Defination of Computers Security: Computers security, also known as cybersecurity, is the protection of computers systems and networks from unauthorized access, use disclosure, disruption, modification or destruction of their hardware, software or data, encompassing various practices, techniques and process to safeguard digital assets and ensure data privacy.

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity availability and confidentiality of information ~~sys~~ resources. (Include hardware, software, firmware, information/data, and telecommunications).

Three key objectives that are the heart of the computer security.

Confidentiality	Integrity	Availability.
① Data Confidentiality.	Data Integrity	
② Privacy.	System Integrity	

The protection afforded (সুরক্ষা প্রদান) to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Three key objectives that are heart of CS

(1) Confidentiality:

i) Data Confidentiality: Ensure that private or confidential information is not made available or disclosed to unauthorized individuals.

ii) Privacy: Ensures that individuals control what information related to them may be collected and stored and by whom and whom that information may be disclosed.

(2) Integrity:

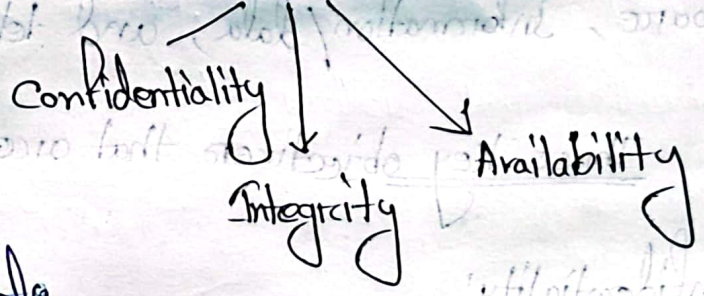
i) Data integrity: Ensure that information and programmes are changed only in a specified and authorized manner.

ii) System Integrity: Ensures the system works correctly and isn't changed or tempered with, either on

purpose or by accident..

③ Availability: Ensures that system work promptly (access) and service is not denied to authorize users.

→ To all Concept in the CIA Triad →



Two other concepts

Authenticity: The property of being genuine and being able to be verified and trusted.

Accountability: A security goal that makes sure every action can be clearly linked backed to the person or system that did it.

OSI Security Architecture:

The OSI security ~~structure~~ architecture focuses on security attacks, mechanisms and services.

(1) Security Attacks: A security attack is an attempt by a person or entity to gain unauthorized access to disrupt or compromise the security of a system, network, or device. These are defined as the actions that put at risk an organization's safety.

A) Passive Attacks: Attacks in which third party try to access the message/content/data being shared by the senders and receivers by keeping a close watch on transmission. Passive attacks are typically focused on gathering information or intelligence, rather than causing damage or disruption.

Two types of passive attacks are the ~~rea~~ release of (i) message contents and (ii) traffic analysis.

Message Contents: A telephone conversation, an electronic mail message and a transferred file may contain ~~sen~~ sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transformation.

Traffic Analysis: Suppose that we had a way of ~~masking~~ masking the contents of messages or other information traffic so that opponents even if they captured the message.

could not extract the ~~message~~ information from the messages. It is called encryption.

B) Active Attacks: Active attacks refers to types of attacks that involve the attackers actively disrupting or altering system network or device actively. Active attacks are typically focused on causing damage or disruption rather than gathering information or intelligence.

② Security Mechanism: A process that is designed to detect, prevent or recover from a security attack. It is also responsible for protecting system network or a device against unauthorized access or ~~there~~ other security threats.

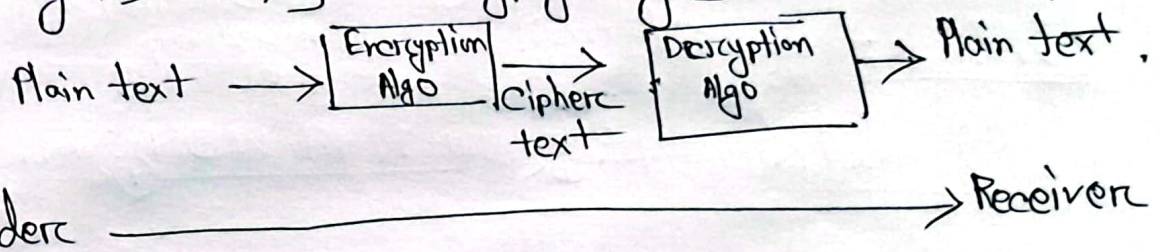
a) Specific Security Mechanism:

Segment-2:

Cryptography: Cryptography is the practice of securing communication by converting plain text into ~~ey~~ ciphertext.

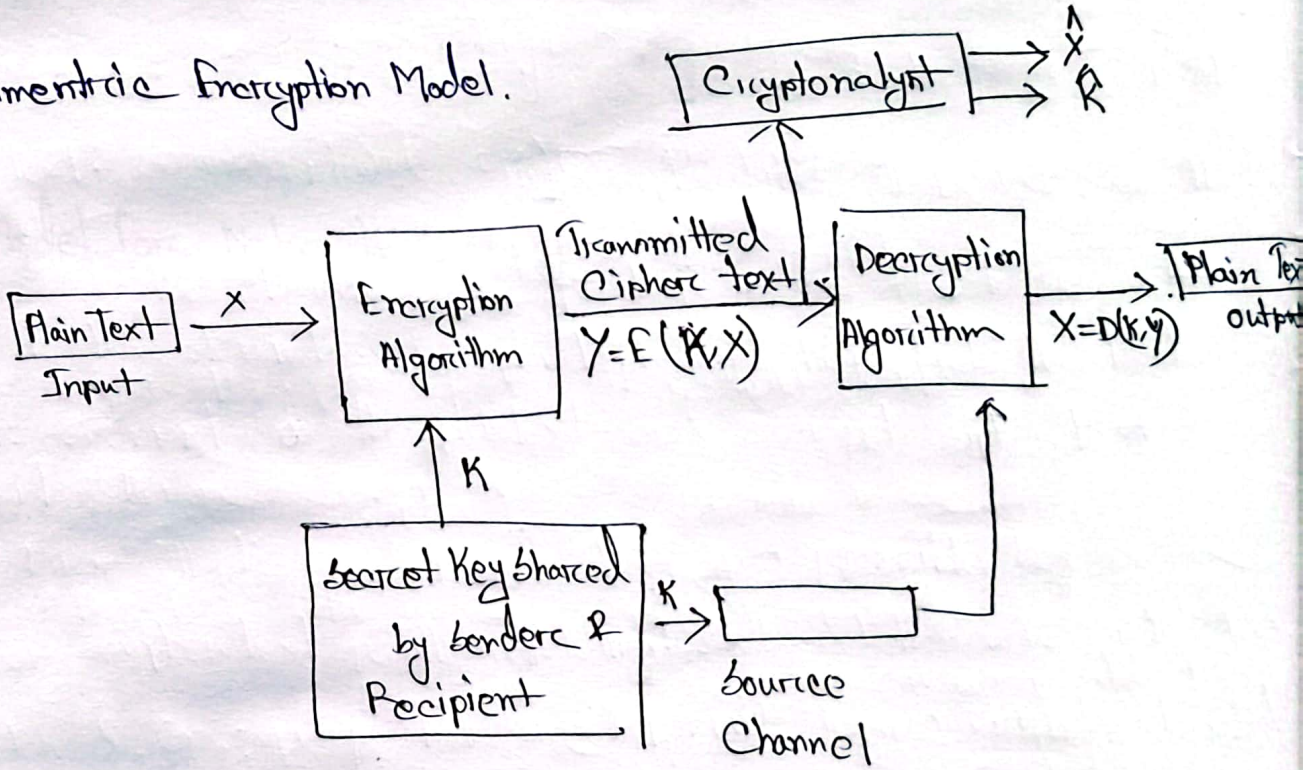
↘ Normal text ↘ Secret message.

Confidentiality বজায় রাখার জন্য আমরা Cryptography ব্যবহার করি।



Sender ——————————→ Receiver.

Symmentric Encryption Model.



(i) Secret Key: The key used for encryption and decryption also known as symmantic keys.

(ii) Plaintext: Normal Message.

(iii) Ciphertext: Secret message.

(iv) Encryption Algorithm: Perform encryption and does various substitution and transformation on the plaintext.

(v) Decryption Algorithm: It taken secret key and ciphertext and produces the original plaintext.

Example: one time pad.

Key - 0101110010

⊕ Plain Text - 1100011000

Cypherc text - 1001101010

Encryption: $C = E_K(m) = m \oplus K$

Decryption $D_K(c) = c \oplus K = (m \oplus K) \oplus K$

$= m$

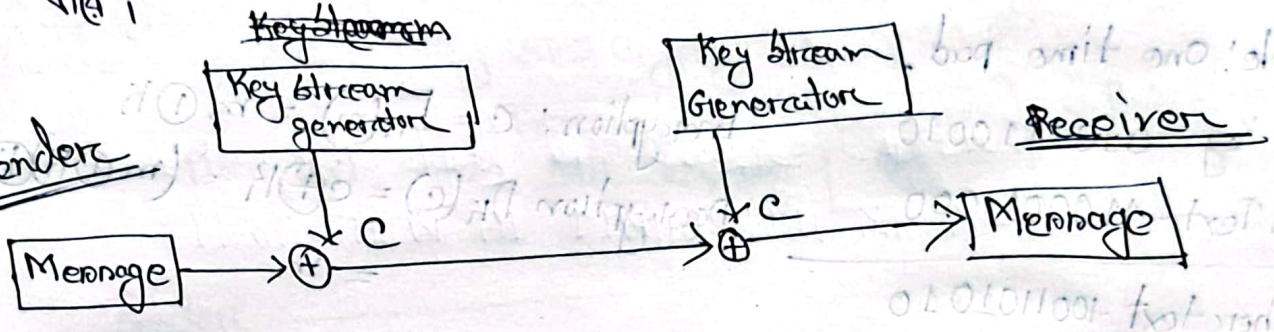
XOR - Same হলে output 0
Diff হলে 1

Requirements for secure use of conventional Encryption.

1. Hackerc এর কাছে একটা কার্যকর plaintext এবং ciphertext থাকা সত্ত্বেও যাতে সে পাঠানো cypherctext decrypt করতে না পারে এ ব্যবস্থা নিতে হবে.
2. যে key টি Cypherctext এ ব্যবহার হয়েছে তার কপি Senderc এবং Receiverc এর কাছে থাকতে হবে এবং তা secure রাখতে হবে।
3. Encryption Algo secure রাখার প্রয়োজন নেই। Key secure রাখতে হবে,
4. Encryption Algo ব্যবহার করে থাকে Developerc কাস্টমারের Data Encrypt করতে, সাথে এবং Encryption Algo chip কাস্টমারকে করে।

Stream Cipher: A symmetric-key encryption method that encrypts data bit by bit or byte by byte by combining the plain text with a pseudorandom keystream.

↳ Pseudorandom generator Message কে bits এ convert করে।



Cryptoanalysis: [cypher text কে key add করে plain text বের করা বা plain text কে understand করা।] Cryptanalytic attacks rely on the nature of the algorithm plus perhaps some knowledge of general characteristics of plaintext and key which the hacker use to understand the plaintext and decrypt cipher text.

Brute Force Attack: (→ Trial and Error) The attacker tries every possible key on a piece of cypher text until an intelligible translation into ciphertext is obtained. On average half of all possible keys must be tried to achieve success.

A Encryption is said to be secure if it contains two criteria.

(i) The cost of breaking the cipher exceeds the value of the encrypted information.

(ii) The time required to breaks the cipher exceeds the lifetime of the information.

Substitution Cipher: It is a technique in which the lattery of plain text are replaced by other lattern or by numbers or symbols.

[ঐ latter বা symbol গুলোর Replaced করার ব্যবহৃত হয়েছে তা 2nd time ব্যবহার হবে না।]

Substitution Technique:

Ceaser Cipher (Shift Cipher):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Plain:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Cipher:	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s

	16	17	18	19	20	21	22	23	24	25
Plain:	Q	R	S	T	U	V	W	X	Y	Z
Cipher:	t	u	v	w	x	y	z	a	b	c

$$3 \overline{)26} \quad 24$$

$$26 \mid 3 \mid 0$$

$$\underline{0}$$

$$3$$

Encryption:

$$C = E(3, P) = (P+3)^{K} \bmod 26.$$

$$A \rightarrow = (0+3) \bmod 26$$

$$= 3 \rightarrow d.$$

plain text: FIVE MINUTES

Cipher text: ilyh plaqxwhv

Decryption: $P = D(3, C) = (C - \frac{K}{3}) \bmod 26$

Brute Force Cryptoralysis for Ceaser Cipher:

Plain: PHHW PH DIWHU WKH NRJD

Key:

1: oggr og chrgt kjg rqic.

2: nffu nf bgufs uif uphb.

3: meet me after the party.

Key ব্যতীত যাতে plain text কে সনাক্ত করা যায় তাই করা হয়।

One time Pad (Vernam Cipher).

Plain text: H E L L O

7 4 11 11 14

Key: b a x y c [random]

1 0 23 24 2

(i) Single in use
(ii) Cannot be cracked.
(iii) Key is random and never reuse so it is impossible to learn anything about message or ciphertext without secret key.

Add: 8 4 34 35 16

Subtract: 8 4 8 8 16

[যোগ সংখ্যা 26 থেকে বড় হলে 26 বাদ দিতে হবে]

Ciphertext: i e i j q

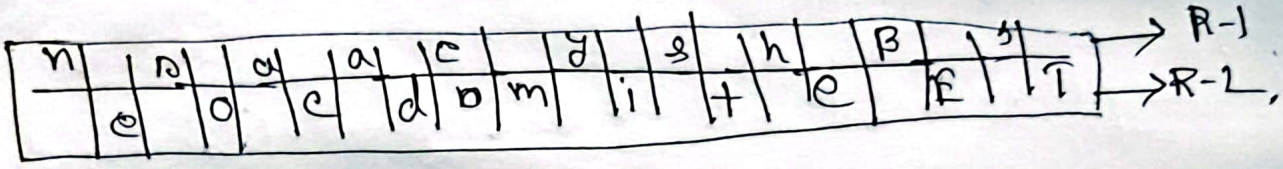
Transposition Techniques / Ciphers.

↳ Plaintext এর position change করা হয় এবং এর 2 টি type Transposition এর।

Rail Fence:

Plain Text: NEGO ACADEMY IS THE BEST

depth : 2 → Row



nnaeyhbeocdomitect.

Columnar Transposition Techniques:

plain text: FIVE MINUTES ENGINEERING

Key: 4351L [column এর নাম্বার অনুযায়ী হবে না]