# 1 Introduction of Cryptography

Cryptography is the study of mathematical techniques related to aspect of information security such as confidentiality, data integrity, entity authentication and data origin authentication. In other words, cryptography is the mathematical foundation on which one builds a secure system. It studies the way of securely storing, transmitting and processing information. It is used to hide information by mangling / mixing with some mathematical techniques and tools. It is not only used by spies but also in telecommunication, email, banking transaction etc. Cryptography is also used for information security including digital signatures which is used for verification and authentication of that are sent on the world wide web.

## Goals of Cryptography

All the information related objectives are divided into four categories:

1. Privacy or confidentiality.
2. data integrity
3. authentication
4. non-repudiation

### 1. Privacy or Confidentiality

It is a service to keep a content of information secured from all but those authorized to have it. There are numerous approaches

for providing confidentiality ranging from physical protection to mathematical algorithm which renders data unintelligible.

2. Data Integrity

It is the service that addresses the unauthorized alternation of data. To assure data integrity, one must have the ability to prevent data manipulation by unauthorized parties.

3. Authentication

It is a service related to identification which applies to both the entity and the information itself. Two parties entering a communication must identify each other. The information delivered over a channel should be authenticated with origin, data content, time sent etc. For this reason, this aspect of cryptography is divided into two categories; entity authentication and data origin authentication.

NOTE: Data authentication implicity provides data integrity.

4. Non repudiation

It is a service that prevents depends upon the entity from denying previous commitments or actions. Whenever this disputes arises due to entity denying that actions were taken, means to resolve the situation is necessary.

# Basic Terminologies using Cryptography.

1. Plain text
   It is the message to be communicated.

2. Cipher text: A disguise or mangle version of plain text.

3. Encryption: Process that turns plain text to cipher text.

4. Decryption: Process that turns cipher text back to plain text.

5. Cryptology: Study of encryption and decryption algorithm.

6. Cryptography: Application of cryptology.

7. Stream cipher: It operates on message symbol-by-symbol, bit-by-bit

8. Block cipher: Operates on message block-wise.

9. Diagraph: Operates on double letters.

10. Triagraph: Operates on three letters.

11. Polygraph: Operates on multiples letter.

12. Transposition cipher: Rearrange letter, symbol or bits in plain text

13. Substitution cipher: It replaces letters, symbols or bits in a plain

-text without changing the order.

14. Product cipher: Alternate transposition and substitution.

15. Crypto-analysis: The study of process by which an enemy tries to turn cipher text to plain text.

16. Crypto system: A system consisting of encryption and decryption algorithm:-

Three ways by which enemy turn cipher text to plain text
1. Steal or purchase or bribe to get the key.
2. Exploit sloppy implementation to get the key.
3. Crypto-analysis

OSI Security Architecture

↳ ITU-T X.800 defines a systamatic way for providing and defining security requirement known as OSI security architecture.

↳ It provides three aspect of security.
1. Security attack
2. Security mechanism
3. Security services.

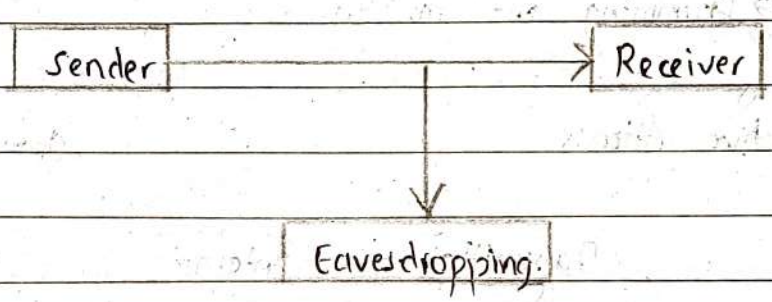
1. Security Attack

It refers to any action that comprises compromises the security of information of an organization. Information security deals with preventing attacks or failing to detect the attack on information system. There are four categories of security attack:

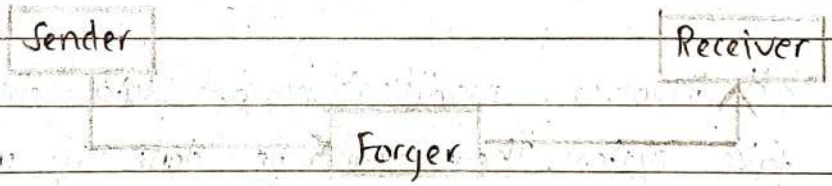
a) Interruption

Completely block or destroy the asset of system so that it becomes unavailable or unusable.

b) Interception




c) Modification




d) Fabrication

An unauthorized party inserts counterfeit objects into the system which can be considered as an attack on authenticity.

Generally, there are two types of attack:

A. Passive attack

B. Active attack.

## A. Passive Attack

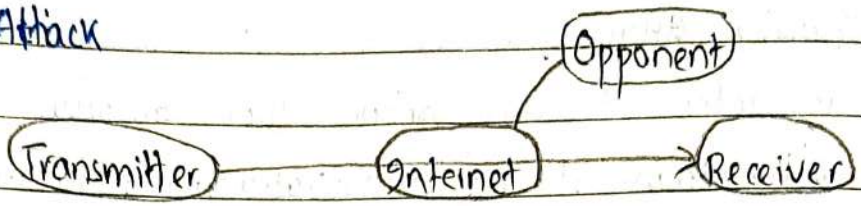



Fig: Passive attack.

↳ Passive attack are of nature of monitoring the transmission. The primary goal of the opponent is to obtain the information being transmitted.
↳ It may be done by message release or traffic analysis.
↳ Spamming and so on. difficult to detect

## B. Active Attack

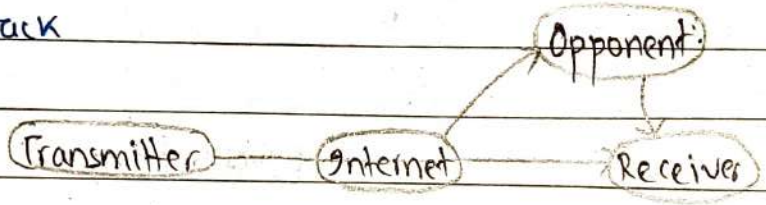



Fig: Active attack

↳ It involves modification of data string or creation of false system. These can be done by using a masquarade.
↳ Using different identity for preventing exposure of one's identity is masquarade.

Activities: categories

a) replay
b) modification
c) denial service
d) masquarade

## 2. Security Services

↳ It enhances the security of the data processing system. It is related with information transfer of an organization using security mechanism. The most widely used security services types are discussed below:

a) X.800

It is service provided by a protocol layer of communicating open system which ensures adequate security of the system.

b) RSE 2828

A communication or processing service provided by system to give specific kind of system protection to system resources.

↳ The different security services of X.800 are:

a) Authentication: Assurance of communicating entity is the one being claimed.

b) Access Control: Prevention of unauthorized use or access of resources.

c) Data Confidentiality: Protection of data from unauthorized disclosure.

d) Data Integrity: Assurance of data received is being sent by authorized entity.

e) Non-repudiation: Protection against denial by one of the party in communication.

3. Security Mechanism

↳ It deals with features, design tools to detect, prevent, or recover from security attack.

↳ No single mechanism that supports all the services is required.

↳ One particular element underlies many of the security mechanism in use.

↳ Security mechanism focus on:

a) Specific security Mechanism

- encipherment, digital signatures, access control authentication, traffic padding, routing control, notarization etc.

b) Persuasive security Mechanism

- trusted functionality, security labels, event detection, security audit trials, security recovery etc.

Generic Model of secure communication

In secure communication we use:

1. Model of Network Security
2. Model of Network Access Security.

1. Model of Network Security

Using this model require us to:

a) Design a suitable algorithm for secure transmission.

b) Generate secret info (key) used by the algorithm.

c) Develop method to distribute and share the secret info.

d) Specify a protocol enabling the principles to use the

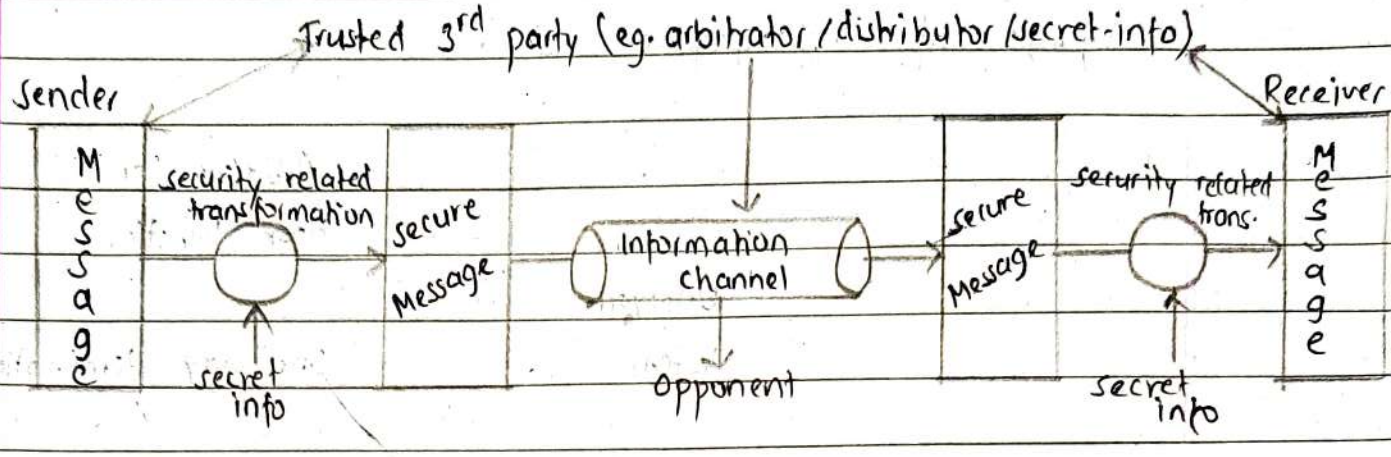



Fig: Model of Network security

transformation for security services.

2. Network of Network Access- Security

Opponent : humans (hackers, crackers), software (worm, trojans, virus etc.)
info system.

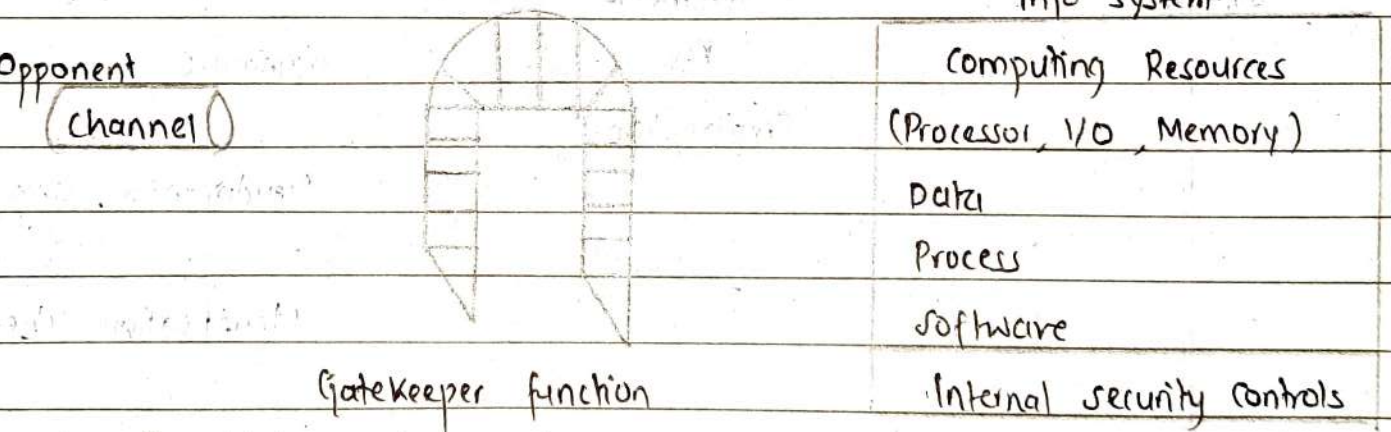



Fig: Model of Network Access Security

Using this model, it require us to:

a) select appropriate gatekeeper function to identify users.
b) Implement security controls to ensure only authorized access designated information source.
c) Trusted computer system may be useful to implement this model.

Categories of Cryptographic System

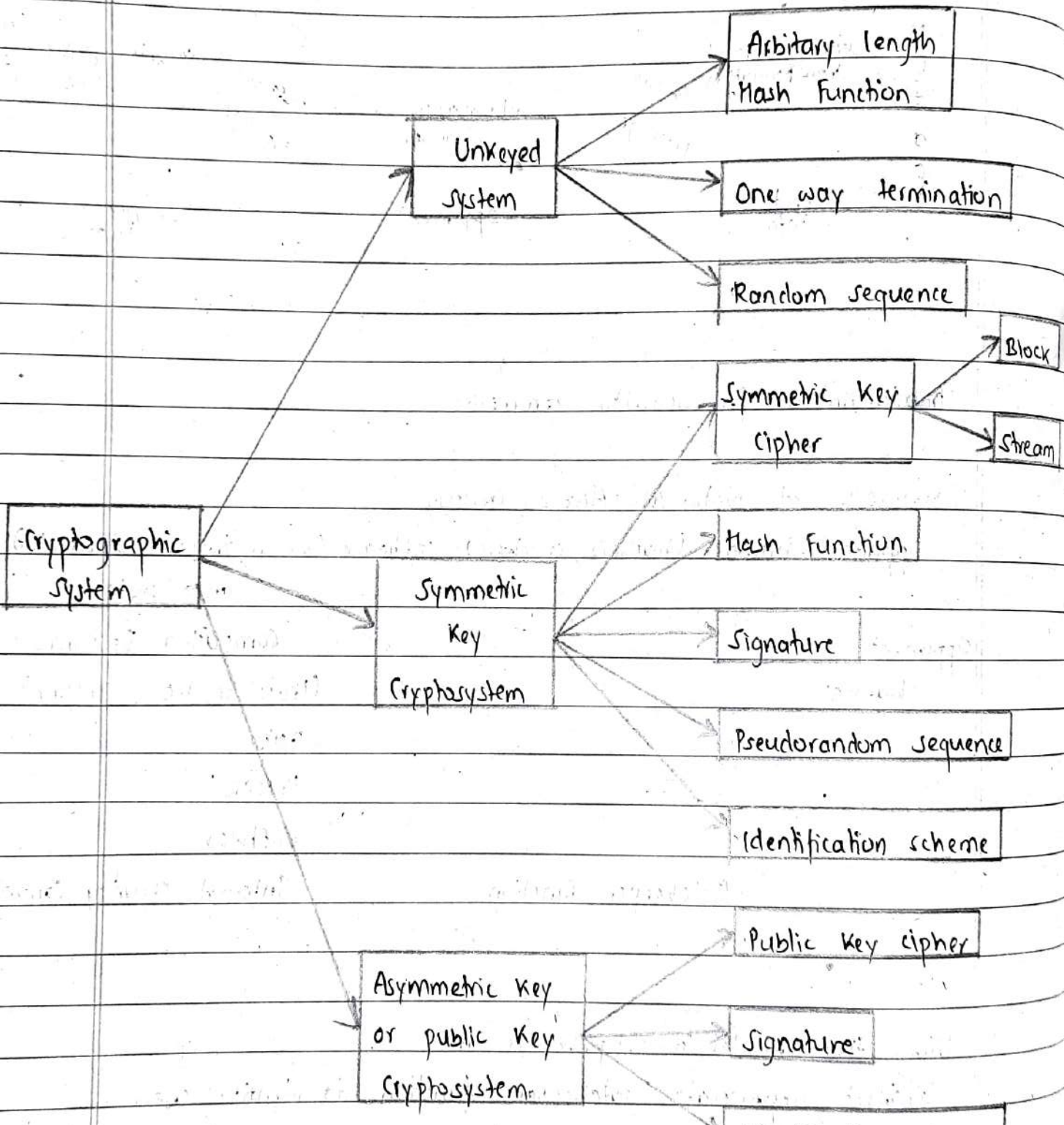



Fig: Taxonomy of Cryptographic Systems

The categorization premitively will be evaluated with respect to various criteria like:

1. Level of security
   → Defined by upper bound on the amount of work necessary to defeat the objective.

2. Method of operation
   → A system should provide very difficult functionality, depending upon mode of operation of use.

3. Performance
   → Efficiency of a system in a particular mode of operation.

4. Ease of implementation
   → Difficulty in realizing system in a particular instantiation.

## Conventional Encryption Model

1. Plain Text
2. Encryption algorithm
3. Secret key
4. Cipher Text
5. Decryption algorithm.

The traditional or conventional encryption model uses a single private key in which the sender and receiver share the same key. All classical encryption techniques / algorithms are private

key techniques and it was the only type used widely before the invention of public key in 1970. The figure below shows the conventional encryption model.

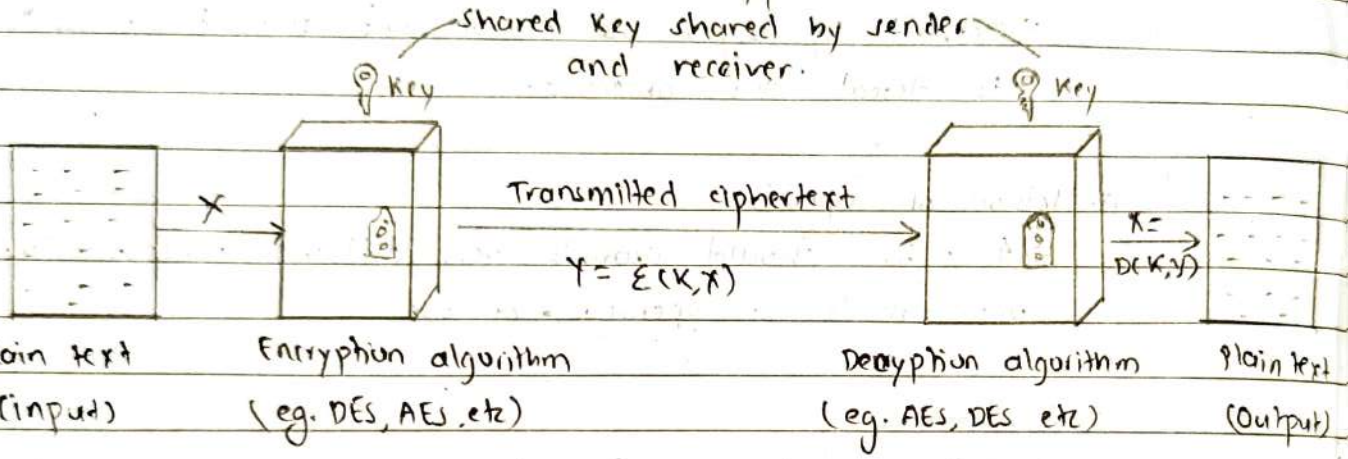



fig: Conventional Encryption Model.

Two requirements for transmission of message through conventional encryption model are:

1. A strong encryption algorithm.
2. A secret key K known to the receiver and sender only.

$$Y = E(K, X)$$

$$X = D(K, Y)$$

where X is plain text and Y is cipher text.

NOTES: If the encryption algorithm is known, a secured channel to distribute key should be implemented.

# 2 Classical Cipher Schemes

Classical substitution cipher

Here, the cipher text is obtained by replacing the letters of plain text with letters, symbols or numbers. If the plaintext is viewed as sequence of bits, the cipher text is obtained by replacing the plaintext bits pattern with cipher text bit pattern.

Ceaser's Cipher

It is the earliest known substitution cipher invented by Julius Ceaser for communicating with his military journals in war. In Ceaser's cipher, the cipher text is obtained by substituting each letter by an arbitary letter say 'm" and so on.

Eg: Plain text : Meet me after the party.

Using key m=3,

Cipher text: 3eet 3e after the party. (By replacing) X

OR

: Phhw ph diwhu dkh sduwb (By substituting)

Here, following transformation is used.

Plain: a b c d ... x y z

Cipher: d e f g ... a b c.

Mathematically, we assign each letter to a number starting from a=0 to z=25. Then, we have the Ceaser's cipher as:

$C = E(x+k) \bmod 26$ ie. $C = E(P)$

$P = D(x-k) \bmod 26$. ie. $P = D(C)$

The widely use ROT-13 encryption is simply a ceaser's cipher with an offset of 13. Vignère is also an encryption technique where ceaser's cipher is employed.

Crypto-analysis of ceaser's cipher

1. Predictable
2. less number of possible cipher (26)
3. A letter 'A' can mapped to 'A', 'B', 'C' ... to 'Z' at no time.
4. With simple try can be cracked within very less time.

Hill Cipher

↳ Invented by Lester S. Hill in 1929. It is polygraphic substitution cipher. The Hill cipher is the best example of block substitution cipher where groups of letter are encrypted together in equal length block.

• Encryption Scheme

The receiver and the sender must agree upon the key matrix in order to encrypt a message using Hill cipher. The key matrix 'A' of size MxN is used and 'A' should be invertible against modulo 26. The plain text is represented as a vector of size M. The following example uses a matrix 'A' of size 2x2 and the plain text will be inciphered in blocks of 2 characters. Let the key matrix be $A = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix}$

The message to ciphered is Mississippi OR MISSISSIPPI.

So, MISSISSIPPIK

$MI = \begin{bmatrix} 12 \\ 8 \end{bmatrix}$, $SS = \begin{bmatrix} 18 \\ 18 \end{bmatrix}$, $IS = \begin{bmatrix} 8 \\ 18 \end{bmatrix}$, $SI = \begin{bmatrix} 18 \\ 8 \end{bmatrix}$,

$PP = \begin{bmatrix} 15 \\ 15 \end{bmatrix}$, $IK = \begin{bmatrix} 8 \\ 10 \end{bmatrix}$

Now,

$MI = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix} \begin{bmatrix} 12 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 236 \\ 424 \end{bmatrix} \bmod m = \begin{bmatrix} 2 \\ 8 \end{bmatrix} = \begin{bmatrix} C \\ I \end{bmatrix} = CI$

$SS = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix} \begin{bmatrix} 18 \\ 18 \end{bmatrix} \bmod 26 = \begin{bmatrix} 504 \\ 738 \end{bmatrix} \bmod 26 = \begin{bmatrix} 10 \\ 10 \end{bmatrix} = KK$

$IS = GE$ & $SI = UW$ [20, 22]

$PP = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix} \begin{bmatrix} 15 \\ 15 \end{bmatrix} = \begin{bmatrix} 420 \\ 615 \end{bmatrix} \bmod 26 = \begin{bmatrix} 4 \\ 17 \end{bmatrix} = ER$

$IK = \begin{bmatrix} 3 & 25 \\ 24 & 17 \end{bmatrix} \begin{bmatrix} 8 \\ 10 \end{bmatrix} = \begin{bmatrix} 274 \\ 362 \end{bmatrix} \bmod 26 = \begin{bmatrix} 14 \\ 24 \end{bmatrix} = OY$

Finally, MISSISSIPPIK = CIKKGEUWEROY

$\therefore$ MISSISSIPPI = CIKKGEUWERO.

The plain text of MISSISSIPPI is CIKKGEUWERO. (cipher text).

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

Encode ur name using 2 bit key and 3 bit key.

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Q. Encrypt DOG using the key GYBMQKURP.

Sol^n

let the key be A = GYBMQKURP.

In matrix, $A = \begin{bmatrix} G & Y & B \\ M & Q & K \\ U & R & P \end{bmatrix} = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

and,

Plain text = DOG $= \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix}$

Now,

$$DOG = \begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \cdot \begin{bmatrix} 3 \\ 14 \\ 6 \end{bmatrix} \bmod 26 = \begin{bmatrix} 360 \\ 323 \\ 388 \end{bmatrix} \bmod 26 = \begin{bmatrix} 22 \\ 11 \\ 24 \end{bmatrix}$$

$\therefore$ DOG = WLY.

Q. Encode your name using 2 bit key and 3-bit key.

Sol^n

Name : ROJINA ie. Plain text : ROJINA

Using 2 bit key,

let the key be $\begin{bmatrix} 17 & 24 \\ 5 & 9 \end{bmatrix}$.

So, $RO = \begin{bmatrix} 17 \\ 14 \end{bmatrix}$, $JI = \begin{bmatrix} 9 \\ 8 \end{bmatrix}$, $NA = \begin{bmatrix} 13 \\ 0 \end{bmatrix}$

Now,

Now, $RO = \begin{bmatrix} 17 & 24 \\ 5 & 9 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ 14 \end{bmatrix} \bmod 26 = \begin{bmatrix} 625 \\ 211 \end{bmatrix} \bmod 26 = \begin{bmatrix} 1 \\ 3 \end{bmatrix} = BD$

$JI = \begin{bmatrix} 17 & 24 \\ 5 & 9 \end{bmatrix} \begin{bmatrix} 9 \\ 8 \end{bmatrix} \bmod 26 = \begin{bmatrix} 345 \\ 117 \end{bmatrix} \bmod 26 = \begin{bmatrix} 7 \\ 13 \end{bmatrix} = HN$

$NA = \begin{bmatrix} 17 & 24 \\ 5 & 9 \end{bmatrix} \begin{bmatrix} 13 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 221 \\ 65 \end{bmatrix} \bmod 26 = \begin{bmatrix} 13 \\ 13 \end{bmatrix} = NN.$

∴ Encoded name using 2 bit key is BDHNNN.

Using 3-bit key,

let key be, $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix}$

So,

$ROJ = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \begin{bmatrix} 17 \\ 14 \\ 9 \end{bmatrix} \bmod 26 = \begin{bmatrix} 72 \\ 222 \\ 312 \end{bmatrix} \bmod 26 = \begin{bmatrix} 20 \\ 14 \\ 0 \end{bmatrix} = UOA$

$INA = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{bmatrix} \begin{bmatrix} 8 \\ 13 \\ 0 \end{bmatrix} \bmod 26 = \begin{bmatrix} 34 \\ 97 \\ 160 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 19 \\ 4 \end{bmatrix} = ITE$

∴ Encoded name using 3 bit key is UOAITE. //

Decryption of Hill Cipher.

To decrypt the ciphertext obtained by hill cipher, we simply calculate the inverse of the key matrix and multiply it with the new cipher obtained during encryption and then take modulo 26 to obtain original plaintext.

Monoalphabetic Cipher

→ Rather than shifting alphabets, shuffle the letter arbitarily.
→ Each plaintext letter maps to a different random cipher letter.
→ Hence, Key is 26 letter long.
→ Each letter in plaintext is encoded by only one letter from cipher alphabet and each letter in cipher text represents only one letter in the plaintext.

Polyalphabetic Cipher

→ Each letter in plaintext can be encoded by any letter in the cipher alphabet and each letter in the alphabet represents different letters from plaintext each time it appears

ATBASH Cipher (Example of Monoalphabetic Cipher)

Plaintext A-M N-Z
Ciphertext Z-N M-A

Plaintext: R O J I N A = 17 14 9 8 13 0 & HENGAJU = 7 4 13 6 0 9 20
Cipher text: I L Q R M Z = 8 11 16 17 12 25. & SVMTZQF
∴ Hence, Cipher text of ROJINA HENGAJU is ILQRMZ SVMTZQF

Affine Cipher

Encryption: $E(x) = (ax+b) \bmod m$

and

Decryption: $D(x) = c(x-b) \bmod m$

where a and b are key values.

NOTE:

⇒ c is the modular multiplicative of a. ie. $a \times c = 1 \bmod m$. It is the number such that when you multiply a by it and keep taking away the length of the alphabet you get to 1.

⇒ a and m should be co-prime.

Q// Encode and decode the text 'AFFINE CIPHER' using key a=5 and b=8.

for:

| Plaintext | A | F | F | I | N | E | C | I | P | H | E | R. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| ax+b | 8 | 33 | 33 | 48 | 73 | 28 | 18 | 48 | 83 | 43 | 28 | 93 |
| (ax+b) mod 26 | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| Ciphertext | I | H | H | W | V | C | S | W | F | R | C | P. |

Now, We know, $ax \equiv 1 \pmod{26}$ ie. $ax = (27 \text{ or } 53 \text{ or } 79 \text{ or } 105 \ldots$

ie. $5x \equiv 1 \pmod{26}$

$\therefore c = 21.$

Then, Decrypting:

| Ciphertext | I | H | H | W | V | C | S | W | F | R | C | P |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x | 8 | 7 | 7 | 22 | 21 | 2 | 18 | 22 | 5 | 17 | 2 | 15 |
| c(x-b) | 0 | -21 | -21 | 294 | 273 | -126 | 210 | 294 | -63 | 189 | -126 | 147 |
| c(x-b) mod m | 0 | 5 | 5 | 8 | 13 | 4 | 2 | 8 | 15 | 7 | 4 | 17 |
| Plaintext | A | F | F | I | N | E | C | I | P | H | E | R. |

What happen when we take a=4 and b=5?
The symbols E and R will map to the same symbols 'V', which will result ambiguity during de-cipher.

Pigpen Cipher

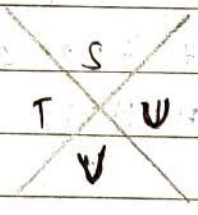
Q. De-cipher following using pigpen cipher.

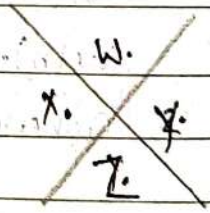
a) ⊐ ⌊ ⌈ ⌊ · □ ⌊ · ⊏ ⌈ ⌊ : ⊐ = PARALLELOGRAM

b) □ · < ⌋ ⊐ · ⌈ ⌊ · ⌋ > □ ⌈ ⌋ ⌊ = QUADRILATERAL

Key:

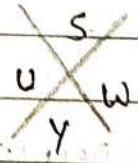
| | | | | | |
|---|---|---|---|---|---|
| A | B | C | J. | K. | L. |
| D | E | F | M. | N. | O. |
| G | H | I | P. | Q. | R. |




Another key:

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




## Polyalphabetic Cipher:

Substitution with keys

→ If sender and receiver agrees in a keyword, then a simple substitution can be generated from that keyword. Consider the keyword 'DEERMOOF'. First, write the letters without repetition. ie. 'DERMOF', place this at the beginning of the table and then proceed alphabetically to fill the rest.

| Plaintext | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext | D | E | R | M | O | F | A | B | C | G | I | J | K | L | M | N | P | Q | S | T |

| Plaintext | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|
| Ciphertext | U | V | W | X | y | z |

NOTE: If there exists any duplication in keywords, we only use that letter for once.

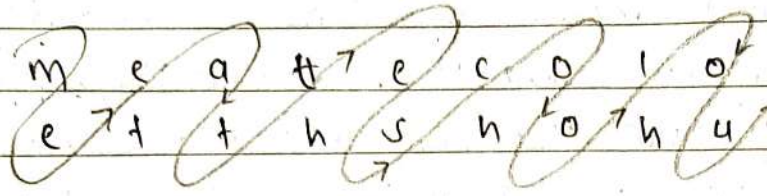
## Transposition Technique

→ A technique different from technique of substitution is achieved by transposing / performing some sort of permutation on the plaintext letters. This technique is called transposition cipher.

Eg: RailFence is the simplest of such cipher in which plaintext is written down as a sequence of diagonal and read the of as sequence of rows.

P.T = 'Meet me at the school house'

To encipher this message using rail fence of depth 2, we write the message as:




The encrypted message is meatecolosetthshohue.

## Row transposition

A more complex scheme is used to write the message in a rectangle row by row and read the message off column by column but permute the order of column. The order of columns become the key of the algorithm.

Eg. P.T : meet at the school house.

Key: 5 4 3 2 1

m e e t a
t t h e s
c h o o l
h o u s e

Encrypted message is asleteosehouethomtch.

NOTE: A pair transposition is easily recognized because it has the same letter frequencies as the original text. The transposition can be made more secured by performing more than one stage of transposition.

# Steganography

→ A plain text maybe hidden in any of the two ways:

a) Cryptography

b) Steganography

Steganography consists of existence of the message whereas cryptography renders the message intelligible to outsiders by various transformation of the text. A simple form of steganography is the one in which the word arrangement is such that the letters within the apparently innocuous (causing no injuries/harmless) text spells out the real message. For eg: (1) A sequence of first letters of each word of overall message spells out the recil message. (2) Subset of words of overall message is used to convey the hidden message.

- Character marking

Selected letters of printed or typewritten text are overwritten with pencil. The marks are not ordinarily visible unless the paper is held at some certain angle to bright light.

- Invisible ink

A number of substances can be used for writing but no leave no visible traces on the paper until heat or some chemical is applied on the paper.

- Pin structure

Small pin structures on selected letters are ordinarily not

visible unless the paper is held against the light.

Drawbacks:

⇒ Requires a lot of overhead to hide relatively few bits of information.

⇒ Once the system is discovered, it becomes virtually worthless.