UNIT-1

Note By: Roshan Bist

Introduction and Classical Ciphers:-

⊛. Security:

It is the protection of computer systems and networks from information disclosure, theft or some damage to hardware, software or electronic data. It is the protection of computer systems and information from harm, theft and unauthorized use. Security is said to be preserved when unauthorized, unauthenticated access and modification to the systems are not allowed.

i) **Computer Security:-** It is 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.

ii) **Information Security:-** It is the protection of information and information systems from unauthorized access, use, modification, or destruction.

iii) **Network Security:-** It is the process of taking physical and software preventive measures to protect the underlying networking insfrastructure. from unauthorized access, misuse, modification etc.

⊛. CIA Traid:-

i) **Confidentiability:-** This term covers two related concepts:

a) **Data Confidentiability** → It assures that private or confidential information is not made available to unauthorized individuals.

b) **Privacy** → It assures that individual control or influence that information related to them may be collected and stored and by whom and to whom that information may be disclose.

ii) **Integrity:-** This term also covers two related concepts:

a) **Data integrity** → It assures that information and programs change only in specified and authorized manner.

b) **System integrity** → It assures that a system performs its intended function in an unpaired manner free from unauthorized manipulation of system.

iii) **Aviability:** It assures that system work promptly and service is not denied to authorized users.

❀. Cryptography:-

The word cryptography comes from two Greek words "Cryptos" and "Graph" meaning "secret writing" and is the art and science of information hiding. It consists of mainly two terms: encryption and decryption. Encryption is the mechanism to convert the readable plaintext into unreadable text (i.e, ciphertext). Decryption is the opposite of encryption i.e, It is the mechanism to convert ciphertext back to plaintext.

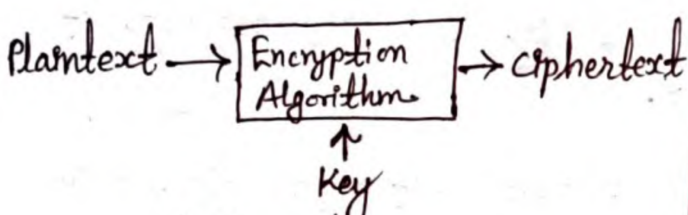

fig: Encryption

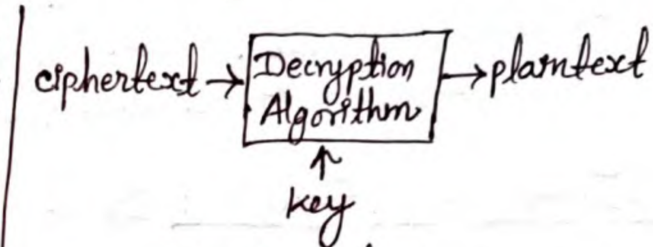

fig: Decryption

❀. Cryptoanalysis:- Cryptoanalysis is the breaking of codes. Cryptoanalysis encompasses all of the techniques to recover plaintext and/or key from the ciphertext. The combined study of cryptography and cryptoanalysis is known as cryptology. Though most of time we use cryptography and cryptology in the same way.

❀. Cryptosystem:- Cryptosystem is a 5-tuple (E, D, M, K, C), where M is the plaintexts, K set of keys, C set of ciphertexts, E set of encryption functions $e: M \times K \rightarrow C$ and D set of decryption functions $d: C \times K \rightarrow M$.

Example:- Caesar Cipher

$M = \{\text{sequence of letters}\}$

$K = \{i \mid i \text{ is an integer and } 0 \leq i \leq 25\}$

$E = \{E_k \mid k \in K \text{ and for all letters } m,\ E_k(m) = (m+k) \bmod 26\}$

$D = \{D_k \mid k \in K \text{ and for all letters } c,\ D_k(c) = (26 + c - k) \bmod 26\}$

$C = M$

Key → A key is a parameter or piece of information used to determine output of cryptographic algorithm.

⊛ Security threat:-

A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

⊛. Security Attacks:-

Security attacks or simply attack is an assault on system security that derives from an intelligent threat to avoid security services and violate the security policy of a system.

Types:

i) Passive Attacks: Passive attacks are in the nature of spy on, or monitoring of, transmissions. The goal of opponent is to obtain information that is being transmitted. There are two types of passive attacks:-

Release of message contents → It is a type of passive attack where contents of message from sender to receiver can be read by the attackers. For example: telephone taping, reading of e-mails, etc.

Traffic Analysis → It is a second type of passive attack. Suppose we encrypted the contents of message or information so that opponents, even if they captured the message, could not extract the information from the message. An opponent might still be able to observe the pattern of these messages. The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.

ii) Active Attacks: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories:

Masquerade → It takes place when one entity pretends to be a different entity.

Replay → It involves the passive capture of a data unit and its subsquent retransmission to produce an unauthorized effect.

Modification of messages → It simply means that some portion of message is altered, or that message are delayed or reordered to produce an unauthorized effect.

Denial of service → It prevents the normal use or management of communication facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

⊛ Security Services:- It is a service that is provided by the protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers. A Security service makes use of one or more security mechanism.

i) Authentication:- The authentication service is concerned with assuring that a communication is authentic. Two specific authentication services are defined in X.800:

Peer Entity Authentication → It is used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication → It is used in association with a connectionless transfer to provide assurance that the source of received data is as claimed.

ii) Access Control:- Access control is the ability to limit and control the access to host systems and applications via communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

iii) Nonrepudiation:- Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus when a message is sent, the receiver can prove that the supposed sender in fact sent the message. Similarly, when a message is received, the sender can prove that the supposed ~~sender~~ receiver in fact received the message.

⊛ Security Mechanisms:-

A security mechanism is a design to detect, prevent or recover from a security attack. Security mechanisms are used to preserve security in every system and make the system consistent. The mechanisms may include cryptography for ensuring confendiality and integrity, authentication systems and digital signature schemes for ensuring integrity and access control lists for authorization.

⊛ Classical Cryptosystems:

Cipher: A cipher is an algorithm for performing encryption and decryption. The operation of cipher depends upon the special information called key.

Types of Ciphers:-

i) **Historical/Classical Ciphers** → These ciphers use processes like substitution and transportation or combination of both called product ciphers. These historic ciphers use the single key for both encryption and decryption.

ii) **Modern Ciphers:-** Modern encryption methods can be divided by two criteria: by type of input data, and by type of key used.

Based upon input data → In this kind of ciphers the plaintext is converted into ciphertext stream by stream. These are called stream ciphers.

Block Ciphers → In this, the plaintext is converted into ciphertext block by block. So, it encrypts of data of fixed size.

Based upon type of key → By type of key used ciphers are divided into symmetric key algorithms and asymmetric key algorithms.

Symmetric key algorithms → These techniques use single key for encryption as well as decryption.

Asymmetric key algorithms → These techniques use two keys, namely private and public keys. One key is used for encryption and the other is used for decryption.

1) Substitution Techniques:-

→ In numericals decryption part can be escaped, only encryption is important according to our syllabus

i) **Monoalphabetic substitution cipher:** In this section we will study Caesar Cipher and Hill Cipher:

[Imp]. **Caesar Cipher:-** It is applicable for english alphabet A-Z. It was defined by Julius Caesar. In this cipher, letters are shifted cyclically over k^{th} place where k is key. Ceasar Cipher is defined over the set {0,1,2,....25} for english alphabet A-Z.

Encryption: $c = E(k,p) = (p+k) \bmod 26.$

Decryption: $p = D(k,c) = (c-k) \bmod 26.$

where, p = plaintext
c = ciphertext.

> we can also denote plaintext by m. It's notation we can't denote by any.

Example:- Given, plaintext = ANT
key = 3
ciphertext = ?

> key को value generally question मा दिएको हुन्छ नदिएको भए given string को length को जतिको जुनसुकै राखेर गर्दा हुन्छ।

Here,
$P_1 = A = 0$
$P_2 = N = 13$
$P_3 = T = 19$

Now, for encryption we have:

$$\boxed{c = (p+k) \bmod 26.}$$

> Less chance but, Exam मा Algorithm सोधे यदि solving process लाई short मा points मा steps बनाएर describe गर्ने (if any confusion refer to book algorith once it's easy)

so,

$$\begin{aligned} C_1 &= (P_1+k) \bmod 26 \\ &= (0+3) \bmod 26 \\ &= 3 \\ &= D \end{aligned}$$

$$\begin{aligned} C_2 &= (P_2+k) \bmod 26 \\ &= (13+3) \bmod 26 \\ &= 16 \\ &= Q \end{aligned}$$

$$\begin{aligned} C_3 &= (P_3+k) \bmod 26 \\ &= (19+3) \bmod 26 \\ &= 22 \\ &= W \end{aligned}$$

Hence, ciphertext = DQW

> Similarly using formula $p = (c-k) \bmod 26$ we can easily convert DQW into ANT which is plaintext and method is decryption.

[Imp] **Hill Cipher:-** It is also applicable for english alphabet A-Z. It is developed by mathematician Lester Hill in 1929. The encryption algorithm takes m successive plaintext letters and substitutes for them m ciphertext letters. It is expressed in the forms:

Encryption: $c = E(k,p) = kp \bmod 26.$

Decryption: $p = D(k,c) = k^{-1}c \bmod 26$

where k is key in the form of matrix & k^{-1} is k inverse.

<u>Example:</u> Let $k=\begin{pmatrix}3 & 6\\1 & 5\end{pmatrix}$ and plaintext = movie. Encrypt using Hill cipher.

<u>Solution</u>:-

The key is 2×2 matrix, so we create 2×1 matrix of plaintext, grouping 2 letters each.

for m×n matrix, m×1 matrix of plaintext.

So, we have plaintext = mo vi ez (here z is used to complete last pair).

<u>Now for mo:</u>

we have, $c = kp \bmod 26$

since, on counting 0,1,2,...
$m=12$
$o=14$

$$=\begin{pmatrix}3 & 6\\1 & 5\end{pmatrix}(12\ \ 14) \bmod 26$$

$$=(36+14\ \ \ 72+70) \bmod 26$$

$$=(50\ \ \ 142) \bmod 26$$

$$=(24\ \ 12)$$

$$= ym$$

Similarly we can encrypt vi and ez also and get complete ciphertext.

<u>Q.</u> Encrypt the plaintext = abll with key = find using Hill cipher.

<u>Solution:</u> Here, $p=\begin{pmatrix}0 & 1\\11 & 11\end{pmatrix}$ & $k=\begin{pmatrix}5 & 8\\17 & 3\end{pmatrix}$

<u>we have</u>, $c = kp \bmod 26$

$$=\begin{pmatrix}5 & 8\\17 & 3\end{pmatrix}\begin{pmatrix}0 & 1\\11 & 11\end{pmatrix} \bmod 26$$

$$=\begin{pmatrix}17 & 3\\242 & 121\end{pmatrix} \bmod 26$$

$$=\begin{pmatrix}17 & 3\\8 & 17\end{pmatrix}$$

$\therefore$ ciphertext = rdir.

less imp. Mainly encrypt is asked always in exam

<u>Note:</u> We can decrypt the ciphertext rdir back to abll as follows:-

we have, $\boxed{p = ck^{-1} \bmod 26}$ for decryption.

We already have value of c but value of k^{-1} is obtained as follows:-

we have $k=\begin{pmatrix}5 & 8\\17 & 3\end{pmatrix}$.

determinant of k (let d) $= (5\times3 - 8\times17) \bmod 26$

$$= -121 \bmod 26$$

$$= 9$$

Now we find multiplicative inverse of 9 as:-

$$d.d^{-1} \equiv 1 \bmod 26$$

or, $9 \times d^{-1} \equiv 1 \bmod 26$.

$26(n)+1 = d\times n$
where $n=1,2,3,\ldots$

d मा 1,2,3,... values राखेर check गर्ने 9× जुन value राख्दा mod 26 गर्दा 1 आउँछ त्यहि multiplicative inverse हो।

Here, 3 is that value because $9 \times 3 = 27 \bmod 26 = 1$.

Therefore we compute inverse of A now as;

$$A^{-1} \bmod 26 = 3\begin{pmatrix} 3 & -8 \\ -17 & 5 \end{pmatrix} \bmod 26$$

adj of k. i.e, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ = $\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

k

adj. of k.

Value of d^{-1} we recently found

$$= 3\begin{pmatrix} 3 & 18 \\ 9 & 5 \end{pmatrix} \bmod 26$$

Since while encryption or decryption we need +ve values so, we convert -ve values into +ve values by adding 26 to -ve values before computing or decrypting.

$-8 + 26 = 18$

$-17 + 26 = 9$

$$= \begin{pmatrix} 9 & 54 \\ 27 & 15 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$$

i.e, $k^{-1} = \begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix}$

Hence, $p = ck^{-1} \bmod 26$

$$= \begin{pmatrix} 17 & 3 \\ 8 & 17 \end{pmatrix}\begin{pmatrix} 9 & 2 \\ 1 & 15 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 156 & 79 \\ 89 & 271 \end{pmatrix} \bmod 26$$

$$= \begin{pmatrix} 0 & 1 \\ 11 & 11 \end{pmatrix}$$

∴ plaintext = abll.

ii) **Polyalphabetic substitution cipher:-** In this section we will study vignere cipher and Playfair cipher.

Vigenere Cipher: Vigenere cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution. A polyalphabetic cipher is any cipher based on substitution, using multiple substitution alphabets. The encryption of the original text is done using the vigenere table. The table consists of the alphabets written out 26 times in different rows, corresponding to the 26 possible caesar ciphers.

Example:-

plaintext = ZONAL

key = PEN , new key = PENPE

starting PE added to end of PEN to make its length equal to plaintext

```
plain text = 25  14  13  0  11
       key = 15   4  13 15   4
           ----------------------
             14  18   0 15  15
```

add with mod 26

always use new key

∴ cipher text = OSAPP

Vingre Table:

→ Key →

plaintext ↓

	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
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Q. Use vignere table to encrypt orignal message ZONAL with key PEN.

Solution :-

Plain text = Z O N A L

key = PEN

new key = PENPE

Since plain text is of length 5 so we should also make key as length of 5 by repeating ~~text~~ letters from beginning until it becomes of length 5, then we use table.

Hence, analysing table we have

cipher text = OSAPP

In the table plain text Z and new key P met at O. Similarly next letter of plain text O and new key letter E meet at S, and similarly we encrypted the whole message.

⊛. Vigenere Cipher has two variants: vernam and one time pad :

1) Vernam Cipher: This system works on binary data (bits) rather than letters. This system can be expressed as follows:-

[Imp] for short note

$$C_i = P_i \oplus k_i$$

where; P_i = ith binary digit of plain text.
k_i = ith binary digit of key.
C_i = ith binary digit of ciphertext.
$\oplus$ = exclusive-or (XOR) operation.

Because of the properties of the XOR, decryption simply involves the same bitwise operation:

$$P_i = C_i \oplus k_i$$

ii) One Time Pad: It is an improvement of vernam cipher. It uses a random key that is as long as the message, so that the key need not be repeated. In addition, the key is to be used to encrypt and decrypt a single message, and then is discarded. Each new message requires a new key of the same length as the new message. Such a scheme, is known as a one-time pad which is unbreakable.

[Imp] Playfair:- It is multi letter encryption cipher. It was introduced by L. playfair in 1854. It is based on the use of 5X5 matrix of letters constructed using keyword. The Playfair cipher is relatively fast and does not require special equipment. British Forces used it for tactical purposes during World War I. It is same as the traditional cipher, the only difference is that it encrypts a diagraph (a pair of two letters) instead of single letter.

Example:
keyword=hieronymus

first we fill keyword rowwise then we complete table writing a,b,c,d,... but omitting/not repeating letters that are already in keyword.

h	i/j	e	r	o
n	y	m	u	s
a	b	c	d	f
g	k	l	p	q
t	v	w	x	z

Playfair initially creates a table of 5X5 matrix. The matrix contains alphabets that act as key for encryption of plaintext. Note that any alphabet should not be repeated and there are 26 alphabets and we have 25 blocks to put letter inside it. Therefore, letters i and j are treated as same letter.

Playfair Cipher Encryption Rules:-

1). First split the plaintext into diagraphs (pair of two letters). If the plaintext has odd number of letters, append the letter at the end of plaintext.

Example1:
plaintext = attack
digraph = at ta ck

Example2:
plaintext = mango
digraph = ma ng oz

2). If any letter appears twice (side by side) in the diagraph then, put x at the place of the second occurance.

Example1:
plaintext = GREET
diagraph = GR EX ET

Example 2:
plaintext = JAZZ
diagraph = JA ZZ
= JA ZX ZX

Z appears twice so 2nd one replaced by X.

This is 2nd Z ~~at~~ shifted right which was replaced by X

Since it is becoming odd so to complete we added Z at end but it is repeating twice so 2nd Z is replaced by X

3). Build a 5*5 key-matrix with the letters of given keyword. Let's create a 5*5 key-matrix for the keyword ATHENS.

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

Now following three conditions may appear:-

If not understood refer to any of youtube video it's easy

i) If a pair of letters (of diagraph) appears in the same row then, replace each letter of diagraph with the letters immediatly to their right. If there is no letter to right consider the first letter of same row as the right letter.

ii) If a pair of letters (of diagraph) appears in the same column then, replace each letter of the diagraph with the letters immediatly to letter below them. If there is no letter below, consider the first letter of same column as the below letter.

iii) If a pair of letters (of diagraph) appears in a different row and different column then, we mark the rectangle that includes diagraph pairs and replace the diagraph each letter with a letter that is at the opposite corner of rectangle.

Q. Suppose a keyword as monarchy. Encrypt a message circular using Playfair cipher.

Solution: keyword = monarchy
plaintext = circular
diagraph = ci rc ul ar.

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

Now,
ci converts as be
rc converts as md
ul converts as mu
ar converts as rm

Hence, ciphertext = bemdmurm

Since c & i appears in different row and different column so on constructing rectangle around it opposite words are b and e respectively

u & l are in same column so letters just below them are replaced

in same row so letters just right to them replaces

2) Transposition Techniques:

[Imp] **Rail Fence Cipher:-** In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails", then moving up when we reach the bottom rail. When we reach the top rail, the message is written downwards again until the whole plaintext is written out. The message is then read off in rows.

Example:- Encrypt a message "meet me after the toga party" with a rail fence depth 3.

Solution:-

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

Since rail fence depth 3 so we constructed 3 rows

∴ ciphertext = mmthgretetefeteoaateartpy

row-wise written

⊛. Symmetric vs. Asymmetric Ciphers/Cryptography:-

	Secret Key (Symmetric)	Public key (Asymmetric)
Number of keys	1	2
Protection of key	Must be kept secret.	One key must be kept secret; other can be freely exposed.
Best uses	Cryptographic workhorse; security and data integrity - single characters to block of data, messages, files.	Key exchange, authentication.
Key distribution	Must be out-of-band.	Public key can be used to distribute other keys.
Speed	Fast	Slow; typically, 10,000 times slower than secret key.

Substitution cipher technique → The technique used to encrypt plaintext into cipher text in which identity of character is changed but not the position is called substitution cipher technique. Monoalphabetic cipher and Polyalphabetic cipher are it's types.

Transportation cipher technique → The technique used to encrypt plaintext into cipher text in which each character position is changed to different position is called transportation cipher technique. Rail Fence Cipher is it's example.

Monoalphabetic cipher → It is an encryption technique that involves Single character during encryption. Examples: Ceasar Cipher, Hill Cipher.

Polyalphabetic cipher → It is an encryption technique that involves two or more than two characters during encryption.
Examples:- Vigenere Cipher, Playfair Cipher.