UNIT-II

Mathematics of Symmetric key Cryptography:-

Symmetric Encryption:-

- Symmetric Ciphers Use Symmetric algorithms to encrypt and decrypt data
- Those ciphers are Used in Symmetric key Cryptography..
- A Symmetric algorithm Uses the Same key to encrypt data as it does to decrypt data.

Example:

A Symmetric algorithm will use key K to encrypt Some plaintext information like a password into a Ciphertext.

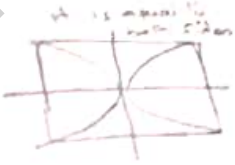
Then it Uses K again to take the Ciphertext and turns it back into the password.

- Symmetric Ciphers are opposite of asymmetric Ciphers, like those Used in public-key-Cryptography.
- Ciphers Use asymmetric algorithm which use one key to encrypt data and a different key to decrypt Ciphers.
- Those, two keys are Called public and private keys as in the case with RSA encryption.
- The public key is Used to encrypt data and private key is Used to decrypt data.

M. Anandarao, M.Sc., M.C.A., (SET)., M.Tech., (CSE)., PhD's.

Mathematics of Symmetric Key Cryptography:-

① Chinese - Remainder Theorem:-



General form

$$\left.\begin{aligned} x &= a_1 \pmod{m_1} \\ x &= a_2 \pmod{m_2} \\ x &= a_n \pmod{m_n} \end{aligned}\right\}$$

Step: 1:-

Find out Common modulus M

$$M = m_1 \times m_2 \times m_3 \times \cdots \times m_n$$

Step: 2:-

(i) $M = m_1 m_2 m_3$

(ii) $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

Find $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $\cdots$ $M_n = \frac{M}{m_n}$

Step: 3:-

(iii) $M_1^{-1} \bmod m_1$, $M_2^{-1} \bmod m_2$, $\cdots$ $M_n^{-1} \bmod m_n$.

Step: 4:-

Find out Inverse M_1^{-1}, M_2^{-1}, $\cdots$ M_n^{-1}

$$x = ((a_1 * M_1 * M_1^{-1}) + (a_2 * M_2 * M_2^{-1}) + \cdots + (a_n * M_n * M_n^{-1})) \bmod M$$

(iv) $x = (a_1 \times m_1 \times M_1^{-1}) + (a_2 \times m_2 \times M_2^{-1}) + (a_3 \times m_3 \times M_3^{-1})$

Ex:-

$$x \equiv 4 \pmod{11}$$
$$x \equiv 5 \pmod{7}$$
$$x \equiv 6 \pmod{13}$$

From the above similarly,

$m_1 = 11$ $\quad a_1 = 4$

$m_2 = 7$ $\quad a_2 = 5$

$m_3 = 13$ $\quad a_3 = 6$

(4)

Step 1:

$$M = m_1 \times m_2 \times m_3$$

$$= 11 \times 7 \times 13$$

$$= 1001$$

Step 2:

$$M_1 = \frac{M}{m_1} = \frac{1001}{11} = 91$$

$$M_2 = \frac{M}{m_2} = \frac{1001}{7} = 143$$

$$M_3 = \frac{M}{m_3} = \frac{1001}{13} = 77$$

Step 3:

To find: $M_1^{-1} = 91^{-1} \pmod{11} \Rightarrow \frac{1}{91} \bmod 11$

$$(n * 91) \bmod 11 = 1$$

Here $n = 1, 2, 3, 4 \ldots\ldots$

$$(4 * 91) \bmod 11 = 1$$

364 mod 11 = 1

$$\boxed{M_1^{-1} = 4}$$

To find: $M_2^{-1} = 143^{-1} \pmod{7} = \frac{1}{143} \bmod 7$

$$= (n * 143) \bmod 7$$

Here $n = 1, 2, 3, 4 \ldots\ldots$

$$= (5 \times 143) \bmod 7$$

5 × 143 = 715

$$\boxed{M_2^{-1} = 5}$$

To find :- $M_3^{-1} = 77 \pmod{13} = \frac{1}{77} \pmod{13}$

$= (n * 77) \bmod 13 = 1$

Here $n = 1, 2, 3, 4, \ldots$

$= (12 \times 77) \bmod 13 = 1$

$= 924 \bmod 13 = 1$

$M_3^{-1} = 12$

13 | 924 (71
91
14
13
1

13 (924) 71
91
14
13
1

Formula:

$x = ((a_1 * M_1 * M_1^{-1}) + (a_2 * M_2 * M_2^{-1}) + \ldots\ldots$

$(a_3 * M_3 * M_3^{-1})) \bmod M.$

$= (4 * 91 * 4) + (5 * 143 * 5) + (6 * 77 * 12) \bmod (1001)$

$= (1456 + 3575 + 5544) \bmod (1001)$

$= 10575 \bmod (1001)$

$x = 565$

Here x Value remains same but a_1, a_2, a_3 & mod Values Changes.

$565 \equiv a_1 \pmod{11}$ $\quad a_1 = 4$

$565 \equiv a_2 \pmod{7}$ $\quad a_2 = 5$

$565 \equiv a_3 \pmod{13}$ $\quad a_3 = 6$

Hence proved that x is Constant.

x is a Unique Solution for all the equations..

(6)

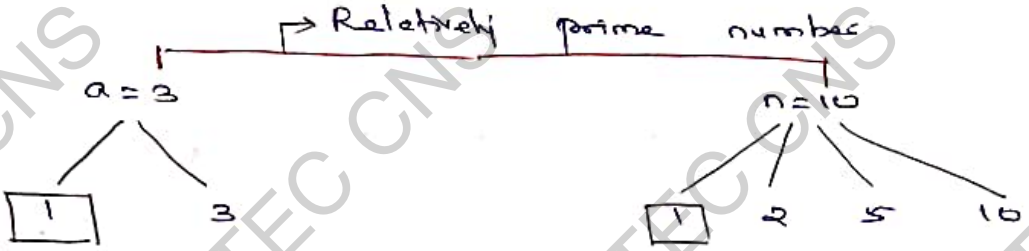
Euler's Theorem :- (Example of Symmetric key).

For every positive integer 'a' & any number 'n' where it is said to be relatively prime.

Then

$$a^{\phi(n)} \equiv 1 \bmod n$$

where $\gcd(a, n) = 1$



Common factor → [1]

Chinese Remainder Theorem:-

Qn:-

$x = 2 \bmod 3$ (a, m)

$x = 3 \bmod 5$

$x = 2 \bmod 7$

Steps:-

i) $M = m_1 m_2 m_3$

ii) $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $M_3 = \frac{M}{m_3}$

iii) $M_1^{-1} (\bmod m_1)$ ....

iv) ~~$x = (a_1 m_1 m_1^{-1} + a_2 m m_2^{-1} + \ldots)$~~

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + \ldots)$

Step 1:-

$a_1 = 2 \quad a_2 = 3 \quad a_3 = 2$

$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7$

Step 2:

$M = m_1 \times m_2 \times m_3$

$= 3 \times 5 \times 7$

$= 105$

Step 3:

$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$, $M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$, $M_3 = \frac{105}{7} = 15$

Step 4:

$M_1^{-1} \bmod m_1 = (35)^{-1} \bmod 3$

$= 35 \bmod 3$

$= 2$

$M_2^{-1} \bmod m_2 = (21)^{-1} \bmod 5$

$= (21)^3 \bmod 5$

$= 9261 \bmod 5$

$= 1$

$M_3^{-1} \bmod m_3 = (15)^{-1} \bmod 7$

$= 15^5 \bmod 7$

$= 759375 \bmod 7$

$= 1$

(Side work: a^{P-2}; $5-2=3$; $7-2=5$; $\frac{35}{3} = 11$; 11×3; $33-35$; 2; $\frac{759375}{7} = 108482 \times 1$; $= 1$)

$$x = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$$

$$= (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$$

$$= (140 + 63 + 30) \bmod 105$$

$$= 233 \bmod 105$$

$$= 23$$

$$105 \overline{)233}\ 2$$
$$210$$
$$23$$

Here the x value remains same but a_1, a_2, a_3 mod value changes.

$$23 \equiv a_1 \bmod 3 \quad a_1 = 2$$

$$23 \equiv a_2 \bmod 5 \quad a_2 = 3$$

$$23 \equiv a_3 \bmod 7 \quad a_3 = 2$$

Hence proved that x is Constant.

x is a Unique solution for all the equations.

$\Rightarrow$

Explain the network Security model with neat sketch?

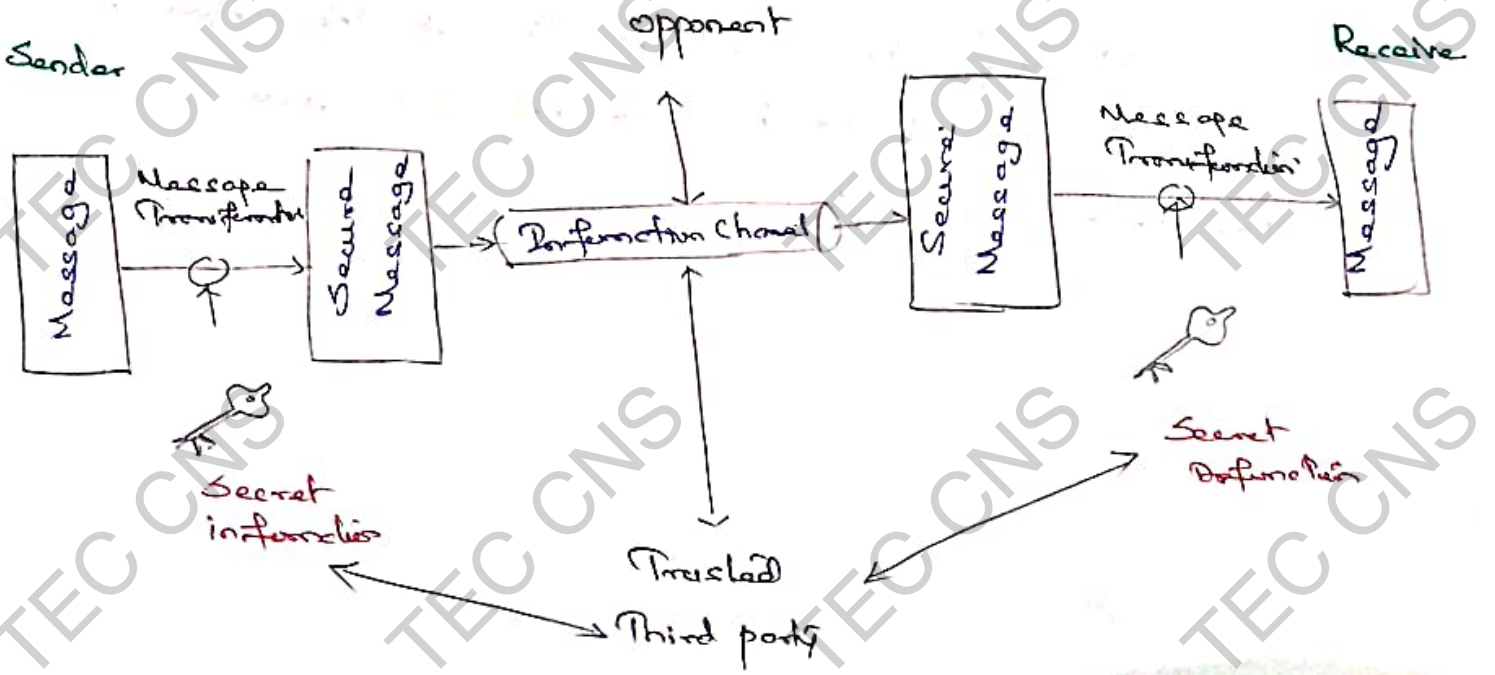
N/w Security Model with neat sketch:

N/w security Model exhibits how the security service has been designed over the n/w to prevent the opponent from causing a threat to the Confidentiality or authenticity of the information that is being transmitted through the n/w.

1. Transformation: of the information which has to be sent to the receiver. So that any opponent present at the intermediate channel is unable to read the message.

This includes the encryption of the message.

It includes the additional code during the transformation of the information, which will be used in verifying the identity of the authentic receiver.



2. Secret information: b/w Sender and the receiver of the which the opponent must not any else.

The encryption key which is used during the encryption of the message at the Sender's end and also during the decryption of message at receiver's end.

3. Trusted third party: which should help the responsibility of distributing the secret information (key) to both the communicating parties and also prevent it from any opponents.

→ The n/w security model print the two communicating parties Sender and receiver who mutually agree to exchange information

→ But Sender cannot send the message on the information channel in the readable form as it will be have a threat being affected by the opponent.

→ Sending the message through the information channel, it should be transformed into an unreadable format.

(X) N.V.U. Expected Question

University Question Paper (Q.) Draw the general structure of DES and explain Encryption and Decryption?

DES (Data Encryption Standard)

-> The Data Encryption Standard (DES) is a Symmetric-key block cipher.

-> DES is published by the National Institute of Standard and Technology (NIST) in the year 1977.

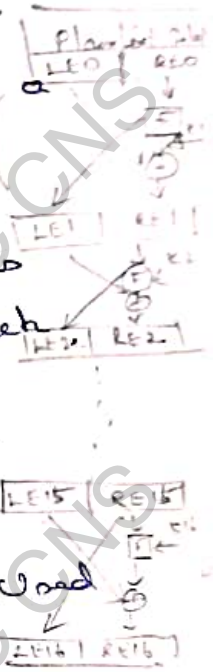
-> It is the based on the Feistel Structure in which the plaintext is Seperated into two halves.

-> It takes input as 64-bit plaintext and a 56-bit key to produce 64-bit Ciphertext.

-> Before processing, the entire plain text is Seperated into two pieces of 32 bits each.

-> Same operation is done on each portion.

-> Each pieces goes through 16 rounds of operation before the final permutation is used to obtain the 64-bit Ciphertext.



DES Algorithm steps:-

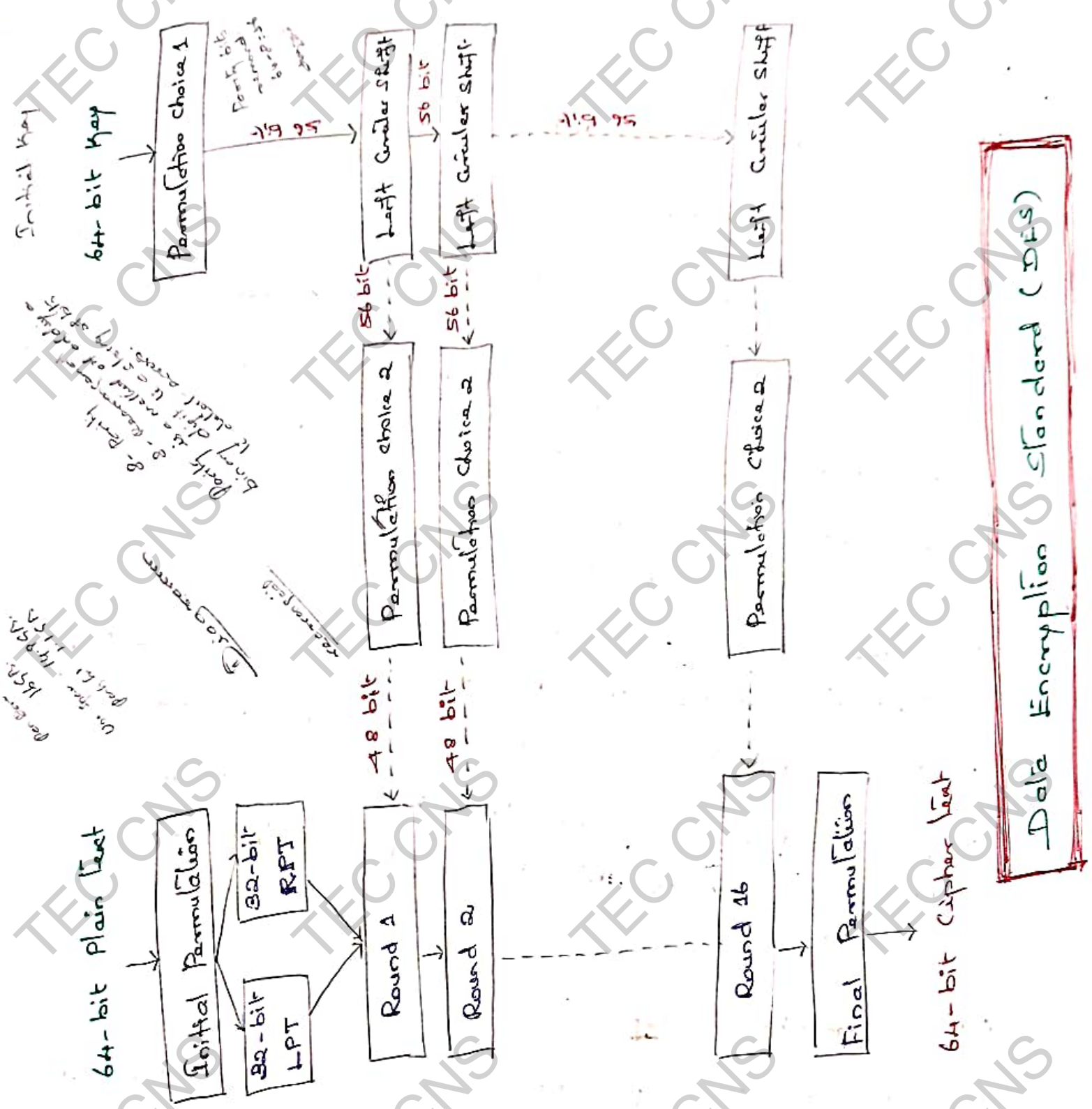
1) In the first step, the 64-bit plain text block is handed over to an initial Permutation (IP) function.

2) The initial permutation is performed on Plain text.

3) Next, the initial Permutation (IP) produces two halves of the permutation block.

Say: Left plain Text (LPT 32 bit)

Right plain Text (RPT 32 bit)



4) Now each LPT and RPT go through 16 rounds of encryption process.

5) In the end, LPT and RPT are rejoined and a Final Permutation (FP) is performed on the Combined block.

6) The result of this process produces 64-bit Cipher text.

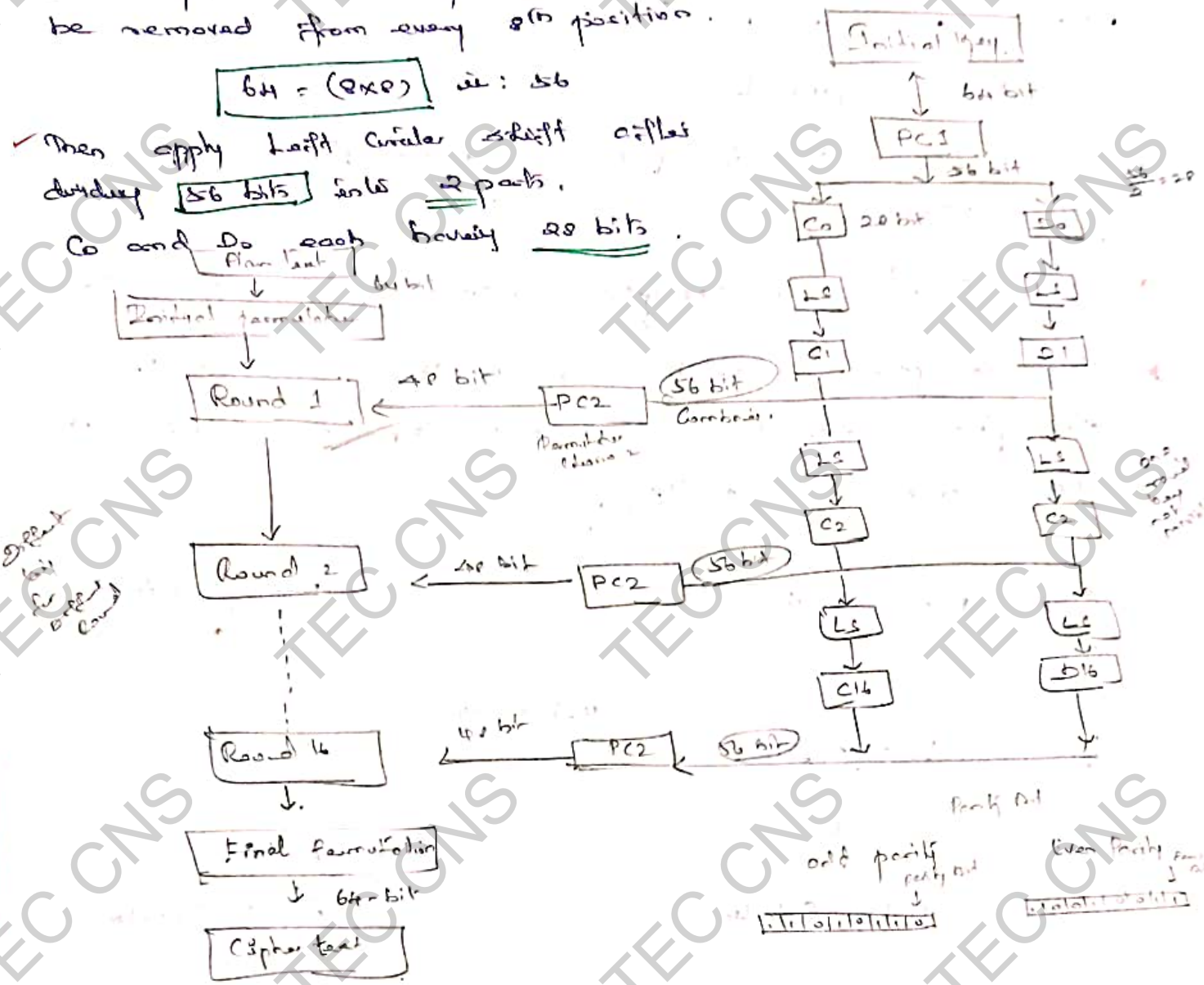
Brief Explanation in depth :- DES.

- Initially, 64 bit, ⑧ parity bits are to be removed from every 8th position.

$64 - (8 \times 8)$ i.e : 56

- Then apply Left Circular shift after dividing 56 bits into 2 parts.

Co and Do each having 28 bits.



Left Circular shift.

- Move the bits based on Round number.

→ for Round 1, 2, 9, 16 — ① bit shift

→ other Rounds — ② bit shift

In PC2,

- $C_1 + C_2$ are combined to form 56 bits again.

Permutation choice 2 is applied,

56 bit are rearranged, permuted and

48 bits are selected

↓

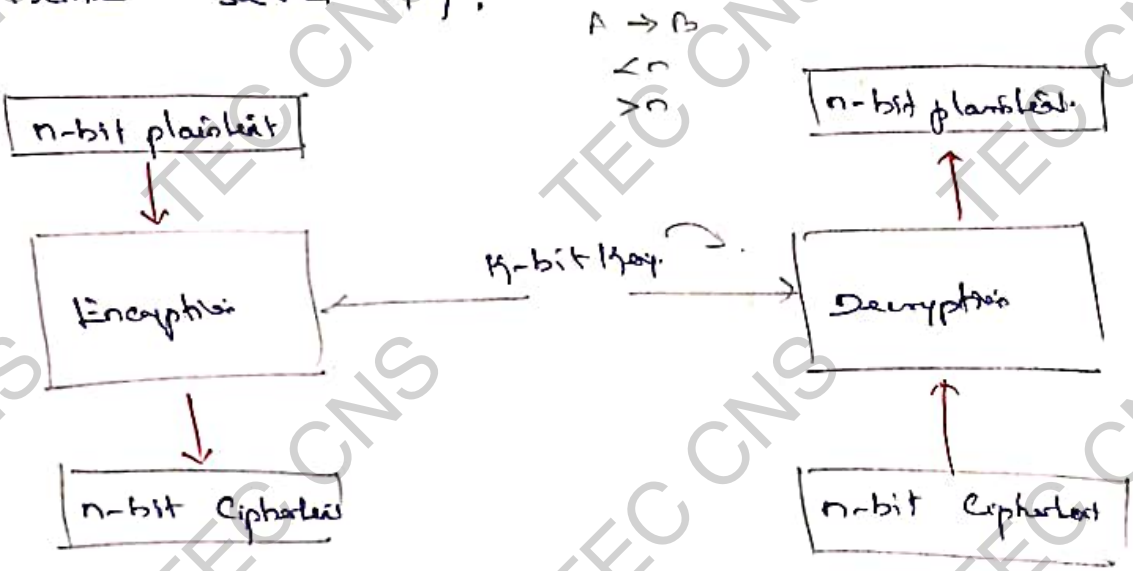
Key for Round ①

→

Symmetric-Key Modern Block Cipher:

A symmetric-key modern block cipher encrypts an n-bit block of plaintext or decrypts an n-bit block of ciphertext.

* The encryption or decryption algorithm uses a k-bit key.
* The decryption algorithm must be the inverse of the encryption algorithm, and both operations must be use the same secret key.



* If the message has fewer than n bits, padding must be added to make it an n-bit block.
* The message more than n-bits it should be divided into n-blocks and the appropriate padding must be added to the last block if necessary.
* The common values for n are 64, 128, 256 or 512 bits

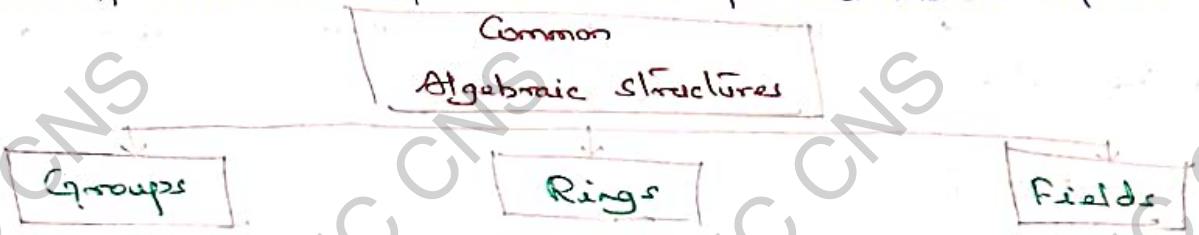
$$|M| + |Pad| = 0 \bmod \text{block size}.$$

Algebraic structures :-

Cryptography requires set of integers and specific operations that are defined for those sets

The combination of the set and the operations that are applied to the elements of the set is called an algebraic structure.

Groups, rings, and fields are the fundamental elements of a branch of mathematics known as abstract algebra or modern algebra



Groups:-

A group G, denoted by $\{G, *\}$ is a set of elements with a binary operation denoted by • that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G, such that the following axioms are satisfied.

i) **Closure** :- if a and b $\in$ G then

$$a \cdot b \in G$$

ii) **Associative**:-

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall \; a, b, c \text{ in } G$$

iii) **Identity element**:- There is an element e in G, such that

$$a \cdot e = e \cdot a = a \quad \forall \; a \text{ in } G$$
$$a + 0 = 0 + a = a \quad \forall \; a \text{ in } G.$$

iv) **Inverse element**:- For each a in G, there is an element a^{-1} in G, such that $a * a^{-1} = a^{-1} * a = e$

$$a \cdot a' = a' \cdot a = e$$

v) **Commutative** :- $a * b = b * a$ for all a, b in G.

If a group has a finite no: of elements it is referred to as a **finite group** and the order of the group is equal to the number of elements in the group. Otherwise the group is an **infinite group**.

A group is said to be **abelian**, if it satisfies the following additional condition

v) Commutative :- $a \cdot b = b \cdot a$ $\forall$ a, b in G .

Cyclic Groups :-

A Group G is Cyclic if every element of G is a power a^k (k is an integer) of a fixed element $a \in G$.

The element a is said to generate the group G or to be a generator of G.

A Cyclic group is always abelian and may be finite or infinite.

Cyclic Subgroup :-

If a Subgroup of a group can be generated using the power of an element, the subgroup is called the Cyclic subgroup.

$a^n \rightarrow a \cdot a \cdot a \cdot \ldots \cdot a$ (n times)

Example : Cyclic Group :

✓ The group $G = (Z_6, +)$ is a Cyclic group with two generators

$g = 1$ and $g = 5$

✓ The group $G = (Z_6, *)$ is a Cyclic Group with two generator

$g = 3$ and $g = 7$

Lagrange's theorem :-

Assume that G is a group, and H is a subgroup of G.

If the order of G and H are $|G|$ and $|H|$, resp/- then based on this theorem

$$\frac{O(G)}{O(H)}$$

Order of an Element :-

The order of an element is the order of the cyclic group it generates.

Ex:-

In the Group $G_1 = \langle Z_6, + \rangle$ the order of the elements are

$ord(0) = 1$
$ord(1) = 6$
$ord(2) = 3$
$ord(3) = 2$
$ord(4) = 3$
$ord(5) = 6$

Rings :-

A ring R, some times denoted by $(R, +, \times)$ is a set of elements with two binary operations called addition and multiplication, such that for all a, b, c in R the following axioms are satisfied

i) ii) iii) iv) v)

R is an abelian group with respect to addition

vi) closure under multiplication :

$a, b \in R$

then $ab \in R$

vii) Associativity of Multiplication :-

$a(bc) = (ab)c \quad \forall \quad a, b, c \text{ in } R$

viii) Distributive laws :-

$(a+b)c = ac + bc \quad \forall \quad a, b, c \text{ in } R$

$a(b+c) = ab + ac \quad \forall \quad a, b, c \text{ in } R$

A ring is said to be Commutative if it satisfies following additional Condition:

ix) Commutativity of Multiplication:

$ab = ba \quad \forall \quad a, b \text{ in } R$

x) Multiplicative identity:

$1 \in R$ such that $a1 = 1a = a \quad \forall \quad a \in R$

xi) No Zero divisors:-

$a, b \in R$ and $ab = 0$

then

$a = 0$ or $b = 0$

Fields:-

A field F, sometimes denoted by $(F, +, \times)$ is a set of elements with two binary operations called addition and multiplication such that for all a, b, c in F the following axioms are obeyed

i) – xi)

xii) Multiplicative inverse:-

$a \in F$, except 0

$a^{-1} \in F$ then

$aa^{-1} = a^{-1}a = 1$

Permutation Groups:-

A permutation of a set A is a function from A to A that is both 1-1 and onto.

Qn: Find the 8-bit word related to the polynomial x^6+x^3+x

x^7	x^6	x^5	x^4	x^3	x^2	x^1	x^0
0	1	0	0	1	0	1	0

This is related to the 8-bit word 01001010

Note:- Polynomial representing n-bit words use two fields.

GF(2) and GF(2^n)

Qn: Figure show how we can represent the 8-bit word (10011001) using a polynomial.

n-bit word	1	0	0	1	1	0	0	1
Polynomial	$1x^7$	$0x^6$	$0x^5$	$1x^4$	$1x^3$	$0x^2$	$0x^1$	$1x^0$

First Simplification $\quad 1x^7+1x^4+1x^3+1x^0$

Second Simplification $\quad x^7+x^4+x^3+1$

$x^0=1$

Points:-

* A prime polynomial cannot be factored into a polynomial with degree of less than n. Such polynomials are referred to as Irreducible polynomials.

Ex:

$(x+1)$ - degree 1

(x^2+x+1) - degree 2

(x^3+x^2+1) - degree 3

$(x^4+x^3+x^2+x+1)$ - degree 4

} Irreducible polynomials.

Galois field (GF)

Addition operation on polynomials are the same operation

Q: $(x^3+x^2) \bmod 2$

$= 2x^2$ (Coefficient belongs to GF(2))

$= 2x^2 \bmod 2$

$= [(2 \bmod 2) \times (x^2 \bmod 2)] \bmod 2$

$= [0 \times (x^2 \bmod 2)] \bmod 2$

Subtraction:-

Q:- $(x^2-x^2) \bmod 2$

$= (x^2-x^2) \bmod 2$

$= 0 \bmod 2$

$= 0$

$\therefore (x^2+x^2) = (x^2-x^2) = 0$.

Example:- Solve $(x^5+x^2+x) \otimes (x^3+x^2+1)$ in $GF(2^8)$

⊗ - Symbol is mean polynomial addition.

Let us solve the above.

For the given $GF(2^8)$

$x^5+x^2+x = 0x^7+0x^6+1x^5+0x^4+0x^3+1x^2+1x^1+0x^0$

$x^3+x^2+1 = 0x^7+0x^6+0x^5+0x^4+1x^3+1x^2+0x^1+1x^0$

Mean polynomial addition ⊗.

$0x^7+0x^6+1x^5+0x^4+1x^3+0x^2+1x^1+1x^0$

This given is,

x^5+x^3+x+1

Note:-

0 XOR 0 - 0 (Same)

0 XOR 1 - 1 (Different)

1 XOR 0 - 1 (Different)

1 XOR 1 - 0 (Same)

Encryption:-

```
0 0 1 1 0 1 0 1   Plain Text
1 1 1 0 0 0 1 1   Secret key.
---------------
1 1 0 1 0 1 1 0   Cipher Text.
```

XOR

Decryption:-

```
1 1 0 1 0 1 1 0   Cipher Text
1 1 1 0 0 0 1 1   Secret key.
---------------
0 0 1 1 0 1 0 1   plain Text.
```

The addition in GF(2) means the exclusive-or (XOR) operation. So we can exclusive-or the two words, bits by bits. To get the result.

In the example:-

$x^5 + x^2 + x$ is 0 0 1 0 0 1 1 0

$x^3 + x^2 + 1$ is 0 0 0 0 1 1 0 1

Result is:- 0 0 1 0 1 0 1 1

The polynomial notation: $x^5 + x^3 + x + 1$

Qn:- Let us define a $GF(2^2)$ field in which the set has four 2-bit word.

$\{00, 01, 10, 11\}$

We can redefine addition and multiplication for this field in such a way that all properties of these operations are satisfied..

$GF(2^2) = \langle \{00, 01, 10, 11\}, \oplus, \otimes \rangle$

Addition:-

$\oplus$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$$\begin{array}{r} 1\ 0 \\ \oplus\ 0\ 0 \\ \hline 1\ 0 \end{array} \qquad \begin{array}{r} 1\ 0 \\ \oplus\ 0\ 1 \\ \hline 1\ 1 \end{array} \qquad \begin{array}{r} 1\ 0 \\ \oplus\ 1\ 0 \\ \hline 0\ 0 \end{array} \qquad \begin{array}{r} 1\ 0 \\ \oplus\ 1\ 1 \\ \hline 0\ 1 \end{array}$$

Multiplication:-

$\otimes$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01

The set is $\{00, 01, 10, 11\}$ $\quad 0x^1+1x^0$

Corresponding polynomial are:- $\quad 0x^1+0x^0 \quad 1x^1+0x^0 / 1x^1+1x^0$

$\frac{100}{0} \quad \frac{100}{1} \quad \frac{100}{x} \quad x+1$

Qn. Generate the elements of the field $GF(2^4)$ using the irreducible polynomial $f(x) = x^4 + x + 1$.

The elements $0, g^0, g^1, g^2$ and g^3 can be easily generated, because they are the first most of $0, 1, x^2, x^3$

$0 = 0\ 0\ 0\ 0$

$g^0 = 0\ 0\ 0\ 1$ $\qquad g^3\ g^2\ g^1\ g^0$

$g^1 = 0\ 0\ 1\ 0$

$g^2 = 0\ 1\ 0\ 0$

$g^3 = 1\ 0\ 0\ 0$

—.

Block Cipher modes of operation (DES).

1. Electronic Codebook (ECB)
2. Cipher Block chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

Block Cipher

* We need a mode of operation
* Fixed - length blocks.
* 'b' bits input and 'b' bits output <or>
* If the amount of PT is the encrypted is > 'b' bits
* Breaking the plaintext into 'b' bits in each block.
* 5 modes of operation defined by NIST.
* Different applications - Different modes of operations.

Modes of Operation.

In 4 +1 Counter Mode.

ECB:-

Deterministic

plaintext blocks $P_1, P_2 \ldots P_m$ are encrypted twice under the same key.

Partially - Initial and end

CBC: Load n-bit data.

Chain Format.

XOR

Initialization Vector.

CFB:- Ciphertext acts Stream operation

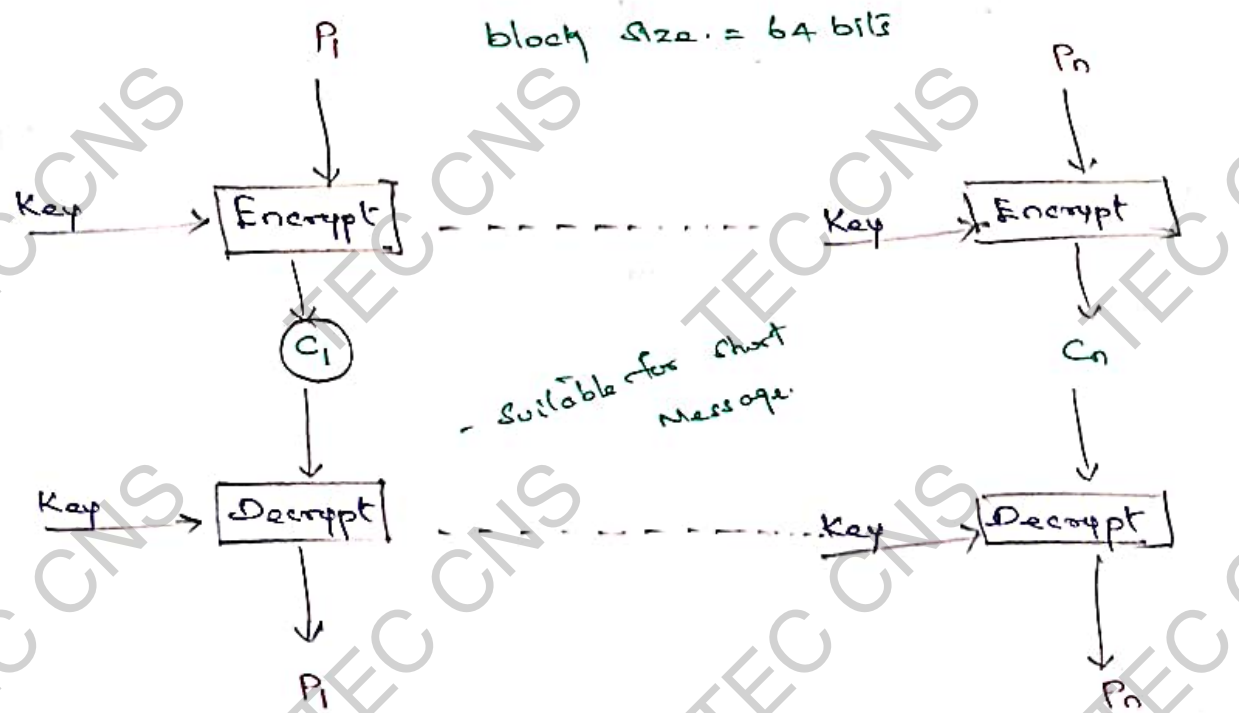
OFB:- None

Block Cipher Modes of operation:

There are 5 modes of operation.

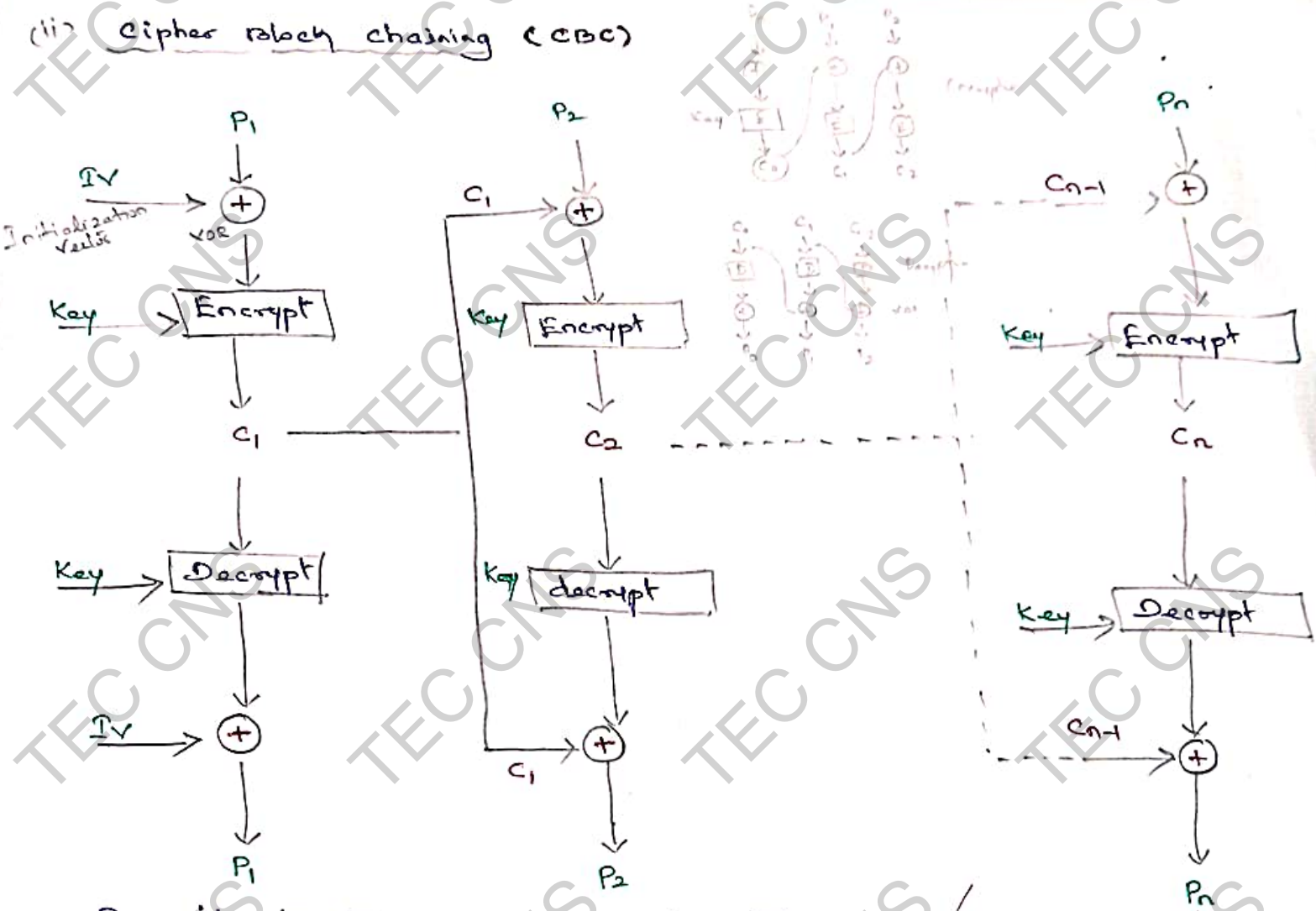
1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback Mode (CFB)
4. Output Feedback Mode (OFB)
5. Counter Mode (CTR)

(1) Electronic Code Book: (ECB)



* Each block of 64-plaintext bits is encoded independently using the same key

(ii) Cipher block chaining (CBC)

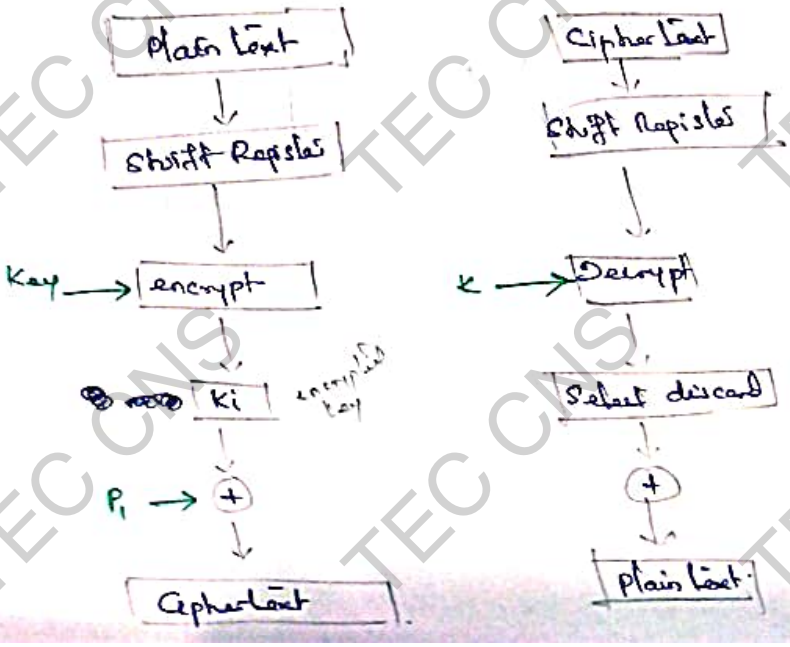


* The i/p to the encryption algorithm is the XOR of the next 64-bits of plaintext and preceding 64-bits of Ciphertext

(iii) Cipher Feedback Mode (CFB)

I/p is processed j bits at a time. Preceding Ciphertext is used as i/p to the encryption algorithm to produce pseudorandom o/p which is XOR with plaintext to produce next unit of Ciphertext.

Encryption parameter is not pedled.



(iii). Output Feedback Mode (OFB)

* It is similar to CFB, except that i/p is the encryption algorithm is the preceding DES output.
* A key stream is generated independently of the plaintext.
* Parallel encryption and decryption is advantage.
* Turns a block cipher into a synchronous stream cipher.

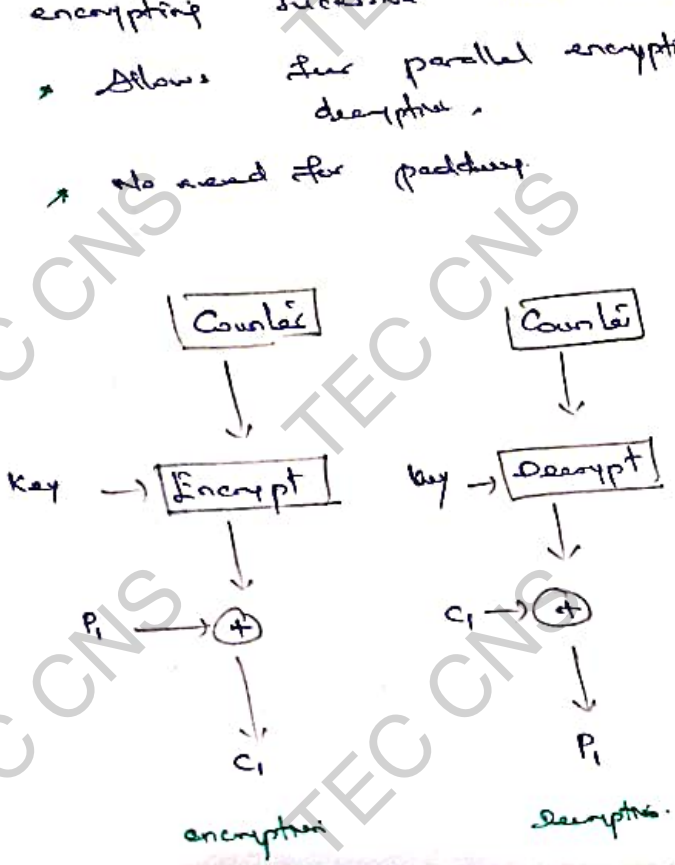
Stream Cipher:

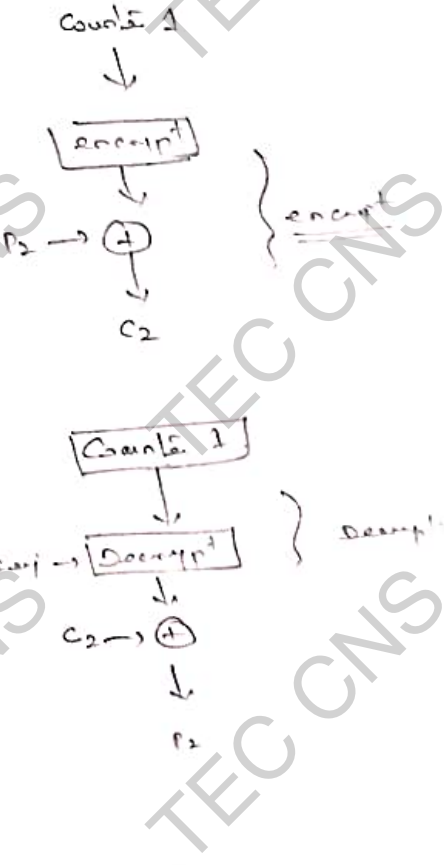
- plaintext : binary string
- key stream : a pseudorandom bit string.
- Ciphertext : bit wise XOR (addition mod 2) of plaintext and key stream.
- Decryption : bit-wise XOR of Ciphertext and key stream.

Ex:- P : 1000110101011110110 C : 11000111100011011110
K : 0100101011010011011 where C = P⊕K (encryption),
P = C⊕K (decryption).

(iv). Counter mode:

* Turns a block cipher into a stream cipher by encrypting successive values of a Counter
* Allows for parallel encryption and decryption.
* No need for padding.





Ingredients Symmetric Cipher Model

There are 5 ingredients

a) Plain Text : Original message it be Communicated between Sender and receiver

b) Cipher Text :- encoded format of the Original message that Cannot be Understood by humans.

c) Secret Key :-
(K)
It is a value / String / text file used by the encryption and decryption algorithm to encode & decode.

d) Encryption (or Enciphering):

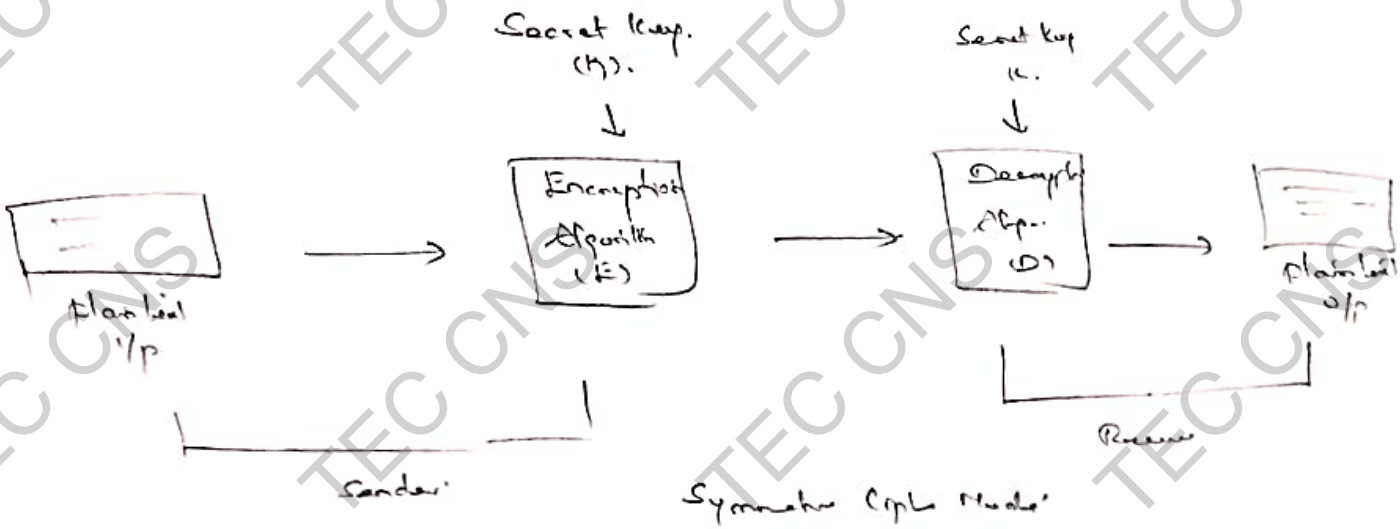
The Conversion of plain text is Cipher text

$$E(x, k) = y$$

e) Decryption (or Deciphering):

The Conversion of Cipher text to plain text. ie: reverse of encryption.

$$D(y, k) = x$$



(1) Comparision b/w public key and private key algorithm.

Symmetric key Cryptography. (public key).	Asymmetric key Cryptography (private key)
1. Same key is used for encryption and decryption	1. One key for encryption and another key for decryption.
2. Very fast	2. Slower.
3. Key exchange is big problem	3. Key exchange is not a problem
4. Also called. Secret key encryption	4. Also called. public key encryption.
5. The key must be kept secret	5. One of the two keys must be kept secret.
6. Cannot be used for digital signature	6. Can be used for digital signature.

AES

Advanced Encryption Standard :-

Introduction :-

* AES is Symmetric Key Cryptographic algorithm published by NIST.
* The algorithm was proposed by Rijndael. It is also known as Rijndael encryption algorithm.
* AES is replacement of DES
* AES works on block cipher technique. Size of plain text and cipher text must be same.
* An i/p key is also required to the AES algorithm. Same size of plain text.
* In AES, the data length (plain text size) of.

  128 bits — 10 rounds
  192 bits — 12 rounds
  &
  256 bits. — 14 rounds

  and supporting three different

* Key length

  128 bits
  192 bits
  and.
  256 bits

* AES Consist of Multiple rounds of processing different key bits like.

10 rounds for processing 128-bit key.
12 rounds 192-bit key.
and,
14 rounds. 256-bit key

* Encrypts data in blocks of 128 bits each.
* It takes 128 bits as input and outputs 128 bits of encrypted cipher text as output.
* It is performed using a series of linked operations which involves replacing and shuffling of the input data

Qn: Difference between DES and AES algorithm:

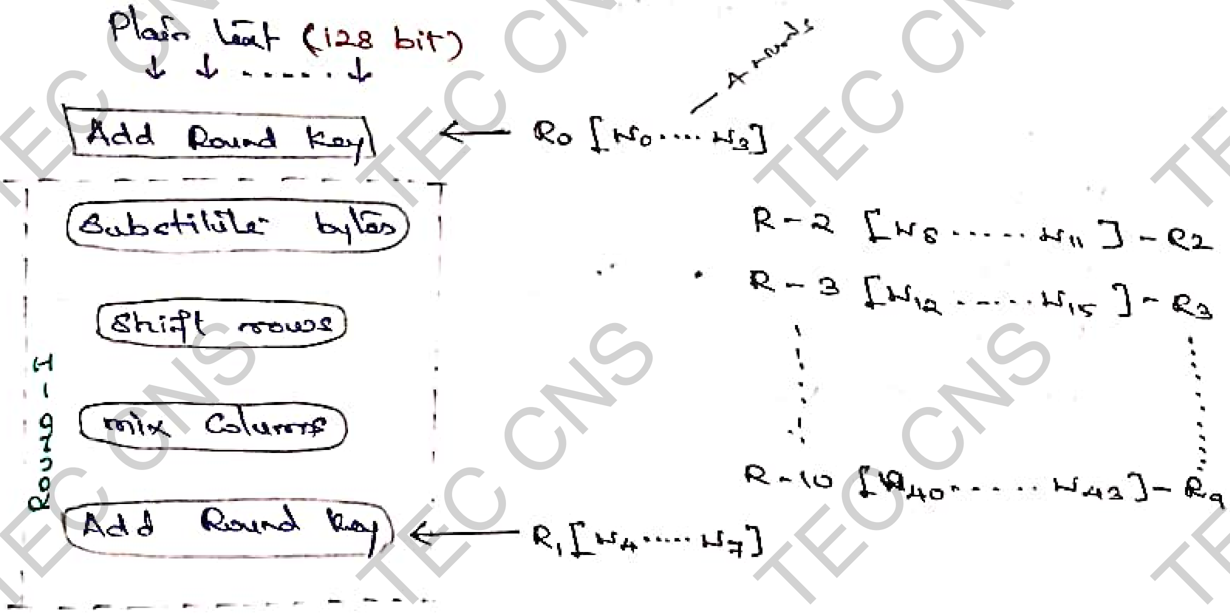
DES	AES
1. Used to encrypt plain text of 64-bit	1. Used to encrypt plain text of 128-bit
2. The key of 56-bit size	2. The key is of different sizes such as 128-bits, 192-bits and so on...
3. Less secure than AES	3. More secure than DES
4. It can be broken by brute force attacks	4. To date, AES has not been attacked
5. It is based on FEISTEL NETWORK	5. It is based on permutation and substitution network.

12-02-2024
11:20pm (19)

ADVANCED ENCRYPTION STANDARD (AES)

Overview:-

Block Size	–	128 bit Plain text
No: of Rounds	–	10 Rounds
Key Size	–	128 bit (4 words / 16 Bytes)
No: of SubKeys	–	44 SubKeys (44 words)
Each SubKey Size	–	32 bit / 1 word / 4 Bytes
Each Round	–	4 Sub keys (128 bit / 4 words / 16 Bytes)
Pre Round Calculation	–	4 SubKeys (128 bit / 4 words / 16 Bytes)
Cipher text	–	128 bit (4 words (16 bytes)
1 SubKey	–	32 bit
4 bytes	=	32 bit [∵ 1 byte = 8 bit]



1. Symmetric Cipher
2. Block Cipher
3. Plain text - 128 bits / 16 bytes

Key 128/192/256

1 byte = 8 bits
16 × 8
128

11 [illegible]

Input:- array 4×4

In_0	In_4	In_8	In_{12}
In_1	In_5	In_9	In_{13}
In_2	In_6	In_{10}	In_{14}
In_3	In_7	In_{11}	In_{15}

PT is represented in the i/p array

each cell = 8 bit
Total = 16 cells

16 bytes
= 16×8
⇒ 128 bit
= 4 words (32 each)

State:- array (or) Intermediate results → bits

word number

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Total ④ words

– Used to store intermediate states within the Rounds

16 bytes → stored column

Output: array

Out_0	Out_4	Out_8	Out_{12}
Out_1	Out_5	Out_9	Out_{13}
Out_2	Out_6	Out_{10}	Out_{14}
Out_3	Out_7	Out_{11}	Out_{15}

Need key

Key:- Array

w_1	w_2	w_3	w_4
K_0	K_4	K_8	K_{12}
K_1	K_5	K_9	K_{13}
K_2	K_6	K_{10}	K_{14}
K_3	K_7	K_{11}	K_{15}

→

w_0	w_1	w_2	......	w_{43}

1 column (1 word) (8 bit)

128 bit
(4 words)

Actually ④ words
They are expanded into ㊹ words.
each Round = 4 words
= 4 words × 10 Rounds
= 40 + 4 (for Add Round key)
= 44 words

initial step
1. Preprocessing
2. Substitute
3. Shift Rows
4. Mix Column – Absent in Round 10
5. Add key

Substitution bytes :-

S-Box

8 bits (each cell size).

Ex:-

0000 0001

First four bit → Row number → 0 - 15

Next four bit → Column number → 0 - 15

Size of Substitution array is 16×16 [256 bits].

256 values

10 - A
11 - B
12 - C
13 - D
14 - E
15 - F

0000 → row = 0

0001 → Column = 1

⇒ 7C [∵ From table].

⇒ 0111 1100

[7C = 12]

Substitution o/p

Shift Rows :-

Shift Row o/p

Row 0 → 0 bit shifted

Row 1 → 1 bit shifted

Row 2 → 2 bits shifted

Row 3 → 3 bits shifted

[Circular right shift].

0	1	2	3
4	5	6	7
8	9	10	11

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,1}$	$S_{1,2}$	$S_{1,3}$	$S_{1,0}$
$S_{2,2}$	$S_{2,3}$	$S_{2,0}$	$S_{2,1}$
$S_{3,3}$	$S_{3,0}$	$S_{3,1}$	$S_{3,2}$

Mix Columns:-

$S_{0,0}$	$S_{0,1}$	$S_{0,2}$	$S_{0,3}$
$S_{1,0}$	$S_{1,1}$	$S_{1,2}$	$S_{1,3}$
$S_{2,0}$	$S_{2,1}$	$S_{2,2}$	$S_{2,3}$
$S_{3,0}$	$S_{3,1}$	$S_{3,2}$	$S_{3,3}$

Inbuild Matrix Table. →

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix} \cdots \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$$

Column access.

$S'_{0,0}$	$S'_{0,1}$	$S'_{0,2}$	$S'_{0,3}$
$S'_{1,0}$	$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$
$S'_{2,0}$	$S'_{2,1}$	$S'_{2,2}$	$S'_{2,3}$
$S'_{3,0}$	$S'_{3,1}$	$S'_{3,2}$	$S'_{3,3}$

Add round key:

o/p from mix Column ⊕ Key (4 words).

$W[0,3]$

$R-1 \quad W[4,7]$

$\vdots$

$R-9 \quad W[40,43]$.

} Total 44 words.

Cipher text Possible.