"Unit - 01"

DATE: __/__/____
PAGE: _____

The OSI (Open System Interconnection) Security Architecture can be divided into 3 parts:
⇒ Security Attack
⇒ Security Mechanism
⇒ Security Service.

* Security Attack: The action that compromises the security of an individual or an organization is called security attack.
It is divided into two types:
1) Passive attack: The unauthorized reading of messages with no modification of passe messages is involved is called passive attack. The characteristics of passive attack can be:
* There are attempts to learn or make use of information from the system
* It does not affect system resources.
* Eavesdropping or monitoring of transmissio

It has a goal to obtain information that is being transmitted.
There are 2 types of passive attack:
i) Release of message contents: To prevent the release of message contentes, that encrypted data should be send and only the receiver can decrypt it.
ii) Traffic Analysis: Here, the hacker might know some information about the communication like; (i) location (ii) identity (iii) length of the message transmitted (iv) frequency of message. The hacker might guess the message/communication based on traffic and observing the pattern of the message.

Good Write

DATE: __/__/____
PAGE: _____

ii) Active attack: Here, some modification of the data stream or the creation of a false stream is involved.

It is divided into 4 categories ⇒

1. Masquerade: Here, one entity pretends to be a different entity. If we take someone else email, password and login, we are masquerader.
2. Replay: The messages are subsiquently re-transmission. The attacker will capture messages from sender to receiver, and later replay the message to receiver again and again to provoke them.
3. Modification of messages: Here, messages are modified. The attacker captures the message and modifies it and send to the receiver.
4. Denial of service (DoS): Here, we are going to get denied from getting the service. The attacker puts load on the server, so performance gets degraded and are not able to do works.

Security Mechanism: There are 2 types of security mechanism. They are:

i) Specific security mechanism: It has appropiate protocol layer.

1. Encipherment: The technique to convert the normal plain text into cipher before

before sending it to the internet. It is also data unfidentiality.

2. Digital Signature: A piece of code will be inserted to the message, which is known as digital signature. It is used to prove the identity of the source.

3. Access control: The access right for the resources to some user is called access access control.

4. Authentication exchange: Exchanging small piece of information periodically to prove their authentication.

5. Data Integrity: Ensuring the message was not modified during transmission.

6. Traffic padding: When there is no communication occurring, we must put a dummy data on the data stream to confuse attackers which will not have any impact on the receiver.

7. Routing control: When sender sends data item to the network, it also specifies the route it should take in order to reach the destination so that this data packet will not go in the hands of the attacker.

Good Write

8. Notarization: It defines to deploying a trusted 3rd party.

ii) Pervasive: It is not going to be incorporated in any particular layer.

1. Trusted Functionality: Perserved to be correct with respect to some criteria. It is a part of security policies.

2. Security label: We are going have some labels in order to archieve security.

3. Event detection: When any activity is carried by out in a system events are generated. These events can be normal event or suspicious event.

4. Security audit trial: When any activity is carried out in a system. We need to collect data, all these data is used for doing security audit. We are going to review the security records, for ensuring the activity is accepted, suspicious or attacks

5. Recovery: We also need to focus on the data recovery after any attackers.

Security Services: The processing on communication service that is provided by a system to give a specific kind of protection to system resources. Security services implement security policies and are implemented by security mechanism.

(i) Authentication ⇒ assurance that the communication entity is the one that claims to be.
→ Peer entity authentication
→ Data origin.

(ii) Access control ⇒ Controlling the access.
(iii) Data confidentiality ⇒ Data is prevented from unauthorized access.

(iv) Data integrity ⇒ Whatever the sender is sending that only the receiver should receive.

(v) Non-repudiation ⇒ After receiving or sending the denial of messages should be handled. It means it gives protection against the denial of messages of one of the entities in communication.

CRYPTOGRAPHY

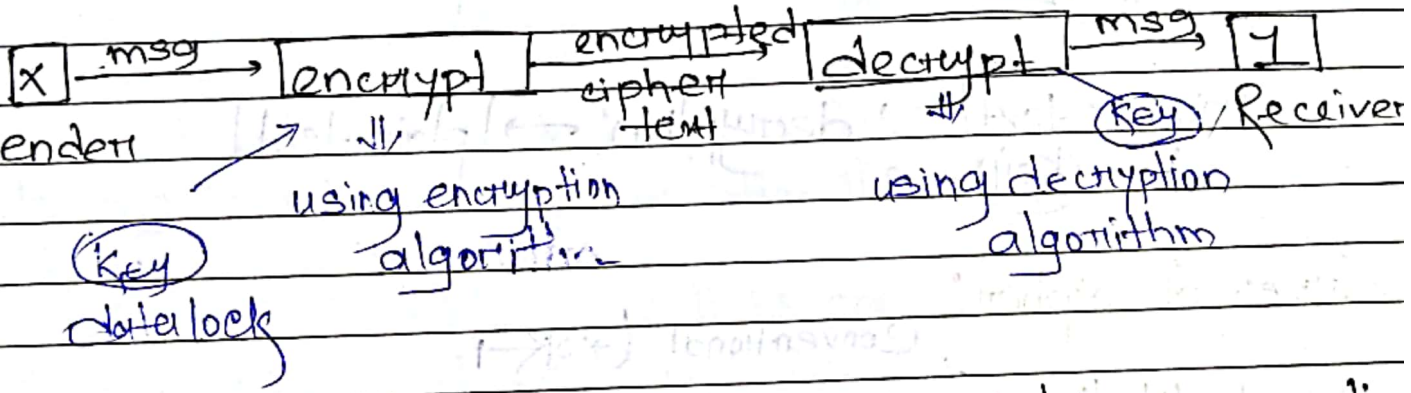
DATE: __/__/____
PAGE: _____

Cryptography: The art of protecting information by transforming it into an unreadable format is called cryptography.

or,

the method of protecting information and communication through the use of codes so that only those for whom the information is intended to read and process it.

To provide security and protect the valuable information, we use cryptography.



case (i) ⇒ if keys are same → symmetric encryption
case (ii) ⇒ if keys are different → assymmetric encryption

Encryption: The process of transforming from readable format to unreadable format. It is done by various encryption algorithm.

Decryption: The process of transforming data from unreadable to readable format.

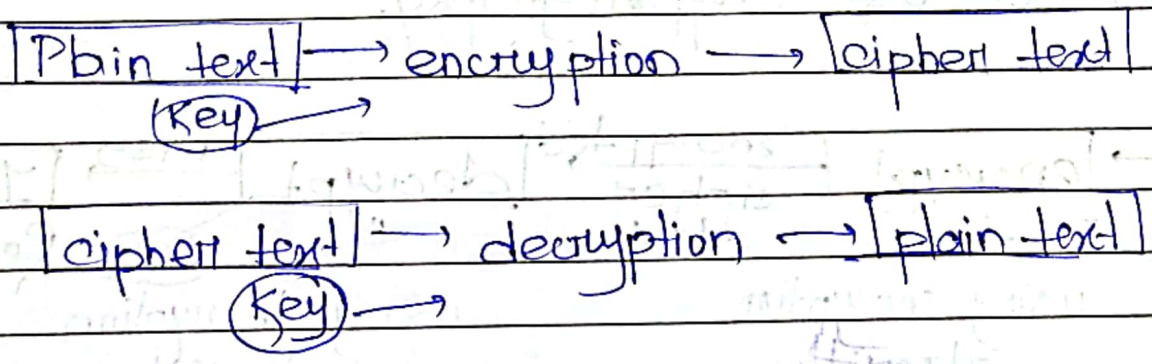
Key: String of bits used by cryptographic algorithm to transform plain text to cipher text or vice-versa

Good Write

It is used for secure communication.

Conventional Encryption: It requires the translation of plain text message into cipher text messages that can only be decrypted by the intendent recipient.

A hidden key to be used in encrypting and decrypting is agreed upon by both sender and recipient. The hidden key is usually conveyed by methods of public key encryption.



Types of cipher:

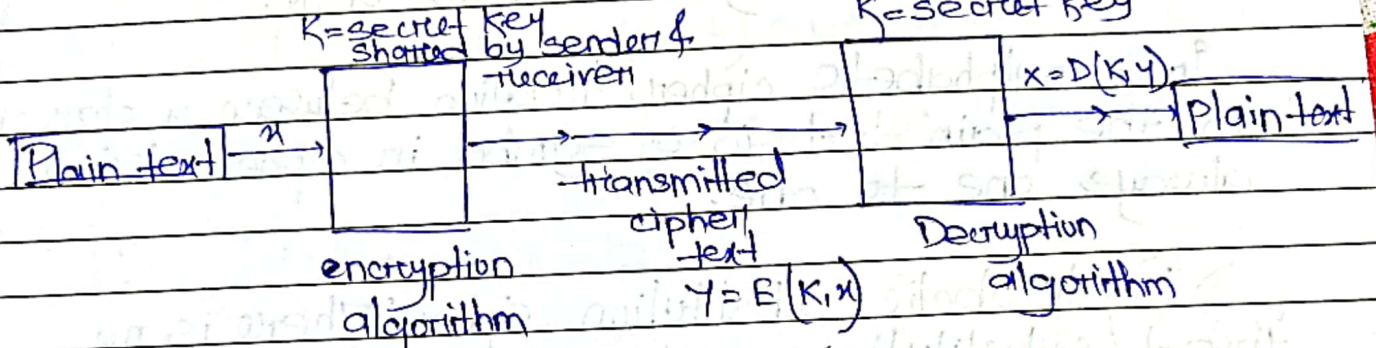
Conventional (XOR)

(i) Substitutional cipher ⇒ substituting with random symb
(ii) Transposition cipher ⇒ permutation / rearranging lett in text.
(iii) Stream transition ⇒ encrypt data in digital forma XOR function size of 1 byte symmetric key of data encryption.
(iv) Block translation ⇒ dividing our data into blocks
(v) Steganography

DATE: __/__/____
PAGE: _____

A symmetric encryption scheme have five ingredients:

i) Plain text
ii) Encryption algorithm.
iii) Secret key
iv) Cipher text
v) Decryption Algorithm.



Classical encryption techniques: Symmetrical encryption also reffered to as conventional encryption is of 2 types:

i) Substitution: It is one in which the letters of the plain text are replaced by other letters or by numbers or symbols.

ii) Transposition: Performing some sort of permutation on the plain text letters/rearrangement of the letters of the plain text.

- Transposition
  - Rail fence
  - Columnar transposition
  - Double transposition

- Transposition cipher
  - Keyless
  - Key

Good Write

Substitution techniques:

i) Monoalphabetic substitution cipher: A single cipher alphabet for each plain text alphabet is used throughout the process.

exp: fixed substitution
if "N" → using x then always use x only in the place of N.

In monalphabetic cipher, relation between a character in the plain text to a symbol in cipher text is always one to one.

ii) Polyalphabetic substitution cipher: There is no fixed substitutions each occurrance of a character may have a different substitute; which is we can use more than 1 substitution for the same letter.

The relationship between a character in the plain text to a character in the cipher text is one to many.

exp: a → d and later "a" may be replaced with m.

iii) Caesar cipher: It is also called shift ciphers/ additive cipher. Each letter in the plain text is replaced by a letter corresponding to a number of shifts in the alphabet.

Formula for encryption:

cipher text, $C = E(K, P) = (P + K) \bmod 26$

for decryption:

plain text, $P = D(K, C) = (C - K) \bmod 26$

④ If (c-k) is -ve then add 26 to it.

DATE: __/__/____
PAGE: _____

Numericals:

1) Message = "Hello" $1 \le k \le 25$.

Let, Key = 4.

$C(H) = (P+K) \bmod 26 = (7+4) \bmod 26 = 11 = L$

$C(E) = (P+K) \bmod 26 = (4+4) \bmod 26 = 8 = I$

$C(L) = (P+K) \bmod 26 = (11+4) \bmod 26 = 15 = P$

$C(L) = (11+4) \bmod 26 = 15$ P.

$C(O) = (P+K) \bmod 26 = (14+4) \bmod 26 = 18 = S$.

C = LIPPS.

For decryption,

$P(C-K) \bmod 26$

$P(L) = (11-4) \bmod 26 = 7 = H$

$P(I) = (8-4) \bmod 26 = 4 = E$

$P(P) = (15-4) \bmod 26 = 11 = L$

$P(P) = (15-4) \bmod 26 = 11 = L$

$P(S) = (18-4) \bmod 26 = 14 = O$.

∴ Plain text, P = Hello.

DATE: __/__/____
PAGE: _____

iv) Playfair Cipher:

Algorithm:

i) Create 5x5 matrix that is called grid of letters.
ii) The matrix is made by inserting the values of key and remaining alphabets into the matrix. (row wise from left to right) where, letter I and J will be combined together.
iii) Convert the text into pairs of alphabet
eg. = Heya → He ya.
Pair cannot be made with same letters. Break the letters into single and add "x" to the previous letter.
eg. Hello → He lx lo

let Hellow → He lx lo wo
↳ alone problem.

If the letter is standing alone in the process of pairing, then add "z" with the letter.

iv) Code will be found using 3 rules:
⇒ If both the alphabets are in the same row, replace them with alphabets to their immediate right.
⇒ If both the alphabets are in the same column, replace them with alphabets immediately below them.
⇒ If not in same row/columns replace them with alphabets in the same row respectively but at other pair of corner.

KEY → ABHJ

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

Plain text

B M → E R
R W → W B.

Same row

F G → G K
U Q → Q R

Horizontal

Q W → R V

K L → D P
K S → F U.

Hill cipher ⇒ It is polyalphabetic cipher.
encrypts a group of letters called
Polygraph = (diagraph, trigraph).

This method makes use of mathematic

To encrypt,

$C = K P \bmod 26.$

step 01: choose a key (key matrix must be a square matrix).

We can take,

$$VIEW = \begin{bmatrix} V & I \\ E & W \end{bmatrix} = \begin{bmatrix} 21 & 8 \\ 4 & 22 \end{bmatrix}$$

(2×2)

Good Write

Exp] Plain text = A T T A C K

⇒ Let, Key = $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ { If it is given (n×n) → turn it to (n×1).

Since, the key is (2×2) matrix, plain text should be converted to vectors of length 2 (n×1).

For 1st, $\begin{bmatrix} A \\ T \end{bmatrix}$ $\begin{bmatrix} T \\ A \end{bmatrix}$ $\begin{bmatrix} C \\ K \end{bmatrix}$

Formula ⇒

$C = K\ P \bmod 26$

$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \Rightarrow \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} A \\ T \end{bmatrix}$

$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2\times0 & 3\times19 \\ 3\times0 & 6\times19 \end{bmatrix} \bmod 26$

$\therefore C = \begin{bmatrix} 57 \\ 114 \end{bmatrix} \bmod 26 = \begin{bmatrix} 5 \\ 10 \end{bmatrix} = \begin{bmatrix} F \\ K \end{bmatrix}$

For 2nd vector, $\begin{bmatrix} T \\ A \end{bmatrix} = \begin{bmatrix} 19 \\ 0 \end{bmatrix}$

$C = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 19 \\ 0 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 2\times19 & 3\times0 \\ 3\times19 & 6\times0 \end{bmatrix} \bmod 26$

Good Write

DATE: __/__/____
PAGE: _____

$= \begin{bmatrix} 38 \\ 57 \end{bmatrix} \bmod 26 = \begin{bmatrix} 12 \\ 5 \end{bmatrix} = \begin{bmatrix} M \\ F \end{bmatrix}$.

For 3rd vector, $\begin{bmatrix} C \\ K \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}$

$C = K P \bmod 26$

$= \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix} \begin{bmatrix} 2 \\ 10 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 34 \\ 66 \end{bmatrix} \bmod 26 = \begin{bmatrix} 8 \\ 14 \end{bmatrix} = \begin{bmatrix} I \\ O \end{bmatrix}$.

ATTACK, cipher text = F K M F I O.

To decrypt ⇒ Find inverse of key matrix K^{-1}

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

Cipher → F K M F I O

$K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$

Now, $K^{-1} = \frac{1}{|K|} adj(K)$

$d = \begin{vmatrix} 2 & 3 \\ 3 & 6 \end{vmatrix} = |12 - 9| = 3$

determinant
$d = \begin{vmatrix} a & b \\ c & d \end{vmatrix}$
$d = |ad - bc|$.

∴ determinant value of K, d = 3.

Good Write

DATE: __/__/____
PAGE: _____

Now, find multiplicative inverse of determinant.

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

So, $3 * d^{-1} = 1 \bmod 26$

So, $d^{-1} = 9$

meaning,

$3 * d^{-1} \equiv 1 \bmod 26$

$(3 * d^{-1}) \bmod 26 = 1$

Hit and trail

$1 \bmod 26 = 1$

$3 * d^1 \bmod 26 = 1$

$3 * 9^1 \bmod 26 = 1$

$27 \bmod 26 = 1.$

$\therefore$ determinant, $d = 3$

$d^{-1} = 9$

Now, we will find adjacent of the matrix,

Let,

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$ then,

$$adj(A) = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$$

$\therefore$ Here, $K = \begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$, $adj(K) = \begin{bmatrix} 6 & -3 \\ -3 & 2 \end{bmatrix}$

$$= \begin{bmatrix} 6 & -3+26 \\ -3+26 & 2 \end{bmatrix} = \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix}$$

Now,

$$K = \frac{1}{|K|} adj(K)$$

$$\Rightarrow |K^{-1}| adj(K) = d^{-1} adj(K)$$

Now, it's module 26,

$$K^{-1} = 9 \begin{bmatrix} 6 & 23 \\ 23 & 2 \end{bmatrix} \bmod 26$$

Good Write

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix}$$

Now, cipher = F K M F I O

$$C = \begin{bmatrix} F \\ K \end{bmatrix} \Rightarrow P = K^{-1} C \text{ mod } 26$$

$$= \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 5 \\ 10 \end{bmatrix} \text{ mod } 26$$

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

Similarly, $C = \begin{bmatrix} M \\ F \end{bmatrix} = \begin{bmatrix} 12 \\ 5 \end{bmatrix}$.

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 12 \\ 5 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 149 \\ 390 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 19 \\ 0 \end{bmatrix} = \begin{bmatrix} T \\ A \end{bmatrix}$$

Again,

$$\begin{bmatrix} I \\ O \end{bmatrix} = \begin{bmatrix} 8 \\ 14 \end{bmatrix}$$

$$P = \begin{bmatrix} 2 & 25 \\ 25 & 18 \end{bmatrix} \begin{bmatrix} 8 \\ 14 \end{bmatrix} \text{ mod } 26$$

$$= \begin{bmatrix} 366 \\ 452 \end{bmatrix} \text{ mod } 26 = \begin{bmatrix} 2 \\ 10 \end{bmatrix} = \begin{bmatrix} C \\ K \end{bmatrix}$$

∴ Plain text = ATTACK

Good Write

DATE: __/__/____
PAGE: _____

Cryptoanalysis: Cryptoanalytic attacks based on information known to the cryptoanalyst.

Types of cryptoanalysis:

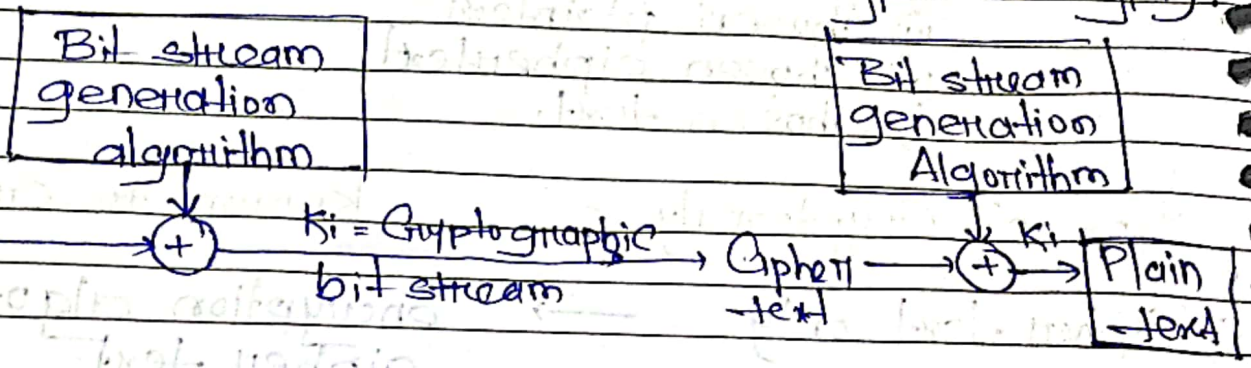
i) Ciphertext only
ii) Known plaintext
iii) Chosen plaintext
iv) Chosen ciphertext
v) Chosen text.

Type of Cryptoanalysis	Known to Cryptoana
i) Ciphertext only	→ encryption algorithm, ciphertext
ii) Known plaintext	→ encryption algorithm, ciphertext, one or more PT-CT (plaintext-ciphertext) pairs formed with secret key.
iii) Chosen plaintext	→ encryption algorithm, ciphertext, PT message choosen by cryptoanalyst, together with it's CT generated with secret key.
iv) Chosen ciphertext	→ encryption algorithm, Ciphertext, CT chosen by cryptoanalyst together with it's corresponding decrypted PT generated with secret key
v) Chosen text	→ Chosen plaintext and Chosen ciphertext

Good Write

Stream Cipher: It is the one that encrypts a digital (101000) data stream one bit or 1 byte at a time.

It is a symmetric key cipher. (i.e. key for encrypt + decrypt).



eg.: to encrypt:

	1	0	1	1	0	1	← message
XOR ⊕	0	1	0	1	0	1	← key
	1	1	1	0	0	0	← cipher

to decrypt:

	1	1	1	0	0	0	
⊕	0	1	0	1	0	1	
	1	0	1	1	0	1	← plain text

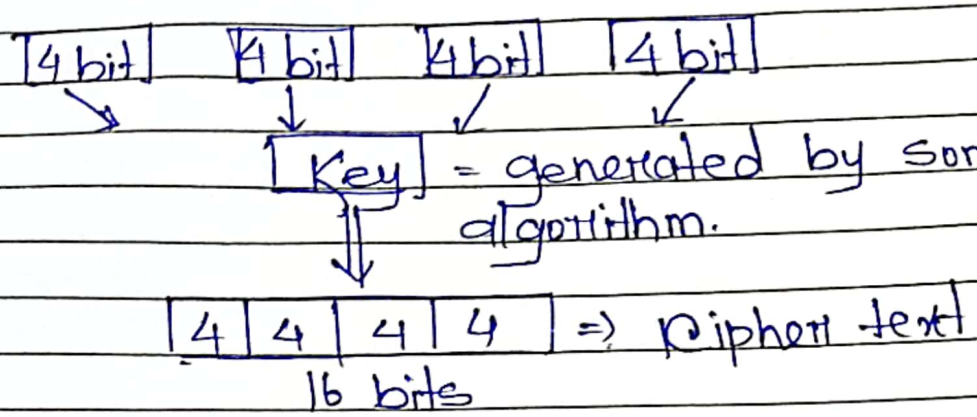
Block Cipher: In this, a blocks of plain text is treated as a whole and used to produce the cipher text of equal length.

Typically, a blocks size of 64 and 128 bits is used and also symmetric key Cipher.

Good Write

DATE: __/__/____
PAGE: _____

eg.



Block cipher	Stream cipher
(i) Plain text to cipher text by taking plain text blocks at a time.	(i) 1 bit or 1 byte of plain text → cipher text.
(ii) It uses 64 bit or more.	(ii) Stream cipher uses 8 bits.
(iii) Complexity of it is simple.	(iii) While stream cipher is more complex.
(iv) In this, reverse encrypted text is hard.	(iv) Reverse encrypted text is easy.
(v) ECB, CBC } algo	(vi) CFB, OFB } algo

Good Write