Date 16/07
Page

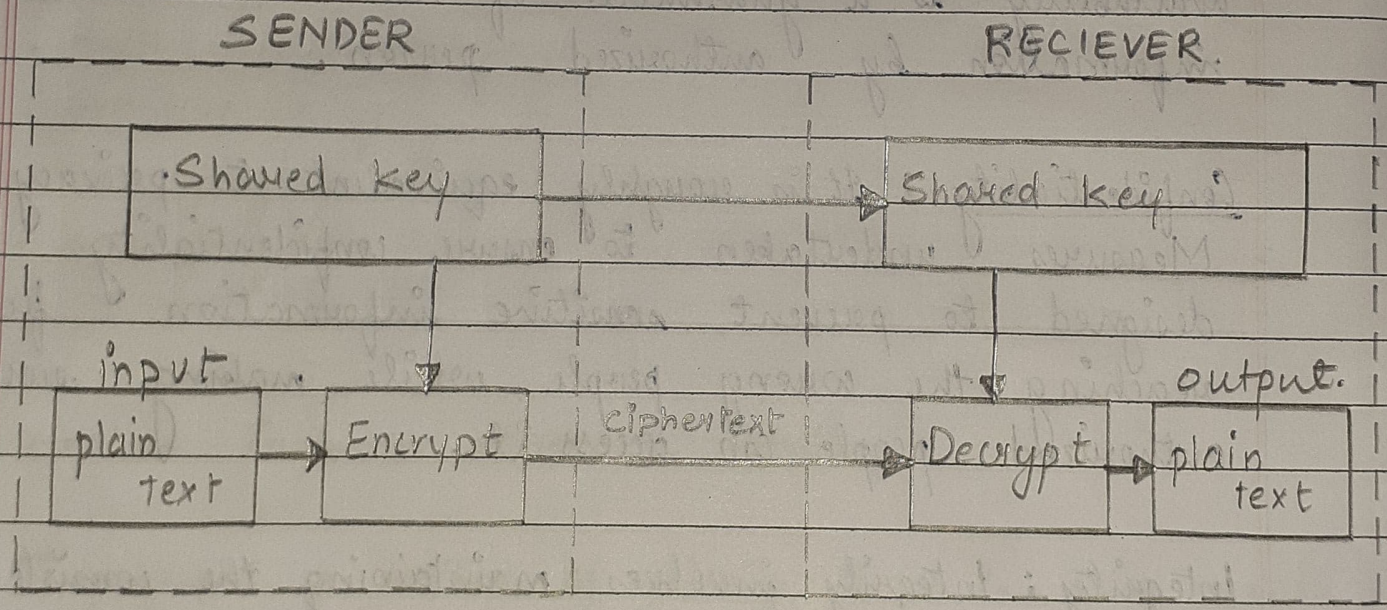
UNIT: 3 CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE.

ASSIGNMENT: 2

Q1. Explain symmetric key and asymmetric key encryption with neat sketch.

Ans. The encryption process where same keys are used for encryption and decryption of the information is known as symmetric key encryption.

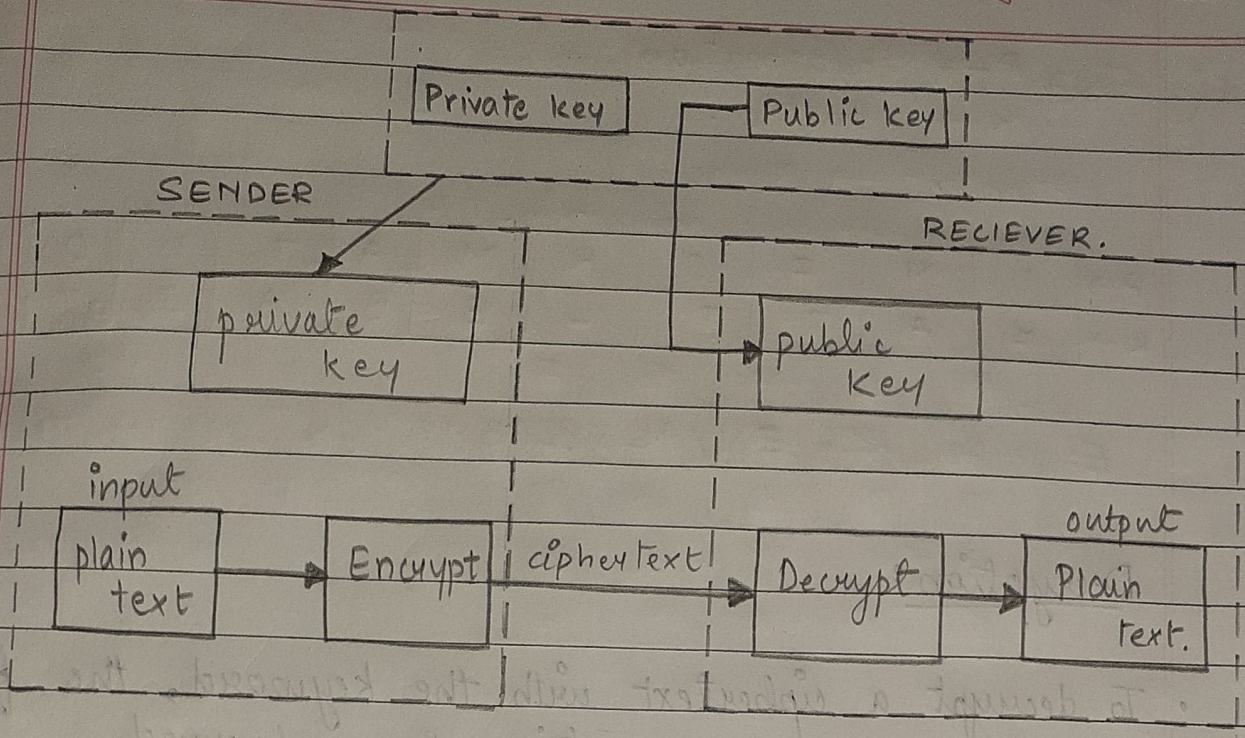
It is also known as conventional or secret key cryptosystem.



Asymmetric key encryption :-

The encryption process where different keys are used for encryption and decryption of the information is known as Asymmetric key encryption.

Though the keys are different, they are mathematically related.



Q2. Explain Vigenere Cipher with ~~Explain~~ Example.

Ans Vigenere Cipher is a method of encrypting alphabetic text. It uses a simple form of polyalphabetic substitution.

The encryption of the original text is done using the Vigenere square or vigenere table.

Method of encryption

- To encrypt a message using the Vigenere Cipher, we first need to choose a keyword.
- Then this keyword is repeated over and over until it is the same length as the plaintext.
- Now for each plaintext letter, find the letter down the left hand side of the vigenere table.
- Now take the corresponding letter from the keystream and find this accross the top of the table.
- Where these two lines cross in the table is the ciphertext letter you use.

P → Information
K → Battle.

P→	I	N	F	O	R	M	A	T	I	O	N
K→	B	A	T	T	L	E	B	A	T	T	L

ENCRYPTION → JNYHCQBTBHY

Decryption:

- To decrypt a ciphertext with the keyword, the ~~first~~ steps same as encryption are performed.

E→ JNYHCQBTBHY.
K→ BATTLE.

J	N	Y	H	C	Q	B	T	B	H	Y
B	A	T	T	L	E	B	A	T	T	L

DECRYPTION → INFORMATION.

Q3. Explain Playfair Cipher with its rules and solve the cipher given below:
(i) Text → Name
key → Playfair encryption.

(ii) Text → Cryptography.
key → Security.

Ans Playfair Cipher was the first practical substitution cipher.

Encryption Algorithm:

1. Generating the key Square:-

- The key square is a 5×5 grid of alphabets that acts as the key for encryption of the plaintext.
- Each of the 25 alphabets must be unique and one letter, usually J and I are considered together in one block.

2. Algorithm to encrypt the plain text:-

- The plaintext is split into pairs of two letters.
- If there is an odd number of letters, a X or Z is added.

* RULES FOR ENCRYPTION

- If both the letters are in the same column: Take the letter below each one.

- If both the letters are in the same rows: Take the letter to the right of each one.

- If neither of the above rules is true: Form a rectangle with two letters and take the letters on the horizontal opposite corner of the rectangle.

Ex: (i)

Plaintext → Name
Key → Playfair encryption.

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

NA ME
EY WB

ENCRYPTED TEXT → EYWB

Ex: (ii)

Plaintext → Cryptography
Key → Security.

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

CR YP TO GR AP HY
US BN AM KC BO GA

ENCRYPTED TEXT :→ USBNAMKCBOGA.

Q4. Explain Hill Cipher with Algorithm / steps. solve the cipher below:

(i) Plaintext → DR GREER ROCKS.

key → $\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$

Ans Hill cipher was invented by Lester S. Hill in 1929. It uses an area of mathematics called linear algebra.

The matrix used for encryption is the cipher key, and should be chosen randomly from the set of invertible n×n matrices.

Encryption:

$$\begin{bmatrix} C1 \\ C2 \end{bmatrix} = \begin{bmatrix} K11 & K12 \\ K21 & K22 \end{bmatrix} \times \begin{bmatrix} x1 \\ x2 \end{bmatrix} \pmod{26}$$

For Decryption the given key must be inversed.

Decryption:

$$\begin{bmatrix} x1 \\ x2 \end{bmatrix} = \begin{bmatrix} K11 & K12 \\ K21 & K22 \end{bmatrix} \times \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} \pmod{26}$$

Ex: (1) P → D R G R E E R R O C K S.
3 17 6 17 4 4 17 17 0 2 10 18

K → $\begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix}$

⇒ $C1 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 3 \\ 17 \end{bmatrix} \pmod{26} = 2 \rightarrow \boxed{C}$

$= 23 \rightarrow \boxed{X}$

3 + 51 → 54 → 2

6 + 17 → 23 → 23

$$C_2 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 6 \\ 17 \end{bmatrix} \pmod{26} = 5 \rightarrow F$$
$$= 3 \rightarrow D$$

$$C_3 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 4 \\ 4 \end{bmatrix} \pmod{26} = 16 \rightarrow Q$$
$$= 12 \rightarrow M$$

$$C_4 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 17 \\ 17 \end{bmatrix} \pmod{26} = 16 \rightarrow Q$$
$$= 25 \rightarrow Z$$

$$C_5 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 14 \\ 2 \end{bmatrix} \pmod{26} = 20 \rightarrow U$$
$$= 4 \rightarrow E$$

$$C_6 = \begin{bmatrix} 1 & 3 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 10 \\ 18 \end{bmatrix} \pmod{26} = 12 \rightarrow M$$
$$= 12 \rightarrow M$$

ENCRYPTED TEXT $\rightarrow$ CXFDQMQZUEMM