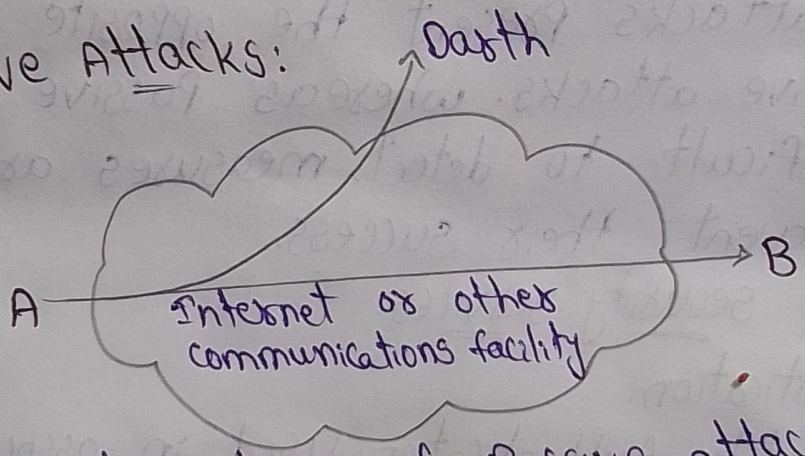
Assignment-1

1. Define the computer security. write the different types of security Attacks, security services and security mechanisms.

Computer security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

Types of security Attacks:-

1. Passive Attacks:



There are two types of Passive attacks:

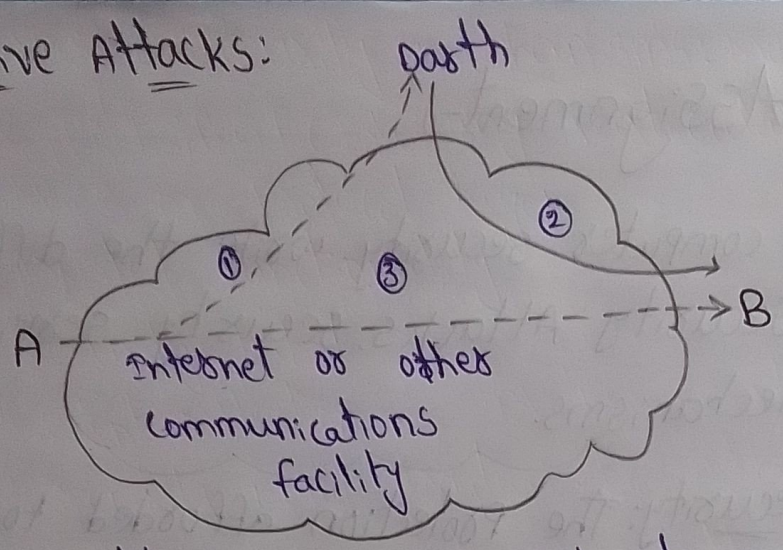
* the release of message contents
* traffic analysis

→ Passive attacks are very difficult to detect, because they do not involve any alteration of data.

→ It is feasible to prevent the success of these attacks, usually by means of encryption.

→ the emphasis in dealing with passive attacks is on prevention rather than detection.

2. Active Attacks:



→ Active attacks are subdivided into 4 categories

* Masquerade
* Replay
* Modification of messages
* Denial of service

→ Active attacks present the opposite characteristics of Passive attacks. whereas Passive attacks are difficult to detect, measures are available to prevent their success.

Types of security services:-

1. Authentication:
   * Peer Entity Authentication: Used in association with a logical connection to provide confidence in the identity of the entities connected.
   * Data-origin Authentication: In a connectionless transfer, Provides assurance that the source of received data is as claimed.
2. Access control: The prevention of unauthorized use of a resource.
3. Data confidentiality: The protection of data from unauthorized disclosure.

→ There are 4 types of data confidentiality:

Connection confidentiality
Connectionless confidentiality
Selective-field confidentiality
Traffic-flow confidentiality

4. Data Integrity: The assurance that data received are exactly as sent by authorized entity.
→ There are 5 types of data integrity
Connection Integrity with Recovery
Connection Integrity without Recovery
Selective-Field connection Integrity
Connectionless Integrity
Selective-Field Connectionless Integrity

5. Nonrepudiation: Provides Protection against denial by one of the Entities involved in a communication of having participated in all or part of the communication.
*Nonrepudiation, origin
*Nonrepudiation, destination

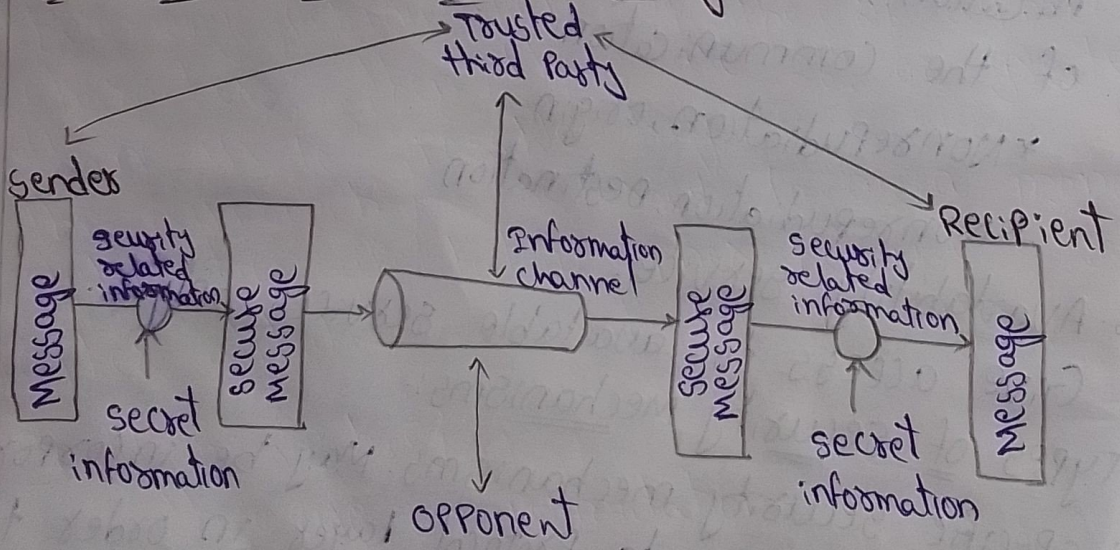
6. Availability service:
Give access to available services only.

Types of security mechanisms:-
1. specific security mechanisms: May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
*Encipherment
*Digital signature
*Access control
*Data Integrity

2. Pervasive security mechanisms: Mechanisms that are not specific to any particular OSI security service or protocol layer.
   * Trusted functionality
   * Security Label
   * Event Detection
   * Security Audit Trail
   * Security Recovery
3. Specific security mechanisms:
   * Authentication exchange
   * Traffic Padding
   * Routing control
   * Notarization

2. Explain the model for network security with diagram and write about block ciphers and stream cipher with diagram.

A model for network security:



→ A message is to be transferred from one party to another across some sort of internet service.

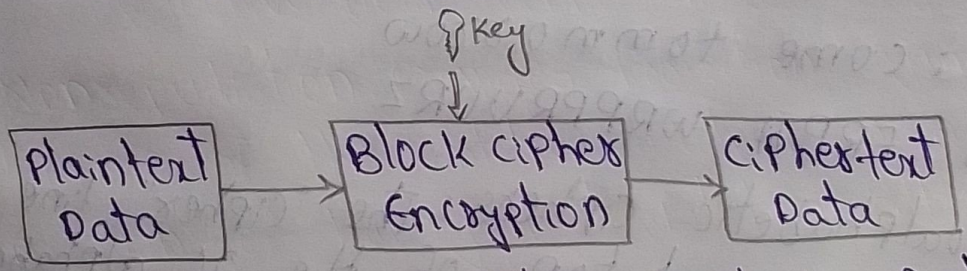
→ A security-related transformation on the information to be sent.

→ some secret information shared by the two principals, and it is hoped, unknown to the opponent.

→ A trusted third party may be needed to achieve secure transmission.

→ A third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

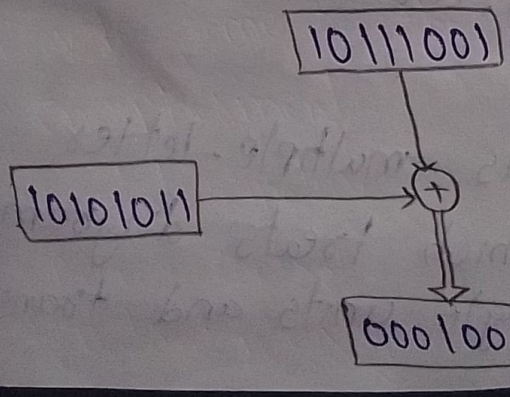
Block cipher: It is a cryptographic algorithm that encrypts data in fixed-sized blocks using a key and algorithm to protect data in transit or at rest.



→ Block ciphers are often used to protect data transmitted over networks or stored. and are a key component in the world of encryption.

Stream cipher:

A stream cipher is a method of encrypting text in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.



3. Discuss about the types of substitution and transposition techniques with their formulas. Give an example.

Substitution Techniques:-

1. Caesar Cipher: It involves replacing each letter of the alphabet with the letter standing three places further down the alphabet.

→ For encryption: $C = E(k, P) = (P + k) \bmod 26$

→ For decryption: $P = D(k, C) = (C - k) \bmod 26$

Ex: a b c d ------ w x y z
D E F G ------ Z A B C

Plain : come tomorrow

Cipher : FRPH WRPPRVURZ

2. Monoalphabetic Ciphers: The "cipher" line can be any permutation of the 26 alphabetic characters, then there are 26! or greater than 4×10^{26} possible keys.
This approach is referred to as a mono-alphabetic substitution cipher, because a single cipher alphabet is used per message.

Ex: if S = {a, b, c}
there are six permutations of S:
abc, acb, bac, bca, cab, cba.

3. playfair Ciphers:

→ It is also known as multiple-letter encryption cipher, which treats diagrams in the plaintext as single units and translates

these units into ciphertext diagrams.

→ The playfair algorithm is based on the use of a 5x5 matrix of letters constructed using a keyword.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

Ex:

Plain : ballon

Cipher : IBSUPMNA

4. Hill Cipher: It uses the concept of linear algebra created by Lester Hill (1929) - mathematician

→ It uses multiplication inverse and modulo.

→ Consider M^{-1} is a square matrix of M by Equation $M(M^{-1}) = (M^{-1})M = I$

Ex: $A = \begin{pmatrix} 5 & 8 \\ 17 & 3 \end{pmatrix}$ $A^{-1} \bmod 26 = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

$$AA^{-1} = \begin{pmatrix} 53 & 130 \\ 156 & 79 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$

Determinent of mxm is 5x3 - 17x8

$(\det(A)) \bmod 26 = (\det(A))^{-1}$

$(A^{-1})_{ij} = (\det A)^{-1} (-1)^{i+j} (D_{ij})$

$C_1 = (K_{11}P_1 + K_{21}P_2 + K_{31}P_3) \bmod 26$

$C_2 = (K_{12}P_1 + K_{22}P_2 + K_{32}P_3) \bmod 26$

$C_3 = (K_{13}P_1 + K_{23}P_2 + K_{33}P_3) \bmod 26$

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3) \begin{bmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{bmatrix}$$

$\therefore \boxed{C = PK \bmod 26}$

5. Polyalphabetic ciphers: It uses different monoalphabetic substitutions as one proceeds through the plaintext message.

→ These have following features

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

6. Vigenese cipher: The set of related monoalphabetic substitution rules consists of the 26 caesar ciphers with shifts of 0 through 25.

Encryption: $C_i = (P_i + K_i \bmod m) \bmod 26$

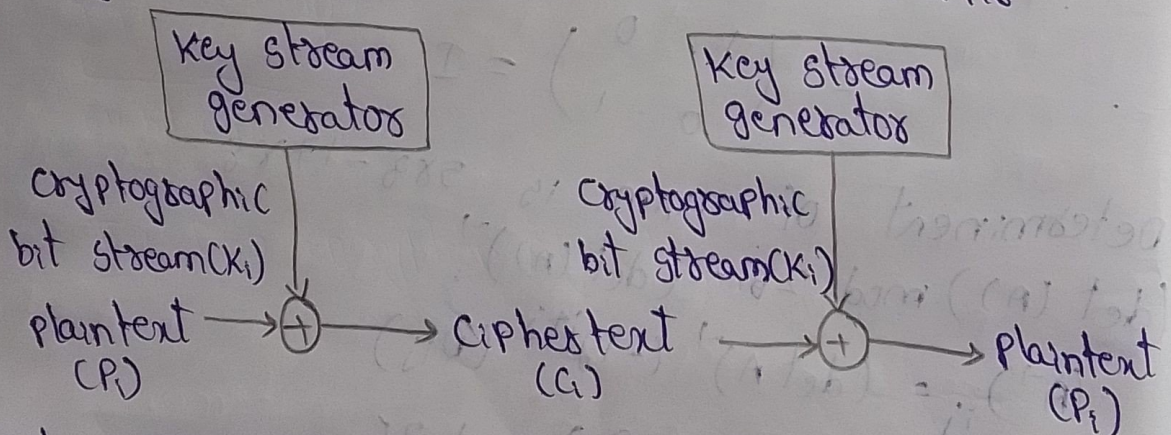
Decryption: $P_i = (C_i - K_i \bmod m) \bmod 26$

Ex: key : deceptivedeceptivedeceptive

plaintext : wearediscoveredsaveyourself

ciphertext : ZICVTWQNGRZGVTWAVZHCQYGLMGJ

7. vernam cipher: It was introduced by an AT&T engineer named Gilbert vernam in 1918.



→ It works on binary data rather than letters.

→ The system can be expressed as follows

$$C_i = P_i \oplus K_i$$

where, P_i = i^{th} binary digit of plaintext

K_i = i^{th} binary digit of key

C_i = i^{th} binary digit of ciphertext

$\oplus$ = exclusive-or (XOR) operation.

8. One-Time Pad: Each new message requires a new key of the same length as the new message.

→ It produces random output that beats no statistical relationship to the plaintext.

* Ciphertext: ANKYODKYUREPFJBYOJDSPLREYIUNOFDOIUERF PLUYTS

Key: Pxlmvmsydofuyrvzwc tnlebnecvgdupahfzzlmnyih

Plaintext: mr mustard with the candlestick in the hall.

Transposition Technique:-

All the techniques examined so far involve the substitution of a ciphertext symbol for a plain-text symbol.

→ The simplest such cipher is the rail fence technique

Ex: m e m a t r h t g p r y
e t e f e t e o a a t

The encrypted message is

MEMATRHTGPRYETEFETEOAAT

* Key: 4 3 1 2 5 6 7
Plaintext: a t t a c k p
o s t p o n e
d u n t i l t
w o a m x y z

Ciphertext: TTNAAPTMTSUOAODWCOIXKNLYPETZ

4. Draw the diagrams of DES for encryption and AES.

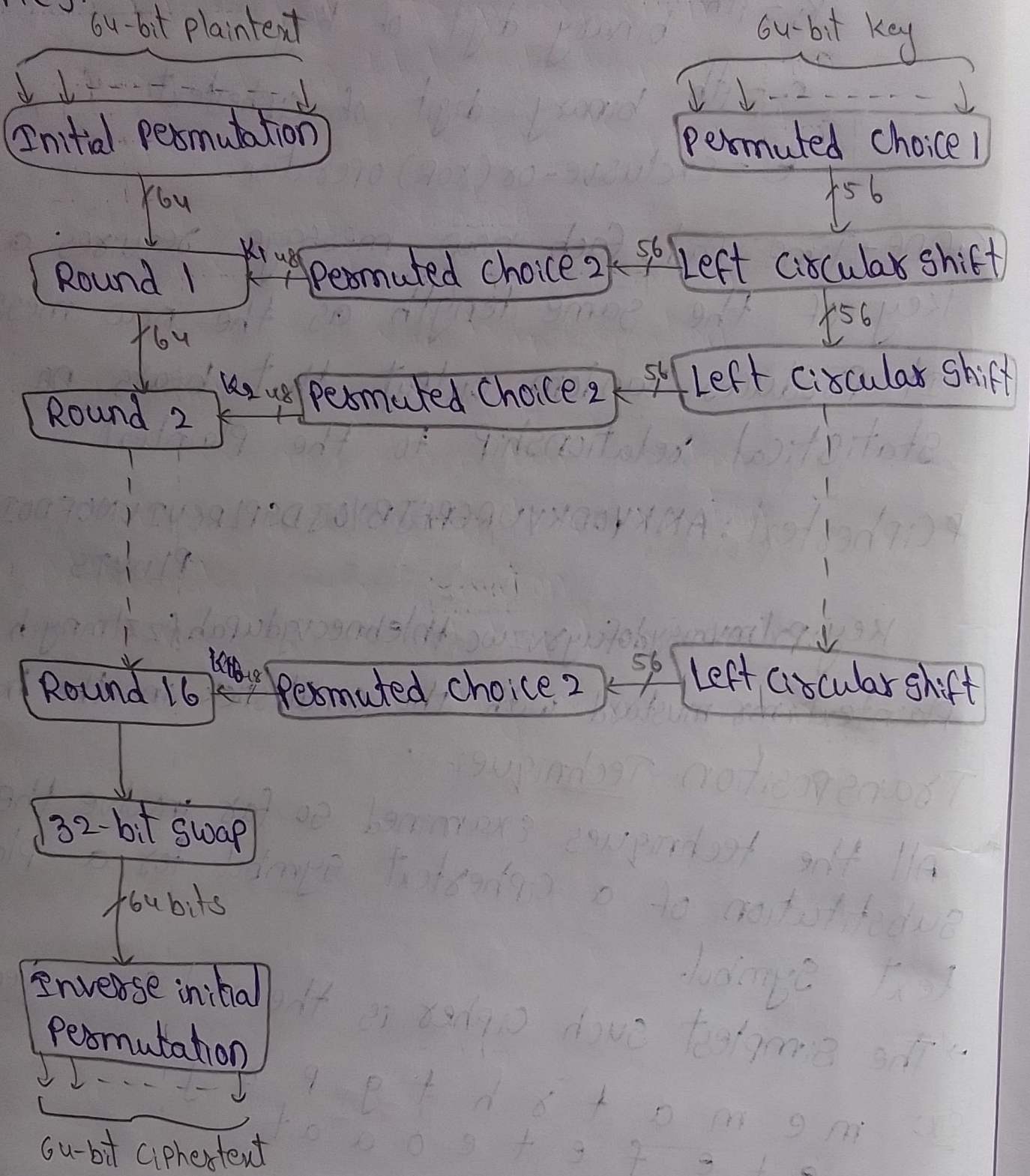


Fig: DES Encryption Algorithm

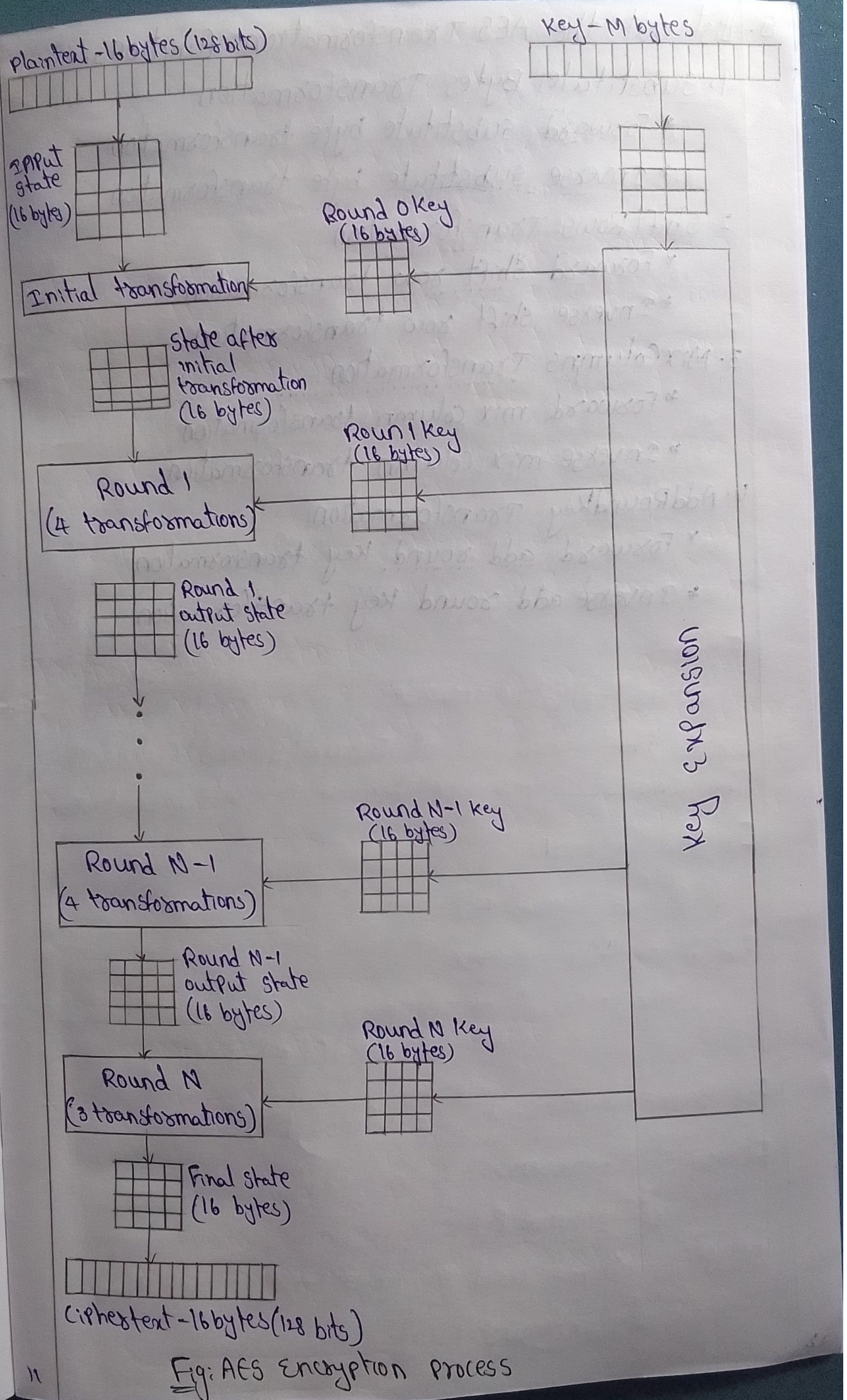


Fig: AES Encryption Process

5. List out the AES Transformation functions.

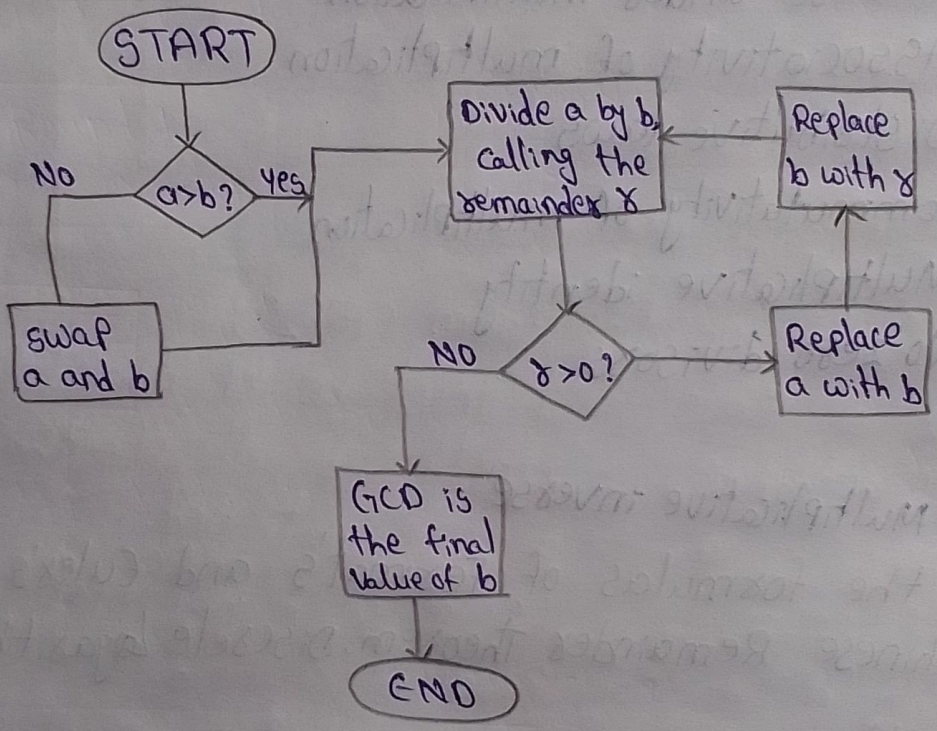
1. Substitute Bytes Transformation
   * Forward substitute byte transformation
   * Inverse substitute byte transformation
2. ShiftRows Transformation
   * Forward shift row transformation
   * Inverse shift row transformation
3. MixColumns Transformation
   * Forward mix column transformation
   * Inverse mix column transformation
4. AddRoundKey Transformation
   * Forward add round key transformation
   * Inverse add round key transformation

Assignment-2

1. Explain about Euclidean Algorithm. List out the properties of groups, rings and fields.

→ One of the basic technique of number theory is the Euclidean algorithm.

→ It is a simple procedure for determining the greatest common divisor of two positive integers.



The result is the following system of Equations:

$$a = q_1 b + r_1 \qquad 0 < r_1 < b$$

$$b = q_2 r_1 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \qquad 0 < r_3 < r_2$$

$$\vdots \qquad \vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$$d = \gcd(a,b) = r_n$$

Properties of Groups, Rings & Fields:-

Groups:

(A1) closure

(A2) Associative

(A3) Identity element

(A4) Inverse element

Rings:

(M1) closure under multiplication

(M2) Associativity of multiplication

(M3) Distributive laws

(M4) Commutativity of multiplication

(M5) Multiplicative identity

(M6) No zero divisors

Fields:

(M7) Multiplicative inverse

2. write the formulas of Fermat's and Euler's theorems The chinese Remainder theorem, Discrete Logarithms.

Euler's theorem:-

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

For a positive integer

$\phi(n)$ = count of integers $1 \le a < n$ such that $\gcd(a, n) = 1$

For Prime Powers: $a^{\phi(p^k)} \equiv 1 \pmod{p^k}$

Fermat's theorem:-

$$a^{p-1} \equiv 1 \pmod{p}$$

If p is prime and a is a +ve integer, then

$$a^p \equiv a \pmod{p}$$

The Chinese Remainder Theorem:-

$$M = \prod_{i=1}^{k} m_i$$

$$A \longleftrightarrow (a_1, a_2, \ldots a_k)$$

where $A \in Z_M$, $a_i \in Z_{m_i}$ & $a_i = A \bmod m_i$

$$C_i = M_i \times (M_i^{-1} \bmod m_i) \quad \text{for } 1 \le i \le k$$

$$A = \left(\sum_{i=1}^{k} a_i C_i\right) \pmod M$$

If $A \longleftrightarrow (a_1, a_2 \ldots a_k)$

$B \longleftrightarrow (b_1, b_2, \ldots b_k)$

then $(A+B) \bmod M \longleftrightarrow ((a_1+b_1) \bmod m_1, \ldots (a_k+b_k) \bmod m_k)$

$(A-B) \bmod M \longleftrightarrow ((a_1-b_1) \bmod m_1, \ldots (a_k-b_k) \bmod m_k)$

$(A \times B) \bmod M \longleftrightarrow ((a_1 \times b_1) \bmod m_1, \ldots (a_k \times b_k) \bmod m_k)$

Discrete Logarithms:-

from Euler's theorem $a^{\phi(n)} \equiv 1 \pmod n$

general Expression: $a^m \equiv 1 \pmod n$

Primitive root of n: $a, a^2, \ldots a^{\phi(n)}$

relatively prime to n: $a, a^2, \ldots a^{p-1}$

3. Examine the finite fields of the form GF(P) and $GF(2^n)$.

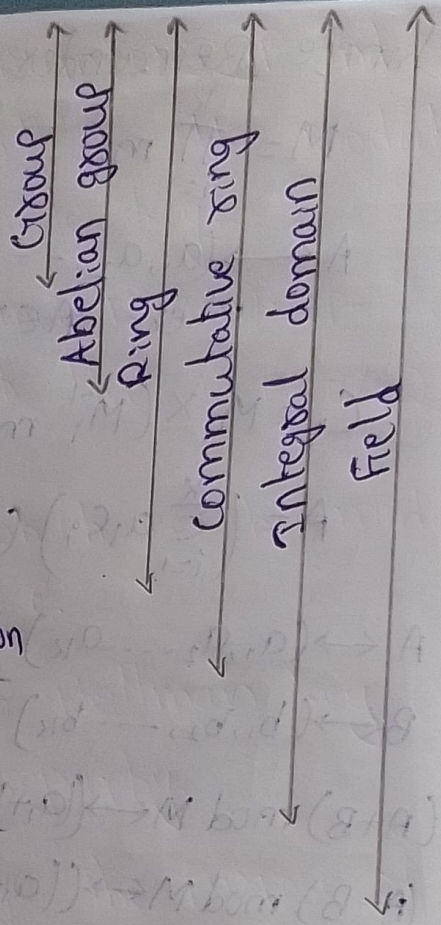
There are 2 types of finite fields

1. GF(P): Finite fields with P elements
2. $GF(p^n)$: Finite fields with p^n elements

→ Finite fields play a crucial role in many cryptographic algorithms.

→ It can be shown that the order of a finite field must be a power of a prime p^n, where n is a positive integer.

(A1) closure under addition
(A2) Associativity of addition
(A3) Additive identity
(A4) Additive inverse
(A5) Commutativity of addition
(M1) clouse under multiplication
(M2) Associativity of multiplication
(M3) Distributive laws
(M4) commutativity of multiplication
(M5) Multiplicative identity
(M6) No zero divisors
(M7) Multiplicative inverse



Finite fields of the form GF(2^n):-

→ order of finite field must be of the form p^n using modular arithmetic Z_p, all of the axioms for a field are satisfied.

→ For polynomials over p^n with $n>1$ operations modulo p^n do not produce a field.

→ Range of integers - 0 through 2^n-1, which fit into an n-bit word.

→ Cryptographic algorithms - attract by finite fields of the form GF(2^n).

→ If not use modular arithmetic - seen that does not result in a field. Instead how Polynomial arithmetic provides a fields for constructing the desire fields.

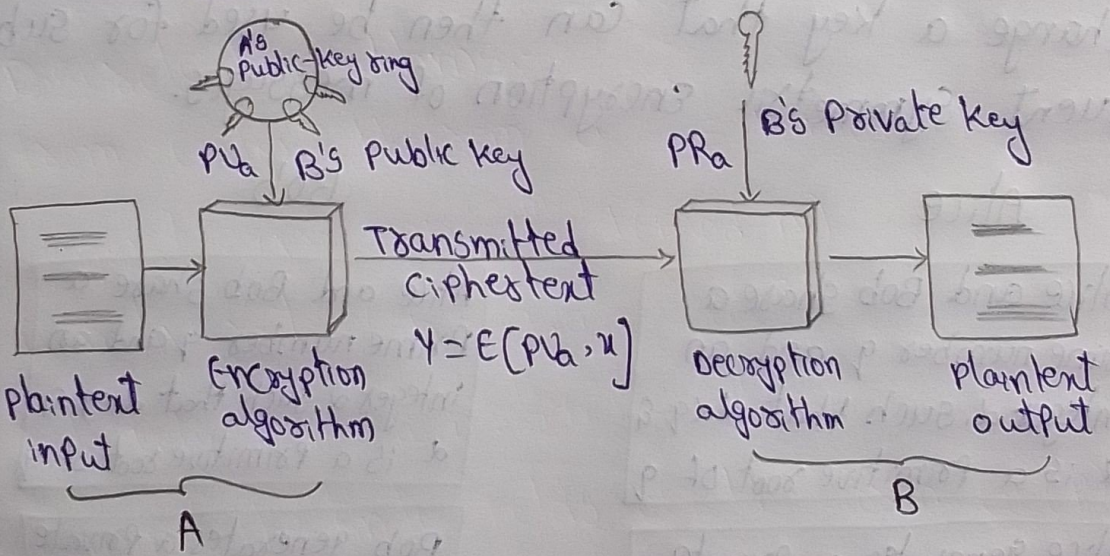
4. How the public key cryptography Algorithms and RSA algorithm works? Explain.

Public key cryptography:-

It is also known as asymmetric cryptography, uses two keys to encrypt and decrypt data:

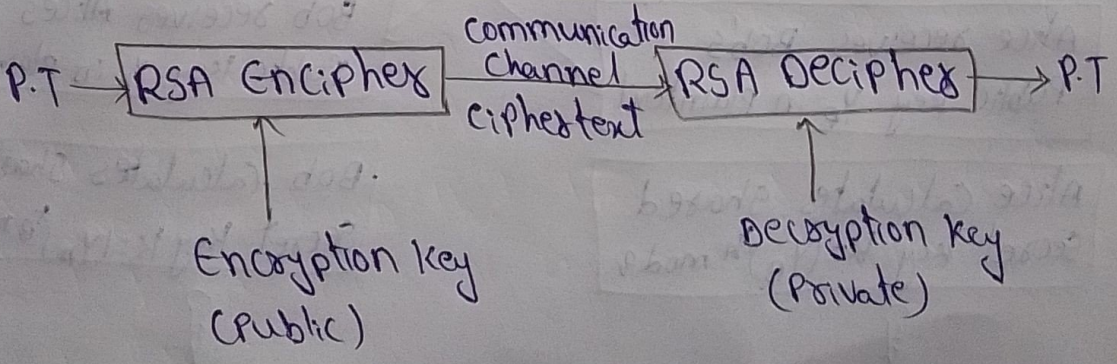
* Public key: This key can be shared openly and used to encrypt data.
* Private key: This key is kept secret and used to decrypt data.

→ The sender uses the public key to encrypt the data.
→ The recipient receives the encrypted data.
→ The recipient uses their private key to decrypt the data.



RSA algorithm:-

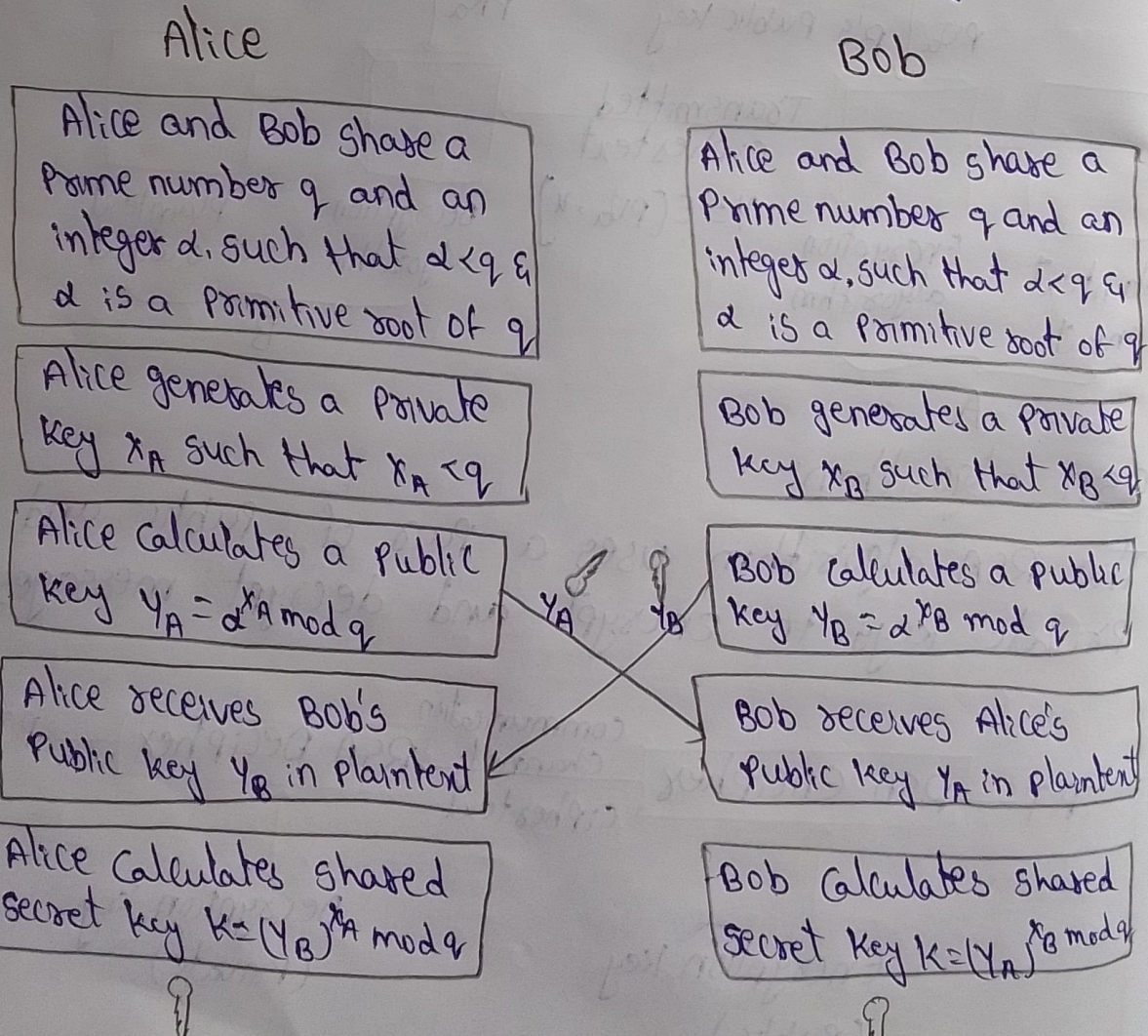
The RSA algorithm uses a pair of public and private keys to encrypt and decrypt messages.



→ Choose two large prime numbers, P and q.
→ Compute $n = p * q$, which will be the modulus for both the Public and Private keys.
→ Compute the totient function, $\phi(n) = (p-1)*(q-1)$.
→ Choose an integer e, such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$.
→ Compute $d = e^{-1} \bmod \phi(n)$, which is the modular multiplicative inverse of e.

5. Discuss about the Diffie Hellman Key Exchange and Elliptic Curve Cryptography.

Diffie Hellman Key Exchange:- The Purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent symmetric encryption of messages.



Elliptic curve cryptography:

→ To form a cryptographic system using elliptic curves, we need to find a "hard problem" corresponding to factoring the product of two primes or taking the discrete logarithm.

Consider the equation $Q = kP$

where, $Q, P \in E_p(a,b)$ and $k < p$.

→ It is relatively easy to calculate Q given k and P, but it is hard to determine k given Q & P. This is called discrete logarithm problem for elliptic curves.