UNIT-2

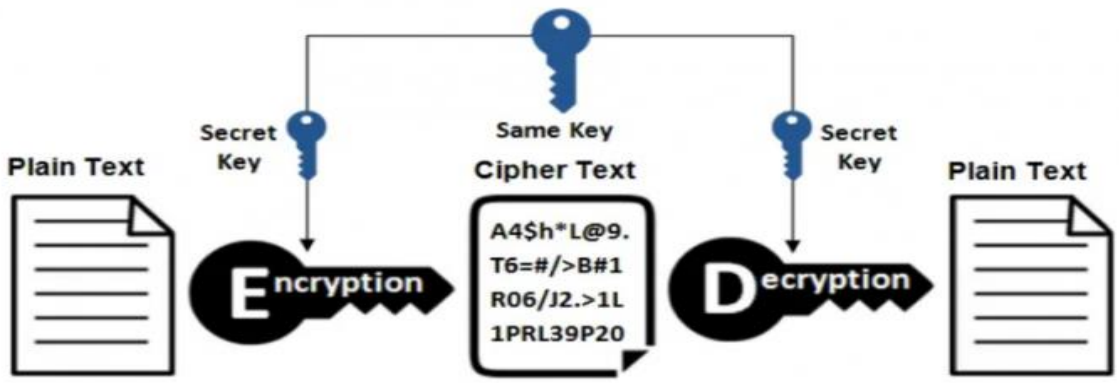
CRYPTOGRAPHY IN NETWORK SECURITY

2.1 INTRODUCTION TO SYMMETRIC ENCRYPTION & ASYMMETRIC ENCRYPTION

2.1.1 Symmetric Encryption

Symmetric Encryption is a type of encryption where only one key (a secret key) is used to both encrypt and decrypt electronic data. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process.

By using symmetric encryption algorithms, data is "scrambled" so that it can't be understood by anyone who does not possess the secret key to decrypt it. Once the intended recipient who possesses the key has the message, the algorithm reverses its action so that the message is returned to its original readable form. The secret key that the sender and recipient both uses could be a specific password/code or it can be random string of letters or numbers that have been generated by a secure random number generator (RNG).



There are two types of Symmetric Encryption Algorithms:

1) **Block Algorithms:** Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.
2) **Stream Algorithms:** Data is encrypted as it streams instead of being retained in the system's memory.

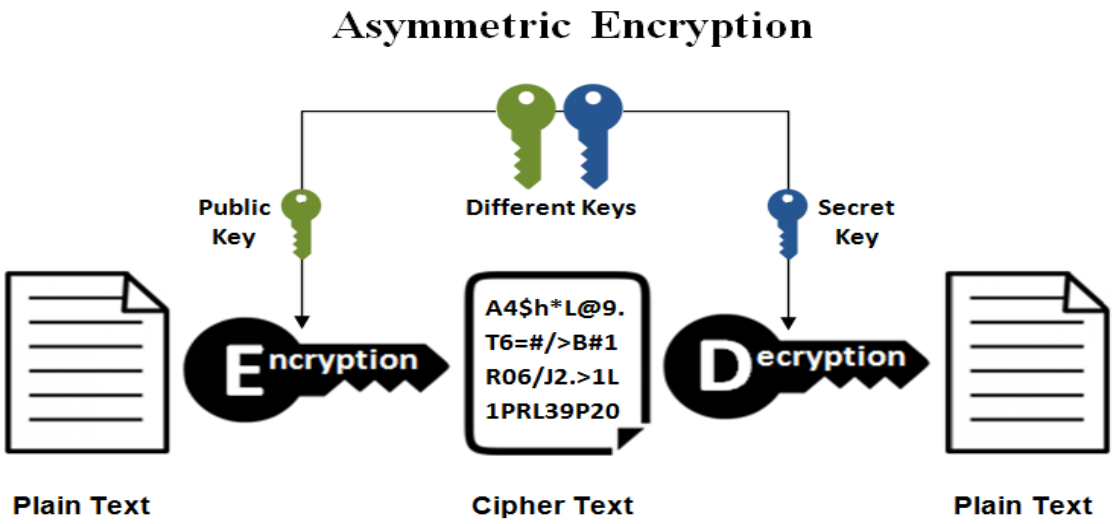
Some examples of symmetric encryption algorithms include:

1) AES (Advanced Encryption Standard)
2) DES (Data Encryption Standard)
3) IDEA (International Data Encryption Algorithm)
4) Blowfish (Drop-in replacement for DES or IDEA)
5) RC4 (Rivest Cipher 4)
6) RC5 (Rivest Cipher 5)
7) RC6 (Rivest Cipher 6)

AES, DES, IDEA, Blowfish, RC5 and RC6 are block ciphers. RC4 is stream cipher.

2.1.2 Asymmetric Encryption

Asymmetric encryption, also known as public-key cryptography, is a type of encryption that uses a pair of keys to encrypt and decrypt data. The pair of keys includes a public key, which can be shared with anyone, and a private key, which is kept secret by the owner. In asymmetric encryption, the sender uses the recipient's public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows secure communication between two parties without the need for both parties to have the same secret key. Asymmetric encryption is commonly used in various applications like secure online communication including email encryption, e-commerce and online banking, digital and secure data transfer. Examples of asymmetric encryption algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC). Digital Signature which is used to confirm the legitimacy of digital documents and messages is another application of it.



Advantages:

1) **Enhanced Security:** Asymmetric encryption provides a higher level of security compared to symmetric encryption where only one key is used for both encryption and decryption with asymmetric encryption a different key is used for each process and the private key used for decryption is kept secret by the receiver making, it harder for an attacker to intercept and decrypt the data.
2) **Authentication:** Asymmetric encryption can be used for authentication purposes which means that the receiver can verify the sender's identity.
3) **Non-repudiation:** Asymmetric encryption also provides non-repudiation which means that the sender cannot deny sending a message or altering its contents this is because the message is encrypted with the sender's private key and only their public key can decrypt it. Therefore, the receiver can be sure that the message was sent by the sender and has not been tampered with.
4) **Key Distribution:** Asymmetric encryption eliminates the need for a secure key distribution system that is required in symmetric encryption with symmetric encryption, the same key is used for both encryption and decryption and the key needs to be securely shared between the sender and the receiver asymmetric

encryption, on the other hand, allows the public key to be shared openly and the private key is kept secret by the receiver.

5) **Versatility:** Asymmetric encryption can be used for a wide range of applications including secure email communication online banking transactions and e-commerce it is also used to secure SSL/TSL connections which are commonly used to secure internet traffic.

2.1.3 Difference between Symmetric Encryption and Asymmetric Encryption

On the basis of	Symmetric Encryption	Asymmetric Encryption
Keys used	It uses a single shared key (secret key) to encrypt and decrypt the message.	It uses two different keys for encryption and decryption.
Size	The size of ciphertext in symmetric encryption could be the same or smaller than the plain text.	The size of ciphertext in asymmetric encryption could be the same or larger than the plain text.
Efficiency	It is efficient as this technique is recommended for large amounts of text.	It is inefficient as this technique is used only for short messages.
Speed	The encryption process of symmetric encryption is faster as it uses a single key for encryption and decryption.	The encryption process in asymmetric encryption is slower as it uses two different keys; both keys are related to each other through the complicated mathematical process.
Purpose	Symmetric encryption is mainly used to transmit bulk data.	It is mainly used in smaller transactions. It is used for establishing a secure connection channel before transferring the actual data.
Security	It is less secured as there is a use of a single key for encryption.	It is safer as there are two keys used for encryption and decryption.
Algorithms	The algorithms used in symmetric encryption are 3DES, AES, DES, and RC4.	RSA, DSA, Diffie-Hellman, ECC, Gamal, and EI.
Existence	It is an old technique.	It is a new technique.

2.2 SUBSTITUTION TECHNIQUES FOR ENCRYPTION AND DECRYPTION

2.2.1 Introduction

The two basic building blocks of all encryption techniques are substitution and transposition. A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. In simple terms, the plaintext characters are substituted and additional substitute letters, numerals and symbols are implemented in their place. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns. A character's identity is changed, but its place remains constant in the substitution technique. There are various methods for substitution techniques such as Caesar Cipher, Shift Cipher, Monoalphabetic Cipher, Playfair Cipher, Polyalphabetic Cipher (Vigenere Cipher), One Time Pad (Vernam Cipher), Hill Cipher.

2.2.2 Caesar Cipher Substitution Technique

It is the earliest known use of a substitution cipher and the simplest method. It was invented by Julius Caesar. The Caesar Cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. The encryption can be represented using modular arithmetic by first transforming the letters into numbers.

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

The formula of Encryption is:

CT = E (K, PT) = (PT + K) mod 26

The formula of Decryption is:

PT = D (K, CT) = (CT - K) mod 26

In any case during decryption if value becomes negative (-ve), then in that case, 26 will be added to that particular negative value and then decryption will be carried out.

EXAMPLE:

Plain Text: SECURITY, Key: 3

ENCRYPTION:

Plain Text	**Encryption** **CT = (PT+3) Mod 26**	**Cipher Text**
S (18)	(18 + 3) mod 26 = 21 mod 26 = 21	V
E (04)	(04 + 3) mod 26 = 07 mod 26 = 07	H
C (02)	(02 + 3) mod 26 = 05 mod 26 = 05	F

U (20)	(20 + 3) mod 26 = 23 mod 26 = 23	X
R (17)	(17 + 3) mod 26 = 20 mod 26 = 20	U
I (08)	(08 + 3) mod 26 = 11 mod 26 = 11	L
T (19)	(19 + 3) mod 26 = 22 mod 26 = 22	W
Y (24)	(24 + 3) mod 26 = 27 mod 26 = 01	B

Cipher Text: VHFXULWB

DECRYPTION:

Cipher Text	**Decryption** **PT = (CT-3) Mod 26**	**Plain Text**
V (21)	(21 - 3) mod 26 = 18 mod 26 = 18	S
H (07)	(07 - 3) mod 26 = 04 mod 26 = 04	E
F (05)	(05 - 3) mod 26 = 02 mod 26 = 02	C
X (23)	(23 - 3) mod 26 = 20 mod 26 = 20	U
U (20)	(20 - 3) mod 26 = 17 mod 26 = 17	R
L (11)	(11 - 3) mod 26 = 08 mod 26 = 08	I
W (22)	(22 - 3) mod 26 = 19 mod 26 = 19	T
B (01)	(01 - 3) mod 26 = 24 mod 26 = 24	Y

Plain Text: SECURITY

***Calculation for (1-3) mod26:**

Here 1 – 3 = -2. Modulo division of negative number is not possible. So firstly, we will add 26 to the negative number i.e. -2+26 = 24. After that modulo division is carried out i.e. 24 mod 26 =24.

Features:

1) **Substitution Cipher:** The Caesar cipher is a type of substitution cipher, where each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
2) **Fixed Key:** The Caesar cipher uses a fixed key, which is the number of positions by which the letters are shifted. This key is known to both the sender and the receiver.
3) **Symmetric Encryption:** The Caesar cipher is a symmetric encryption technique, meaning that the same key is used for both encryption and decryption.
4) **Easy to Implement:** The Caesar cipher is very easy to implement and requires only simple arithmetic operations, making it a popular choice for simple encryption tasks.

Advantages:

1) Easy to implement and use thus, making suitable for beginners to learn about encryption.
2) This method is the simplest method of cryptography.
3) Only one short key is used in its entire process.
4) If a system does not use complex coding techniques, it is the best method for it.
5) It requires only a few computing resources.

Disadvantages:

1) It is not secure against modern decryption methods.
2) Vulnerable to known-plaintext attacks, where an attacker has access to both the encrypted and unencrypted versions of the same messages.
3) It is not suitable for long text encryption as it would be easy to crack.
4) It is not suitable for secure communication as it is easily broken.
5) Does not provide confidentiality, integrity, and authenticity in a message.

2.2.3 Playfair Technique

The best-known multiple-letter encryption cipher is the Playfair. The Playfair algorithm is based on the use of a 5 x 5 matrix of letters constructed using a keyword. The matrix is constructed by filling in the letters of the keyword (minus duplicates) from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

1) Firstly, breakdown plain text in the pair of 2. For example, **playfair** would be **pl ay fa ir**.
2) While making pair from plain text, if last letter is single than add filler letter such as x. For example, **technique** would be **te ch ni qu ex**.
3) Repeating plain text letters that are in the same pair are separated with a filler letter such as x. For example, **balloon** would be treated as **ba lx lo on**.
4) If repeating plain text letters that are in the different pair then there is no need to separate it with any other filler letter.
5) Two plain text letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row circularly following the last.
6) Two plain text letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last.
7) Otherwise, each plain text letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other plain text letter.
8) For decryption, if two cipher text letters that fall in the same row of the matrix are each replaced by the letter to the left, with the last element of the row circularly following the first.

9) For decryption, if two ciphertext letters that fall in the same column are each replaced by the letter above, with the bottom element of the column circularly following the first.

10) Otherwise, each cipher text letter in a pair is replaced by the letter that lies in its own row and the column occupied by the other cipher text letter.

EXAMPLE:

1) Plain Text: COMPUTER, Key: NETWORK

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

Solution (for encryption):

- First, break plain text into pair of 2. i.e. CO MP UT ER
- Here CO is in same column. So, replace it with below letter in that column. So, CO will be IC.
- Here MP is in same row. So, replace it with next letter in that row. So, MP will be PQ.
- Here UT is neither in same row nor in same column. Then as per rule 7, UT will be replaced by XN.
- Here ER is neither in same row nor in same column. Then as per rule 7, ER will be replaced by NK.
- Therefore, cipher text will be **ICPQXNNK.**

Solution (for decryption):

- First, break cipher text into pair of 2. i.e. IC PQ XN NK.
- Here IC is in same column. So, replace it with above letter in that column. So, IC will be CO.
- Here PQ is in same row. So, replace it with previous letter in that row. So, PQ will be MP.
- Here XN is neither in same row nor in same column. Then as per rule 10, XN will be replaced by UT.
- Here NK is neither in same row nor in same column. Then as per rule 10, NK will be replaced by ER.

2) Plain Text: INSTRUMENTS

Key: MONARCHY

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

Solution (for encryption):

- First, break plain text into pair of 2. i.e. IN ST RU ME NT S
- Here, last letter is single. So as per rule no. 2, add filler letter X.
- Therefore, it would be now IN ST RU ME NT SX.
- Here IN is neither in same row nor in same column. Then as per rule 7, IN will be replaced by GA.
- Here ST is in same row. So, replace it with next letter in that row. So, ST will be TL. (Here, T is the last letter in that particular row. So, it is replaced with the very first letter of that particular row).
- Here RU is neither in same row nor in same column. Then as per rule 7, RU will be replaced by MZ.
- Here ME is in same column. So, replace it with below letter in that column. So, ME will be CL.
- Here NT is neither in same row nor in same column. Then as per rule 7, NT will be replaced by RQ.
- Here SX is in same column. So, replace it with below letter in that column. So, SX will be XA. (Here, X is the last letter in that particular column. So, it is replaced with the very first letter of that particular column).
- Therefore, cipher text will be **GATLMZCLRQXA.**

Solution (for decryption):

- First, break cipher text into pair of 2. i.e. GA TL MZ CL RQ XA.
- Here GA is neither in same row nor in same column. Then as per rule 10, GA will be replaced by IN.
- Here TL is in same row. So, replace it with next letter in that row. So, TL will be ST. (Here, L is the first letter in that particular row. So, it is replaced with the very last letter of that particular row).
- Here MZ is neither in same row nor in same column. Then as per rule 10, MZ will be replaced by RU.
- Here CL is in same column. So, replace it with below letter in that column. So, CL will be ME.
- Here RQ is neither in same row nor in same column. Then as per rule 10, RQ will be replaced by NT.
- Here XA is in same column. So, replace it with below letter in that column. So, XA will be SX. (Here, A is the first letter in that particular column. So, it is replaced with the very last letter of that particular column).
- Therefore, plain text will be **INSTRUMENTSX**.

2.2.4 Shift Cipher Technique

Shift Cipher Technique is one of the earliest and simplest known substitution techniques. It is similar to Caesar Cipher Technique. The only difference is that in Caesar cipher, key value is fixed i.e. 3 whereas in shift cipher, key value ranges from 0 to 25. A given plain text is encrypted into cipher text by shifting each letter of the plain text by n positions.

The encryption/decryption can be represented using modular arithmetic by first transforming the letters into numbers.

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

The formula of Encryption is:

CT = E (K, PT) = (PT + K) mod 26

The formula of Decryption is:

PT = D (K, CT) = (CT - K) mod 26

In any case during decryption if value becomes negative (-ve), then in that case, 26 will be added to that particular negative value and then decryption will be carried out.

EXAMPLE:

1)Plain Text: HELLO

Key: 6

ENCRYPTION:

Plain Text	**Encryption** **CT = (PT+3) Mod 26**	**Cipher Text**
H (07)	(07 + 06) mod 26 = 13 mod 26 = 13	N
E (04)	(04 + 06) mod 26 = 10 mod 26 = 10	K
L (11)	(11 + 06) mod 26 = 17 mod 26 = 17	R
L (11)	(11 + 06) mod 26 = 17 mod 26 = 17	R
O (14)	(14 + 06) mod 26 = 20 mod 26 = 20	U

Cipher Text: NKRRU

DECRYPTION:

Cipher Text	**Decryption** **PT = (CT-3) Mod 26**	**Plain Text**
N (13)	(13 - 06) mod 26 = 07 mod 26 = 07	H
K (10)	(10 - 06) mod 26 = 04 mod 26 = 04	E
R (17)	(17 - 06) mod 26 = 11 mod 26 = 11	L
R (17)	(17 - 06) mod 26 = 11 mod 26 = 11	L
U (20)	(20 - 06) mod 26 = 14 mod 26 = 14	O

Plain Text: HELLO

2) Plain Text: LAYOUT

Key: 15

ENCRYPTION:

Plain Text	Encryption CT = (PT+3) Mod 26	Cipher Text
L (11)	(11 + 15) mod 26 = 26 mod 26 = 00	A
A (0)	(00 + 15) mod 26 = 15 mod 26 = 15	P
Y (24)	(24 + 15) mod 26 = 39 mod 26 = 13	N
O (14)	(14 + 15) mod 26 = 29 mod 26 = 03	C
U (20)	(20 + 15) mod 26 = 35 mod 26 = 09	J
T (19)	(19 + 15) mod 26 = 34 mod 26 = 08	I

Cipher Text: APNCJI

DECRYPTION:

Cipher Text	Decryption PT = (CT-3) Mod 26	Plain Text
A (0)	(00 - 15) mod 26 = 18 mod 26 = 11	L
P (15)	(15 - 15) mod 26 = 04 mod 26 = 00	A
N (13)	(13 - 15) mod 26 = 02 mod 26 = 24	Y
C (03)	(03 - 15) mod 26 = 20 mod 26 = 14	O
J (09)	(09 - 15) mod 26 = 17 mod 26 = 20	U
I (08)	(08 - 15) mod 26 = 08 mod 26 = 19	T

Plain Text: LAYOUT

***Calculation for (0-15) mod26:**

Here 0 – 15 = -15. Modulo division of negative number is not possible. So firstly, we will add 26 to the negative number i.e. -15+26 = 11. After that modulo division is carried out i.e. 11 mod 26 =11.

*** Same rule is applicable whenever we get negative value while subtracting key value from cipher text during decryption.**

.

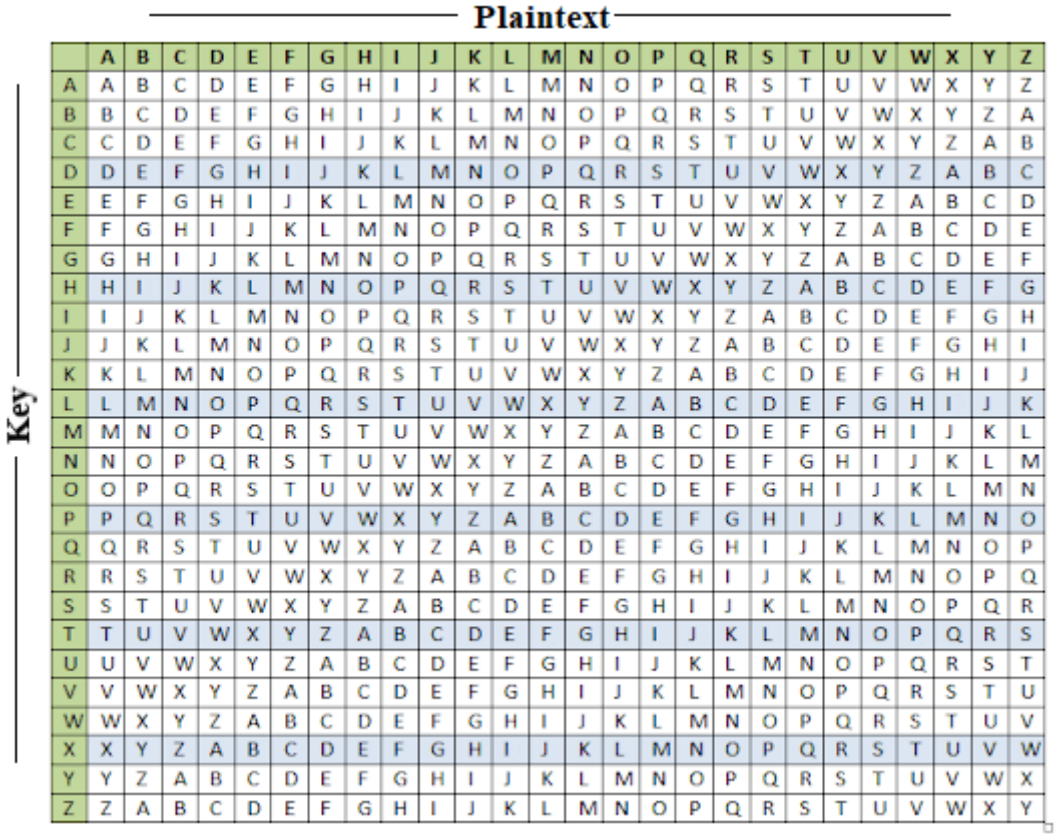
2.2.5 Vigenere Cipher Technique

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. This algorithm was first described in 1553 by Giovan Battista Bellaso. It uses a Vigenere table or Vigenere square

for encryption and decryption of the text. The Vigenere table is also called the tabula recta. There are two methods perform the Vigenere cipher.

Method 1:

When the Vigenere table is given, the encryption and decryption are done using the Vigenere table (26 * 26 matrix) in this method.



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

For generating key, the given keyword is repeated in a circular manner until it matches the length of the plain text.

EXAMPLE: The plaintext is **"JAVATPOINT"**, and the key is **"BEST".**

J	A	V	A	T	P	O	I	N	T
B	E	S	T	B	E	S	T	B	E

ENCRYPTION:

The first letter of the plaintext is combined with the first letter of the key. The column of plain text "J" and row of key "B" intersects the alphabet of "K" in the Vigenere table, so the first letter of ciphertext is "K".

Similarly, the second letter of the plaintext is combined with the second letter of the key. The column of plain text "A" and row of key "E" intersects the alphabet of "E" in the Vigenere table, so the second letter of ciphertext is "E".

This process continues continuously until the plaintext is finished.

Ciphertext = KENTUTGBOX

DECRYPTION:

Decryption is done by the row of keys in the Vigenere table. First, select the row of the key letter, find the ciphertext letter's position in that row, and then select the column label of the corresponding ciphertext as the plaintext.

K	E	N	T	U	T	G	B	O	X
B	E	S	T	B	E	S	T	B	E

For example, in the row of the key is "B" and the ciphertext is "K" and this ciphertext letter appears in the column "J", that means the first plaintext letter is "J".

Next, in the row of the key is "E" and the ciphertext is "E" and this ciphertext letter appears in the column "A", that means the second plaintext letter is "A".

This process continues continuously until the ciphertext is finished.

Plaintext = JAVATPOINT

Method 2:

When the Vigenere table is not given, the encryption and decryption are done by Vigenar algebraically formula in this method (convert the letters (A-Z) into the numbers (0-25)).

The formula of Encryption is:

Ei = (Pi + Ki) mod 26

The formula of Decryption is:

Di = (Ei - Ki) mod 26

***If any case (Di) value becomes negative (-ve), in this case, we will add 26 in the negative value.**

Where,

E denotes the encryption, D denotes the decryption, P denotes the plaintext, K denotes the key.

Note: "i" denotes the offset of the ith number of the letters, as shown in the table below.

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

EXAMPLE:

Plaintext: JAVATPOINT

Key: BEST

ENCRYPTION:

Ei = (Pi + Ki) mod 26

Plaintext	J	A	V	A	T	P	O	I	N	T
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Key	B	E	S	T	B	E	S	T	B	E
Key value (K)	01	04	18	19	01	04	18	19	01	04
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Ciphertext	K	E	N	T	U	T	G	B	O	X

Cipher Text: KENTUTGBOX

DECRYPTION:

Di = (Ei - Ki) mod 26

If any case (Di) value becomes negative (-ve), in this case, we will add 26 in the negative value.

Like, the third letter of the ciphertext;

N = 13 and S = 18

Di = (Ei - Ki) mod 26

Di = (13 - 18) mod 26

Di = -5 mod 26

Di = (-5 + 26) mod 26 = 21 mod 26 = 21

Ciphertext	K	E	N	T	U	T	G	B	O	X
Ciphertext value (E)	10	04	13	19	20	19	06	01	14	23
Key	B	E	S	T	B	E	S	T	B	E
Key value (K)	01	04	18	19	01	04	18	19	01	04
Plaintext value (P)	09	00	21	00	19	15	14	08	13	19
Plaintext	J	A	V	A	T	P	O	I	N	T

Plain Text: JAVATPOINT

2.2.6 One Time Pad (Vernam Cipher) Technique

One Time Pad algorithm is the improvement of the Vernam Cipher, proposed by An Army Signal Corp officer, Joseph Mauborgne. It is the only available algorithm that is unbreakable (completely secure). It is a method

of encrypting alphabetic plain text. It is one of the substitution techniques which converts plain text into ciphertext. In this mechanism, we assign a number to each character of the Plain-Text. Vernam Cipher is a method of encrypting alphabetic text. It is one of the Substitution techniques for converting plain text into cipher text. In this mechanism we assign a number to each character of the Plain-Text, like (a = 0, b = 1, c = 2, … z = 25).

Method to take key/ OTP:

In the Vernam cipher algorithm, we take a key to encrypt the plain text whose length should be equal to the length of the plain text.

ENCRYPTION:

Treat each plaintext character as a number in an increasing sequence from a = 0, b= 1 … z = 25. Do the same for each character of the input cipher text/ OTP. Add each number corresponding to the plain text character to the corresponding input cipher text character number. If the produced cipher text is greater than 25; then subtract 26 from it. Convert each number of the cipher text into corresponding alphabet character.

Plain Text	C (02)	O (14)	M (12)	P (15)	U (20)	T (19)	E (04)	R (17)
Key/ OTP	S (18)	E (04)	C (02)	U (20)	R (17)	I (08)	T (19)	Y (24)
PT + Key	20	18	14	35 35-26=09	37 37-26=11	27 27-26=01	23	41 41-26=15
Cipher Text	U (20)	S (18)	O (14)	J (09)	L (11)	B (01)	X (23)	P (15)

Cipher Text: USOJLBXP

DECRYPTION:

Treat each cipher text character as a number in an increasing sequence from a = 0, b= 1 … z = 25. Do the same for each character of the input cipher text/ OTP. Subtract each number corresponding to the cipher text character to the corresponding OTP character number. If the produced cipher text is a negative number; then add 26 to it. Convert each number of the plain text into corresponding alphabet character.

Cipher Text	U (20)	S (18)	O (14)	J (09)	L (11)	B (01)	X (23)	P (15)
Key/ OTP	S (18)	E (04)	C (02)	U (20)	R (17)	I (08)	T (19)	Y (24)

CT - Key	02	14	12	-11 -11+26 = 15	-06 -06+26 = 20	-07 -07+26 =19	04	-09 -09+26 =17
Plain Text	C	O	M	P	U	T	E	R

2.2.7 Hill Cipher Technique

The Hill Cipher was invented by Lester S. Hill in 1929, and like the other digraphic ciphers, it acts on groups of letters. Unlike the others though it is extendable to work on different sized blocks of letters. So, technically it is a polygraphic substitution cipher, as it can work on digraphs, trigraphs (3 letter blocks) or theoretically any sized blocks.

The Hill Cipher uses an area of mathematics called linear algebra and in particular requires the user to have an elementary understanding of matrices. It also makes use of modulo arithmetic. Because of this, the cipher has a significantly more mathematical nature than some of the others. However, it is this nature that allows it to act (relatively) easily on larger blocks of letters.

ENCRYPTION:

To encrypt the text using hill cipher, we need to perform the following operation.

E (K, P) = (K * P) mod 26

Where K is the key matrix and P is plain text in vector form. Matrix multiplication of K and P generates the encrypted ciphertext.

Step 1: Convert key using a substitution scheme into a 2x2 key matrix

Step 2: Now, we will convert our plain text into vector form. Since the key matrix is 2x2, the vector must be 2x1 for matrix multiplication. (Suppose the key matrix is 3x3, a vector will be a 3x1 matrix.)

Step 3: Multiply the key matrix with each 2x1 plain text vector, and take the modulo of result (2x1 vectors) by 26.

DECRYPTION:

To encrypt the text using hill cipher, we need to perform the following operation.

D (K, C) = (K^{-1} * C) mod 26

Where K is the key matrix and C is the ciphertext in vector form. Matrix multiplication of inverse of key matrix K and ciphertext C generates the decrypted plain text.

Step 1: Calculate the inverse of the key matrix. First, we need to find the determinant of the key matrix (must be between 0-25). Here the Extended Euclidean algorithm is used to get modulo multiplicative inverse of key matrix determinant

Step 2: Now, we multiply the 2x1 blocks of ciphertext and the inverse of the key matrix. The resultant block after concatenation is the plain text that we have encrypted.

EXAMPLE:

1) Plain Text: HI

Key: BEAT

Solution (Encryption):

Convert key into 2*2 matrix and then convert it into numeric form (A = 0, B = 1 ……. Z = 25)

$K = \begin{bmatrix} B & E \\ A & T \end{bmatrix} = \begin{bmatrix} 1 & 4 \\ 0 & 19 \end{bmatrix}$

Convert plain text into 2*1 matrix and then convert it into numeric form.

$P = \begin{bmatrix} H \\ I \end{bmatrix} = \begin{bmatrix} 7 \\ 8 \end{bmatrix}$

E = KP mod 26

$= \begin{bmatrix} 1 & 4 \\ 0 & 19 \end{bmatrix} \begin{bmatrix} 7 \\ 8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 1*7+4*8 \\ 0*7+19*8 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 7+32 \\ 0+152 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 39 \\ 152 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 13 \\ 22 \end{bmatrix}$

$= \begin{bmatrix} N \\ W \end{bmatrix}$

Cipher Text = NW

2) Plain Text: CIPHER

Key: HILL

Solution:

Convert key into 2*2 matrix and then convert it into numeric form (A = 0, B = 1 ……. Z = 25)

$K = \begin{bmatrix} H & I \\ L & L \end{bmatrix} = \begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix}$

Here, plain text of 2*1 is only possible. So, break given plain text into 3 parts of 2*1 matrix and then convert it into numeric form.

$P1 = \begin{bmatrix} C \\ I \end{bmatrix} = \begin{bmatrix} 2 \\ 8 \end{bmatrix}$

$P2 = \begin{bmatrix} P \\ H \end{bmatrix} = \begin{bmatrix} 15 \\ 7 \end{bmatrix}$

P3 = $\begin{bmatrix} E \\ R \end{bmatrix} = \begin{bmatrix} 4 \\ 17 \end{bmatrix}$

E = E1 + E2 + E3

= K P1 mod 26 + K P2 mod 26 + K P3 mod 26

= $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 2 \\ 8 \end{bmatrix}$ mod 26 + $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 15 \\ 7 \end{bmatrix}$ mod 26 + $\begin{bmatrix} 7 & 8 \\ 11 & 11 \end{bmatrix} \begin{bmatrix} 4 \\ 17 \end{bmatrix}$ mod 26

= $\begin{bmatrix} 78 \\ 110 \end{bmatrix}$ mod 26 + $\begin{bmatrix} 161 \\ 242 \end{bmatrix}$ mod 26 + $\begin{bmatrix} 192 \\ 231 \end{bmatrix}$ mod 26

= $\begin{bmatrix} 0 \\ 6 \end{bmatrix} + \begin{bmatrix} 5 \\ 8 \end{bmatrix} + \begin{bmatrix} 10 \\ 23 \end{bmatrix}$

= $\begin{bmatrix} A \\ G \end{bmatrix} + \begin{bmatrix} F \\ I \end{bmatrix} + \begin{bmatrix} K \\ X \end{bmatrix}$

Cipher Text = AGFIKX

2.3 TRANSPOSITION TECHNIQUE: RAIL FENCE CIPHER

2.3.1 Introduction

Transposition Technique rearranges the position of the plain text's characters. In transposition technique, the position of the character is changed but character's identity is not changed. Transposition is a type of encryption technique where the positions of the letters in the plaintext message are rearranged to form a ciphertext message. This technique does not alter the letters themselves but rather the order in which they appear.

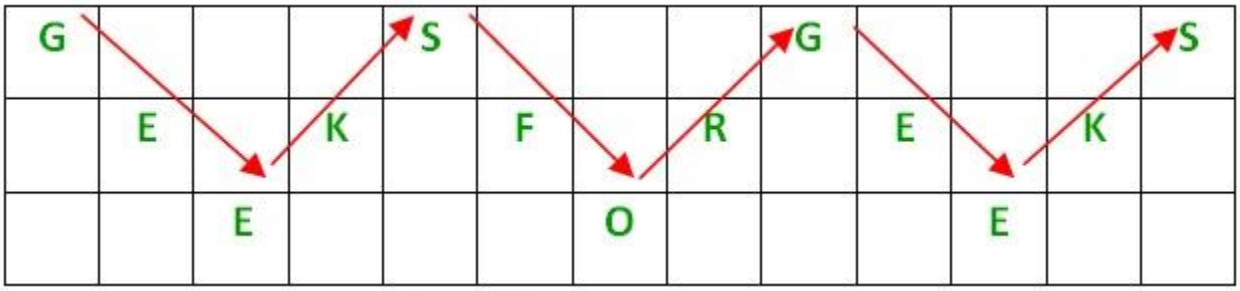
2.3.2 Rail Fence Cipher Technique

The rail fence cipher (also called a zigzag cipher) is a form of transposition cipher. It derives its name from the way in which it is encoded.

ENCRYPTION:

In the rail fence cipher, the plain-text is written downwards and diagonally on successive rails of an imaginary fence. When we reach the bottom rail, we traverse upwards moving diagonally, after reaching the top rail, the direction is changed again. Thus, the alphabets of the message are written in a zig-zag manner. After each alphabet has been written, the individual rows are combined to obtain the cipher-text.

For example, if the message is "GeeksforGeeks" and the number of rails = 3 then cipher is prepared as:



Its encryption will be done row wise i.e. **GSGSEKFREKEOE**

DECRYPTION:

Let cipher-text = "GSGSEKFREK EOE", and Key = 3

Number of columns in matrix = length (cipher-text) = 13

Number of rows = key = 3

Hence original matrix will be of 3*13, now marking places with text as '*' or any other symbol (-) we get

The decryption process for the Rail Fence Cipher involves reconstructing the diagonal grid used to encrypt the message. We start writing the message, but leaving a dash in place of the spaces yet to be occupied. Gradually, you can replace all the dashes with the corresponding letters, and read off the plaintext from the table.

We start by making a grid with as many rows as the key is, and as many columns as the length of the ciphertext. We then place the first letter in the top left square, and dashes diagonally downwards where the letters will be. When we get back to the top row, we place the next letter in the ciphertext. Continue like this across the row, and start the next row when you reach the end

Here the ciphertext received is " GSGSEKFREK EOE ", encrypted with a key of 3, you start by placing the "G" in the first square. You then dash the diagonal down spaces until you get back to the top row, and place the "S" here.

-				-				-				-
	-		-		-		-		-		-	
		-				-				-		

G				**S**				**G**				**S**
	-		-		-		-		-		-	
		-				-				-		

Continuing to fill the rows you get the pattern below

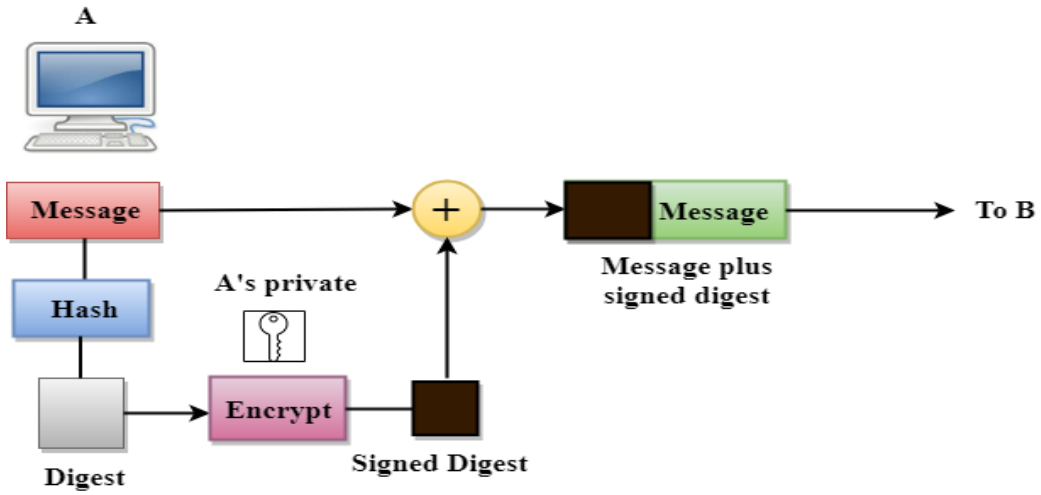
G				**S**				**G**				**S**
	E		**K**		**F**		**R**		**E**		**K**	
		-				**-**				**-**		

G				**S**				**G**				**S**
	E		**K**		**F**		**R**		**E**		**K**	
		E				**O**				**E**		

2.4 ASYMMETRIC ENCRYPTION: DIGITAL SIGNATURE

A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature is formed by taking the hash of the message and encrypting message with creator's private key. The signature guarantees the source and integrity of the message.

Digital signatures rely on asymmetric cryptography, also known as public key cryptography. An asymmetric key consists of a public/private key pair. The private key is used to create a signature, and the corresponding public key is used to verify the signature.



By the use of a public key algorithm, such as RSA, one can generate two keys that are mathematically linked- one is a private key, and another is a public key.

The user who is creating the digital signature uses their own private key to encrypt the signature-related document. There is only one way to decrypt that document is with the use of signer's public key.

This technology requires all the parties to trust that the individual who creates the signature has been able to keep their private key secret. If someone has accessed the signer's private key, there is a possibility that they could create fraudulent signatures in the name of the private key holder.

The **steps** which are followed in creating a digital signature are:

1) Select a file to be digitally signed.

2) The hash value of the message or file content is calculated. This message or file content is encrypted by using a private key of a sender to form the digital signature.

3) Now, the original message or file content along with the digital signature is transmitted.

4) The receiver decrypts the digital signature by using a public key of a sender.

5) The receiver now has the message or file content and can compute it.

6) Comparing these computed message or file content with the original computed message. The comparison needs to be the same for ensuring integrity.

Applications of Digital Signature:

The important reason to implement digital signature to communication is:

1) Authentication

2) Non-repudiation

3) Integrity

Authentication:

Authentication is a process which verifies the identity of a user who wants to access the system. In the digital signature, authentication helps to authenticate the sources of messages.

Non-repudiation:

Non-repudiation means assurance of something that cannot be denied. It ensures that someone to a contract or communication cannot later deny the authenticity of their signature on a document or in a file or the sending of a message that they originated.

Integrity:

Integrity ensures that the message is real, accurate and safeguards from unauthorized user modification during the transmission.