① Substitution Technique

* Substitution Technique is also called classical Encryption Technique
* In substitution Technique, there are several cipher techniques are there.

① Caesar Cipher
② Monoalphabetic Cipher
③ Play-fair Cipher
④ Hill Cipher
⑤ Poly-alphabetic cipher
⑥ One-time pad

1) Caesar Cipher:

* In this technique we substitute the plain text alphabets by using formula

$$C_i = (P_i + K) \bmod 26$$

Where C_i = Cipher text
P_i = Plain text
K = key

* For decryption we use $P_i = (C_i - K) \bmod 26$

Where P_i = Plain Text
C_i = Cipher text
K = key

* The main drawback of this method is it is used for very short length communication and it is easy to attack.
* We use symmetric key for encryption and also decryption.
* Here the key is numerical which ranges from 1 to 26

* Substitution Table used for encryption and decryption is

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	26
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

* Let us do a example for encryption and decryption

Plain Text = Hello

Key = 4

From substitution table

Plain Text = Hello = 8 5 11 11 15

For encryption $C = (P_i + K) \bmod 26$

H → $(8+4) \bmod 26 = 12 \bmod 26 = 12$

E → $(5+4) \bmod 26 = 9 \bmod 26 = 9$

L → $(12+4) \bmod 26 = 16 \bmod 26 = 16$

O → $(15+4) \bmod 26 = 19 \bmod 26 = 19$

From substitution Table

C = 12 9 16 16 19 = L I P P S

For decryption $P = (C_i - K) \bmod 26$

L → $(12-4) \bmod 26 = 12 \bmod 8$

I → $(9-4) \bmod 26 = 5$

P → $(16-4) \bmod 26 = 12$

S → $(19-4) \bmod 26 = 15$

From substitution table

P = 8 5 12 12 15 = H E L L O

* The main drawback of this technique is we can only use 26 possibilities of letters

2) Mono alphabetic Cipher:

* Caesar cipher is not safe because the key size consist of 26 possibilities only. So as a result brute force attack are common. So in order to enhance security of encryption monoalphabetic ciphers are used.
* In this technique we will create a substitution table with alphabets replacing with random alphabets without ~~repret~~ repetation which decreases the chance of attack as possibilites increases.
* This substitution table will be used for encryption and and sent to receiver for decryption which makes it difficult to attak to get plain text but it is easy to attack by using few frequently repeated letters used.
* let us do a example for better understanding

Substitution Table:

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	26
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	

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

Plain Text: Computer Science

Cipher Text: PUEUNGFZ RPKFWPPF

* Here we are replacing letters with the respective letters in table

3) Play fair Cipher:

* In this technique we will be using a 5x5 matrix
* We will fill the matrix first with key and then we will remaining alphabets inthe matrix.
* If the matrix is filled only 25 alphabets and if the matrix needs 26 alphabets to get filled we will keep I and J in the same block.
* There are 3 rules for filling
  1. Divide a plain text to a pair of letter
  2. Differentiate repeated letters in the place with dummy letters.
  3. If the pair of plain text letter are in a same row then replace them with right most letter similarly if the plain text letters are in a same coloumn then replace them with beneath latter.
* If the plain text letters are in different row and column then replace them with by diagonal position.

Example:

Plain Text: BALLOON

Key: NETWORK

* Divide into pair of letters and add ~~empty~~ dummy letters if there exist any single letter

P.T: BA|LL|OO|NX

* Now make the repeated letters as dummy

BA|LX|OX|NX

* With rule 3 write cipher text from plain text.

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

C.T = CB|PO|ZT|UT

4) Hill Cipher:

* It is a polygraphic substitution cipher based on linear algorithm (or) linear algebra.
* It is the first polygraphic cipher in which it was practical to operand on more than 3 symbols on advance. Here we are using 2x2 matix for key.
* The plain text should be made of pair of two letters.
* Formula to find the cipher text using pair of Plain Text:

$$C.T = KP \bmod 26$$

* Formula to find plaintext using cipher text

$$P.T = K^{-1}C \bmod 26$$

Eg: HELP → plain text

HE|LP $\quad HE = \begin{bmatrix}7\\4\end{bmatrix}$ $\quad Key = \begin{bmatrix}3&3\\2&5\end{bmatrix}$

$$CT = KP \bmod 26$$

$$= \begin{bmatrix}3&3\\2&5\end{bmatrix}\begin{bmatrix}7\\4\end{bmatrix} \bmod 26$$

$$= \begin{bmatrix}33\\34\end{bmatrix} \bmod 26$$

$$= \begin{bmatrix}7\\3\end{bmatrix}$$

$$= \begin{bmatrix}H\\I\end{bmatrix}$$

$LP = \begin{bmatrix} 11 \\ 15 \end{bmatrix}$ Key $= \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$CI = KP \bmod 26$

$= \begin{bmatrix} 3*3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} 11 \\ 15 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 33+45 \\ 22+75 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 78 \\ 97 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 \\ 19 \end{bmatrix}$

$= \begin{bmatrix} A \\ T \end{bmatrix}$

C. Text : HIAT

Decryption:

$K^{-1} = \frac{1}{|K|} adj(K)$ $\quad K = \begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$

$|K| = |15-6| = 9$

$adj(K) = \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$

$K^{-1} = \frac{1}{9} \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$

$= 3 \begin{bmatrix} 5 & -3 \\ -2 & 3 \end{bmatrix}$

$= 3 \begin{bmatrix} 5 & 23 \\ 24 & 3 \end{bmatrix}$

$= \begin{bmatrix} 15 & 69 \\ 72 & 9 \end{bmatrix}$

$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix}$

[∵ 69, 72 are not in range of 25 we change them by doing mod|26| with values not in range]

Plain Text $= K^{-1} C \bmod 26$

$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 105+136 \\ 140+72 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 241 \\ 212 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7 \\ 4 \end{bmatrix} = \begin{bmatrix} H \\ E \end{bmatrix}$

Plain Text $= K^{-1} C \bmod 26$

$= \begin{bmatrix} 15 & 17 \\ 20 & 9 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0+323 \\ 0+171 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 11 \\ 15 \end{bmatrix}$

$= \begin{bmatrix} L \\ P \end{bmatrix}$

Plain Text = HELP

5) Poly Alphabetic Cipher / Vigener Cipher:

* In order to use the vigener cipher method we need the help of vigener table also called vigener tabular. It is the kretp good encryption technique and it is practically implemented in many ways.

Ex: P.T : SHE IS LISTENING

KEY : PASCAL

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

24	25
Y	Z

Plain Text: SHE IS L | ISTENI | NG
18 7 4 8 18 11 | 8 18 19 4 13 8 | 13 6

* We divided Plain text into pairs of 6 letter as key size is 6

K: PASCAL | PASCAL | PA
15 0 18 2 0 11 | 15 0 18 2 0 11 | 15 0

Encryption:

$C_i = P_i + K \bmod 26$

S → 18+15 mod 26 = 32 mod 26 = 7 = H

H → 7+0 mod 26 = 7 mod 26 = 7 = H

E → 4+18 mod 26 = 22 mod 26 = 22 = W

I → 8+2 mod 26 = 10 mod 26 = 10 = K

S → 18+0 mod 26 = 18 mod 26 = 18 = S

L → 11+11 mod 26 = 22 mod 26 = 22 = W

I → 8+15 mod 26 = 23 mod 26 = 23 = X

S → 18+10 mod 26 = 18 mod 26 = 18 = S

T → 19+18 mod 26 = 37 mod 26 = 11 = L

E → 4+2 mod 26 = 6 mod 26 = 6 = G

N → 13+0 mod 26 = 13 mod 26 = 13 = N

I → 8+11 mod 26 = 19 mod 26 = 19 = T

N → 13+15 mod 26 = 28 mod 26 = 2 = C

G → 6+0 mod 26 = 6 mod 26 = 6 = G

C.T → HHWKSW | XSLGNT | CG

Decryption Process.

C.T → HHWKSW | XSLGNT | CG
7 7 22 10 18 22 | 23 18 11 6 13 19 | 2 6

Key → PASCAL | PASCAL | PA
15 0 18 2 0 11 | 15 0 18 2 0 11 | 15 0

$P_i = C_i - K \bmod 26$

H → 7-15 mod 26 = -8 mod 26 = 18 = S

H → 7-0 mod 26 = 7 mod 26 = 7 = H

W → 22-18 mod 26 = 4 mod 26 = 4 = E

K → 10-2 mod 26 = 8 mod 26 = 8 = I

S → 18-0 mod 26 = 18 mod 26 = 18 = S

W → 22-11 mod 26 = 11 mod 26 = 11 = L

X → 23-15 mod 26 = 8 mod 26 = 8 = I

S → 18-0 mod 26 = 18 mod 26 = 18 = S

L → 11-18 mod 26 = -7 mod 26 = 19 = T

G → 6-2 mod 26 = 4 mod 26 = 4 = E

N → 13-0 mod 26 = 13 mod 26 = 13 = N

T → 19-11 mod 26 = 8 mod 26 = 8 = I

C → 2-15 mod 26 = -13 mod 26 = 13 = N

G → 6-0 mod 26 = 6 mod 26 = 6 = G

6) One time Pad: It uses a random key of the same length of message. Hence the key is not repeated centre is generating a new key for every new message while sending to receiver. So, it is called one-time-pad.

P.T: HOW ARE YOU

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U

21	22	23	24	25
V	W	X	Y	Z

Key: NCBTZQARX

P.T: HOWARE YOU

7 14 22 0 17 4 24 14 20

K: N C B T Z Q A R X

13 2 1 19 25 16 0 17 23

Encryption:

$C_i = P_i + K \bmod 26$

H → 7+13 mod 26 = 20 = U

O → 14+2 mod 26 = 16 = Q

W → 22+1 mod 26 = 23 = X

A → 0+19 mod 26 = 19 = T

R → 17+25 mod 26 = 16 = Q

E → 4+16 mod 26 = 20 = U

Y → 24+0 mod 26 = 24 = Y

O → 14+17 mod 26 = 31 mod 5 = F

U → 20+23 mod 26 = 17 = R

C.T = UQXTQUYFR

Decryption: C.T = U Q X T Q U Y F R

20 16 23 19 16 20 24 5 17

K = N C B T Z Q A R X

13 2 1 19 25 16 0 17 23

$P_i = C_i - K \bmod 26$

U → 20-13 mod 26 = 7 = H

Q → 16-2 mod 26 = 14 = O

X → 23-1 mod 26 = 22 = W

T → 19-19 mod 26 = 0 = A

Q → 16-25 mod 26 = 17 = R

U → 20-16 mod 26 = 4 = E

Y → 24-0 mod 26 = 24 = Y

F → 5-17 mod 26 = 14 = O

R → 17-23 mod 26 = 20 = U

② Transposition Technique:

* In this technique there is no replacement and substitution technique.
* In this technique rearranging the order of bits to provide the security. In substitution technique we are replacing the plain text with cipher text character, but there in this transposition technique we are not going to replace any character just arranging the order of bits position to provide the security.
* In this there are mainly 2 techniques
  1. Railfence
  2. Columnar

1) Railfence Transposition Technique

In this technique the plain text can be return in a zig-zag position by drawing one line at the middle of the text and the plain text

P.T = WE ARE DISCOVERED

W	A	E	I	C	V	R	D
A	R	D	S	O	E	E	

CT: WAEICVRDERDSOEE

* For decryption we divide the text into two halfs and write one above the line and another below
* If the no.of letters is odd we add a dummy letter for dividing

Ex: C.T = WAEICVRD|ERDSOEEX

W	A	E	I	C	V	R	D
E	R	D	S	O	E	E	X

P.T= WE ARE DISCOVERED.

2) Columnar Transposition Technique:

* In columnar transposition the message is written out in a rows of fixed length and then read out again column by column and the column choosen in scramled order. Both the width of the rows and permutation of the columns are usually defined by a keyword

Ex:

Key: ZEBRAS

P.T: WE ARE DISCOVERED FILE AT ONCE

Key: ZEBRAS
6 3 2 4 1 5

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	X	Y

Dummy letters

C.T: EVINX ACDTK ESEAQ RDFOJ DELCY
① ② ③ ④ ⑤

WIREE
⑥

Decryption:

Key: ZEBRAS
6 3 2 4 1 5

CT: EVINXACDTKESEAQRDFOJ
DELCY WIREE

P.T: WEARE DISCOVERED
FILE AT ONCE

6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	I	L
E	A	T	O	N	C
E	Q	K	J	Y	X

3) Model For Network Security:

Encryption: Conversion of plain text to cipher text at sender side.

Decryption: Conversion of cipher text to plain text at receiver side.

Cryptography: The study of Encryption

Cryptanalysis: The study of decryption.

Cryptology: The study of both encryption and decryption.

Key: The major role in encryption and decryption process.

Encryption can be done in 2 ways

① Stream Cipher

② Block Cipher

Stream Cipher: The conversion by means of bit by bit. This is valid for short length messages

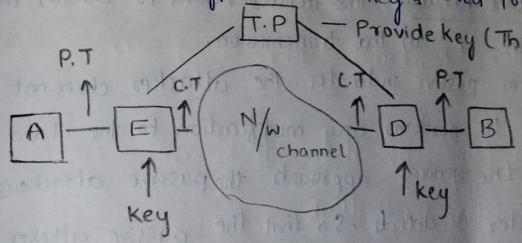
Block Cipher: The conversion may happen block by block. A plain text can be converted into different blocks. Each block should be converted to cipher text till all the blocks are converted to cipher.

Encryption can be done in 2 mechanisms

① Symmetric: Same key is to be used for both encryption and decryption

② Asymmetric: There are 2 independent keys namely public key (PU) and private key (PK). PU is used for encryption and PK is used for decryption.

Every user having this pair of key. If one key is used for encryption, other key is used for decryption.



NETWORK

P.T → Plain Text

A → Sender

E → Encryption

C.T → Cipher text

D → Decryption

B → Receiver

T.P → Third Party who provides key for Sender and receiver for encryption and decryption.

4) Types of Attacks.

* There are two types of attaks in computer and network system.
  ① Theoretical Attacks
  ② Practical Attacks.

1) Theoretical Attacks: The principle of security phase threats from various attacks. These attacks are classified into 2 types

ⓐ Passive Attack: The attacker aims to obtain the information i.e., in the transmission.
The term passive indicates the attacker does not attempt to perform any modification to the data So that the general approach the passive attackers are harder to detect. So that the passive attacker about it prevention rather than detection

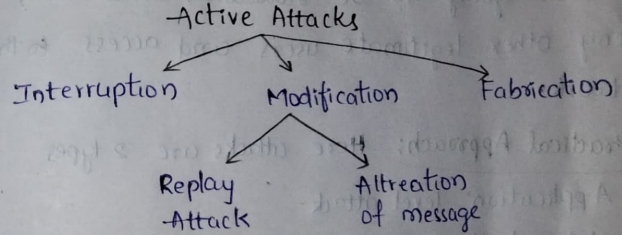
* Passive attacks classified into 2 types

ⓘ Release of Message Content:
In this using certain security mechanism we can prevent release of message content.
Eg: We can encode message using code language so that only destination party only can understand.

ⓘⓘ Traffic Analysis: If any search message are passing through, a passive attacker, could try to figure of similarities between them to come up some sort of patterns that provide some clue regarding it.

ⓑ Active Attacks: Active attacks are based on modification of original message in the some manner or the creation of false message. These attackers cannot be prevented easily. These attacks can be in the form of interruption, modification and fabrication.

In active attack the content of original message is modified in some ways. This modification attack can be classified into further 3 types.



ⓘ Interruption: It is caused when ~~an~~ unauthorised entity pretends to the other entity. As an instance the attack may involve capturing the user authentication sequence (user id & password) later the details can be replayed to gain illegal access to computer system.

ⓘⓘ ~~Alteration of Message~~

ⓘⓘ Modification:
a) Replay Attack: A user capture sequence of events on some data units and resend them.

(ii) Alteration of message: It involves some change to the original message

(iii) Fabrication: It attacks may on attempt to prevent legitimate user from accessing some services which they are eligible for. For instance an authorised user might send to many login request to the server using random user IDs one after another in quick sucession. So, the network going to be slowdown attack and deny other legitimate users and access to the network.

2) Practical Approach: Here attacks are 2 types

(i) Application level attack

(ii) Network level attack

i) Application level attack: These attacks may happen at application level in the sense that the attackers attempts to int access, modify or prevent access to information of the particular applica-tion.

(ii) Network level Attack: These attacks generally aim to reduce the capabilities of a network by numbers of possible means. These attacks generally make an attempt to either slowdown or hault the computer network so it can automatically leads to application level attack if someone is gain access to the network they can easily change the content too.