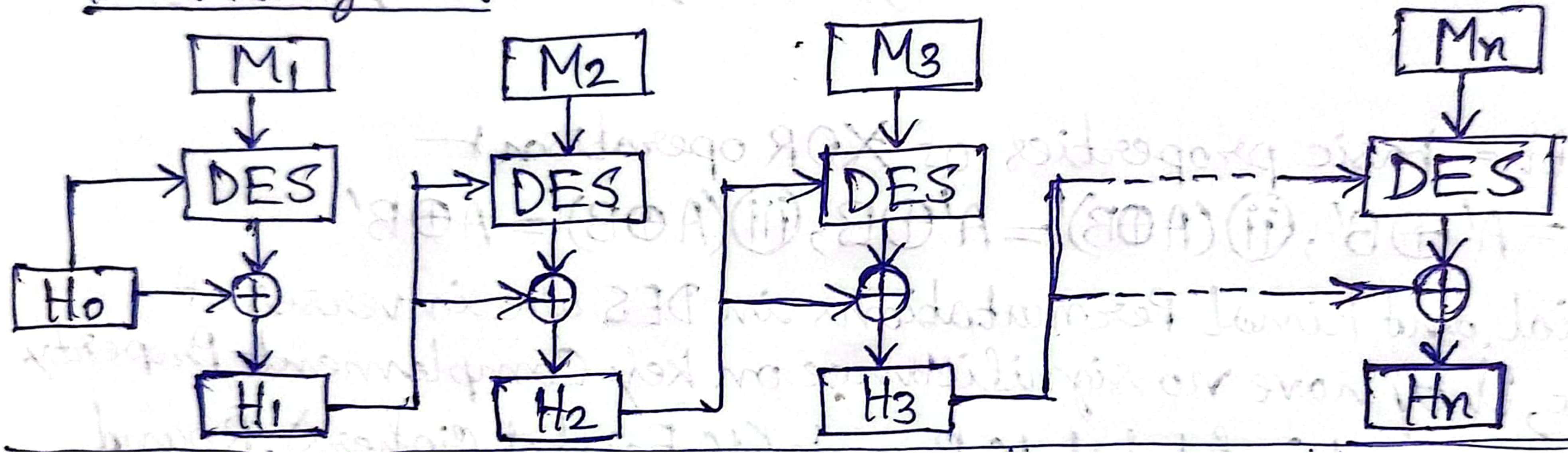
→ For the function $h(x) = x \bmod n$, it is not difficult to find any of $(x + kn)$ (where, k is an integer) by the use of Randomized algorithm. So all the above three critarias fail for the given function.

→ Hence, $h(x) = x$ can not be regarded as Cryptographic Hash Function.

5) Given hash scheme:- $H_i = H_{i-1} \oplus DES(M_i, H_{i-1})$

H_0 is set by Sender and transmitted to receiver along with the message. sequence $M = M_1, M_2, ----, M_n$.

→ Block Diagram:-



6) H_0 may not be same for every M, as H_0 is set by Sender and transmitted to the receiver along with M.

$\rightarrow$ For $M^1 = M_1 M_2 \cdots M_n$ and H_0, $h(H_0, M^1) = H_1 H_2 \cdots H_n$

$\rightarrow$ let, $M^2 = M_1' M_2 \cdots M_n$ and H_0', then $H_0 \neq H_0'$ and $M^1 \neq M^2$;

~~then~~ and also let, corresponding $h(H_0', M^2) = a_1 a_2 \cdots a_n$.

$\Rightarrow a_1 = H_0' \oplus DES(M_1', H_0')$

$= H_0' \oplus [DES(M_1, H_0)]'$ [Key Complement property of DES]

$= H_0 \oplus DES(M_1, H_0)$ [Applying Property (i) of XOR]

$= H_1 \Rightarrow \boxed{a_1 = H_1}$

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

for $i = 2$ to n. $\Rightarrow a_i = H_i$ for $i = 1$ to n,

$\Rightarrow h(H_0', M^2) = H_1 H_2 \cdots H_n = h(H_0, M^1)$ such that $(H_0', M^2) \neq (H_0, M^1)$

Where, $M^1 = M_1 M_2 \cdots M_n$ and $M^2 = M_1' M_2 \cdots M_n$.

$\rightarrow$ Hence, the above hash scheme is not resistant to collision attack.

CamScanner

Q7) Steps performed by the receiver upon receipt of $Y = E_{K_1}(X \| H(K_2 \| x))$ are as follows:-

1. decrypt Y using the key $K_1 \Rightarrow D_{K_1}(Y) = x \| H(K_2 \| x)$.
2. extract x and $H(K_2 \| x)$ from the decrypted result.
3. Calculates $H(K_2 \| x)$ and verifies it with extracted $H(K_2 \| x)$.

⇒ The protocol,

→ ensure Confidentiality, as the message is encrypted and decrypted only by K_1

→ ensure Integrity, as the calculated $H(K_2 \| x)$ and extracted $H(K_2 \| x)$ should match for the Integrity of the message.

→ Not ensure Non-repudiation, as the key ~~[illegible]~~ can be used by more than one senders, one can deny a message encrypted by the same key is ~~not~~ sent by him.

Q8) Steps performed by the receiver upon receipt of $Y = x, E_{kpub}(H(x))$ are as follows:

1. extract x and $E_{kpub}(H(x))$ from Y
2. decrypt $E_{kpub}(H(x))$ using $k_{private} \Rightarrow D_{kprivate}(E_{kpub}(H(x))) = H(x)$,
   where, k_{pub} = Public key of Receiver, $k_{private}$ = Private key of Receiver.
3. Calculates $H(x)$ and verifies it with ~~other~~ decrypted $H(x)$.

⇒ The protocol,

→ Not ensure Confidentiality, as x is not encrypted and anyone intercepting the message can see x.

→ Not ensure Integrity, as the attacker can modify x and calculate $H(x)$ and encrypt it with k_{pub}.

→ Not ensure Non-Repudiation, as anyone can send Y with k_{pub} because Sender didn't use its private key ~~to encrypt~~ for encryption which does not provide authentication that Y is sent by that sender.