Date: __/__/2023 M T W T F S

INFORMATION SECURITY:-

→ Information Security covers the tools and processes that organizations use to protect information. This include policy settings that prevent the unauthorized people from accessing personal information.

→ Information security protects sensitive information from unathorized activitis, including inspection, modification, recording, and any disruption and destruction.

Goal:-

The goal is to ensure the safety and privacy of critical data such as customer

Date: __/__/2023

account details, financial data or intellectual property.

→ "The process in which we take different measures and use different tools to secure the information."

Attack / Threat :-

→ An activity in which data is on risk is called attack or threats.
e.g : Hacking

Types of threats :-

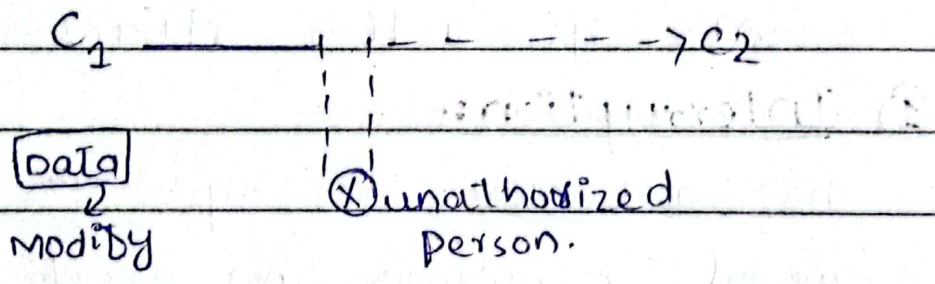
1. Active threats
2. Passive threats

Active Threat :

An active threat is there is a communication

Date: __/__/2023

takes place between two computers C1 and C2. C1 sends message and on the same time unathorized person comes and modify the message (data) and send to the second computer (C2).



→ Data send to the receiver after modification.

Passive Threat :-

In passive threat if C1 send data to C2. It cannot reach on the receiver end, because when C1 send data it

Date: __/__/2023 M T W T F S

will be blocked by anathorized person.

e.g:

Scamming, Fraud

Variations:-

Security Threats:-

There are four common varients of active attacks.

① Interruption:-

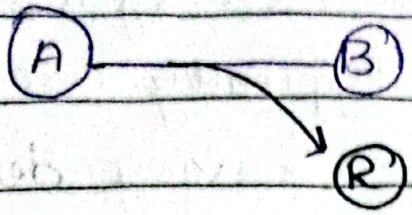
The attacker interrupts the origional communication and creats new malacious messages, pretending to be one of the communication parties.

② Interception:-

In the interception the third party listen the communication between

Date: __/__/2023

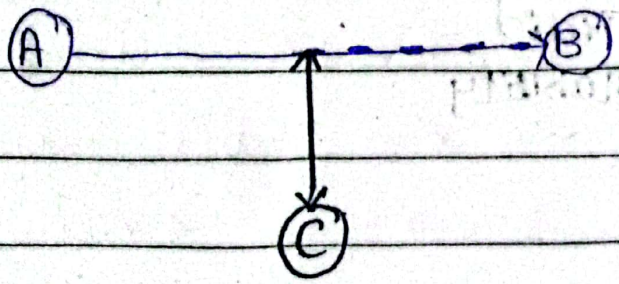
A and B.



(3) **Modification:-**

→ The attacker (third-party) steal the data and modify this data with respect to their requirements.

→ The attacker uses existing communications, and either replays them to fool one of the communicating parties, or modifies them according to their need / to gain an advantage.



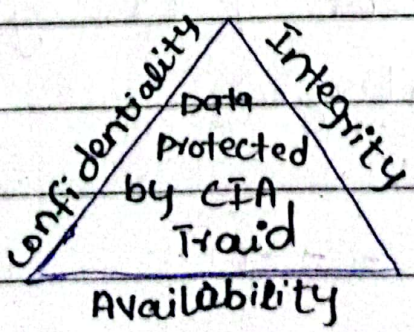
Date: __/__/2023 M T W T F S

Fabrication :-

Creates fake, or synthetic, communications, typically with the aim of achieving denial of service (DoS). This prevents users from accessing system or performing normal operations.

PRINCIPLES OF Infosec :-

1. Confidentiality
2. Integrity
3. Access control
4. Authenticity
5. Availability

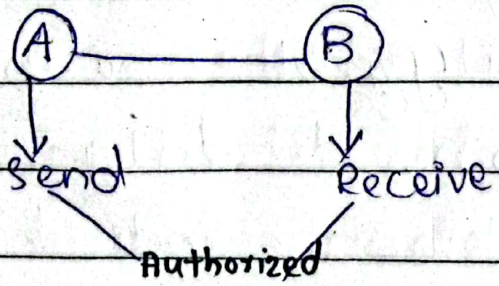


Date: __/__/2023

M T W T F S

Confidentiality :-

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of this principal is to keep personal information private and to ensure that it is visible and accessible only those individuals who own it or need it to perform their organizational functions.

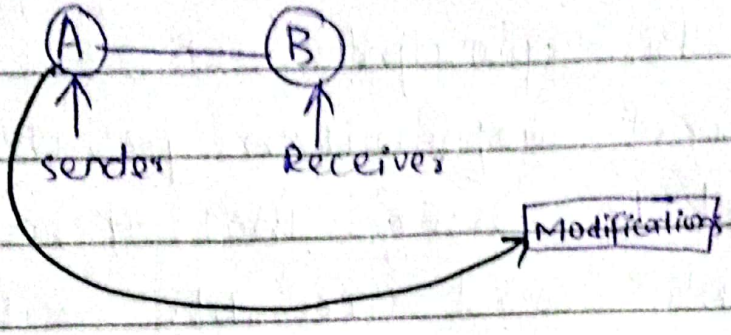


Integrity :-

Consistency includes protection against unathorized changes (addition, depetion, alterations etc)

Date: __/__/2023

to data. It ensures that no one can modify the data untill the sender itself want to change the data.



Availability :-

This means The final component of CIA Traid is availability. It means the system and data are available to individuals when they need it under any circumstances; including power outages or natural disasters.

Date: __/__/2023

M T W T F S

Access Control :-

Access control is a data security process that enables organizations to manage who is authorized to access coperate data and resources.

Security Mechanism :-

Security Mechanism: are the set of steps that are used to detect, prevent and recover the data from attacks to make a system secured.

Types of Security Mechanism are:

① Encipherment ② Access control

Date __/__/2023

(3) Authentication (4) Data Integrity
(5) Routing control (6) Traffic padding (7) Notarization (8) Digital signature.

Encryption:-

This security mechanism deals with hiding and covering of data which help of data to become confidential. It is acheived by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is acheived by two famous techniques named Cryptography and Enchipherment.

Plain text → Simple
Cipher text → Encrypted.

Date: __/__/2023

M T W T F S

Access Control :

→ Who can access what?

- User pannel
- Admin Pannel

جس کو جتنی زیادہ authority دی جائے گی
اس کا access control اتنا ہی زیادہ ہوگا۔

Authentication :-

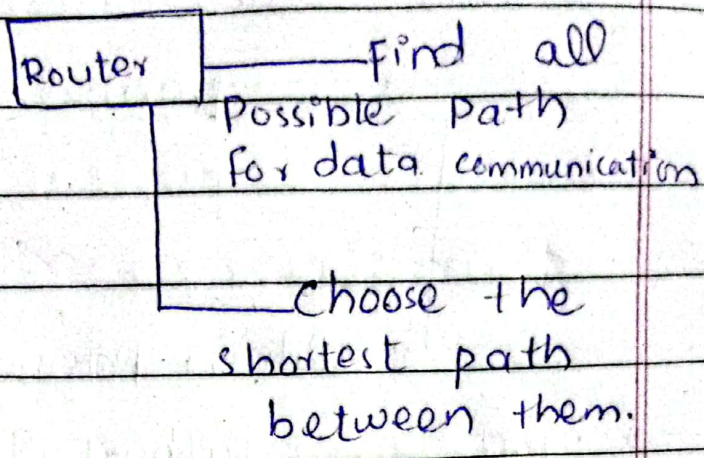
Authentication technology provides access control for system by checking to see if a user's credantials match the credantials in a database of authorized user or in a data authentication server.

جس کے پاس credantials ہونگے وہی استعمال کر سکے گا
یہ۔

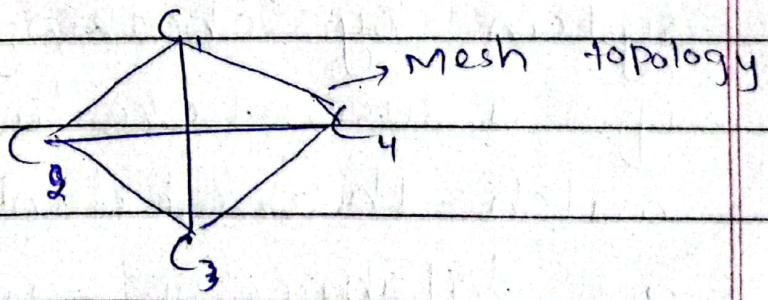
Date: __/__/2023

M T W T F S

Routing Control:-



→ Routing means selecting and continously changing different available routes between sender and receiver to prevent the opponent from, eavesdropping on a particular route.



Available path:-

$C_1 - C_3$

$C_1 - C_2 - C_3$

$C_1 - C_4 - C_3$

$C_4 - C_2 - C_4 - C_3$

Date:__/__/2023

M T W T F S

Advantages:-

- Time
- Cost
- Privacy
- shortest path (if one blocked the other can use for communications.)

Data Integrity:-

Data integrity is a concept and process that ensures the accuracy, completeness, consistency and validity of an organization's data. It is also ~~refered~~ a concept of delivering data based on rules(accuracy).

e.g.:

The sender sends three messages to the receiver. When the data (msg) is received on the receiver

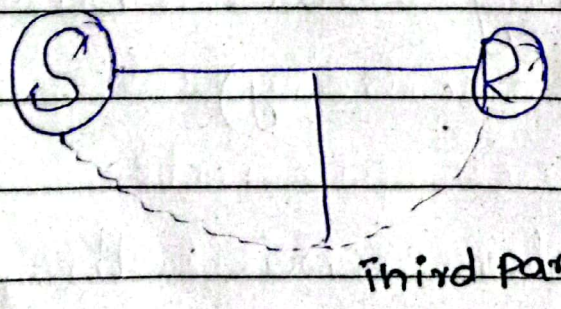
end, the data must be complete, accurate and consistant.

Traffic Padding :-

The insertion of bits into gaps in an information flow is known as traffic padding.

Nortraization :-

The process of solving a conflict between sender and receiver is known as nortraization.



Digital Signature :-

(Electronically verification)

Date __/__/2023

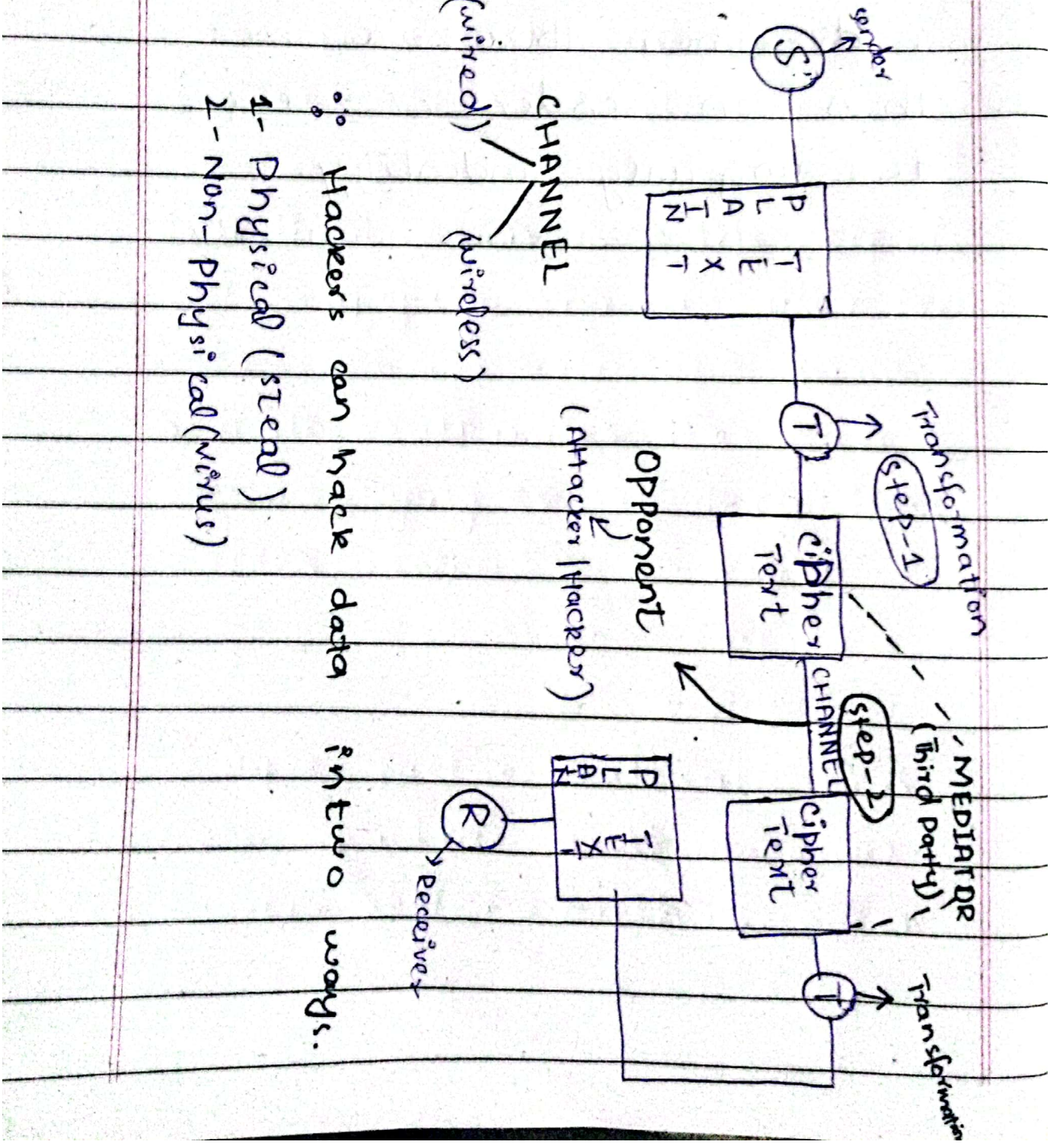
M T W T F S

→ Digital signatures are like electronic "fingerprints". They are a specific type of ~~code~~ electronic signature (e-signature), in the form of coded message.

→ These are the special codes used when there are more than on senders or receiver, to uniquelly identify.

Security Model:-

It is a model which describes the different phases of communication over a secured network.



∴ Hackers can hack data in two ways.

1- Physical (steal)

2- Non-Physical (virus)

Date: __/__/2023

M T W T F S

Security Models:-

1- Protocols (http, https)

→ Protocols are the set of instructions that governs the operating system.

2- Algorithm:-

Different algorithms are used to convert plain text into cipher text (msg+3) and transform cipher text into plain text (msg-3).

3- Channel:-

(i) Wired (ii) Wireless

4- Security:-

(i) Symmetric (ii) A-Symmetric

→ Symmetric:

Protecting data using a secret key to encrypt (lock) and decrypt (unlock) it.

→ Asymmetric:

Allows users to encrypt

Date: __/__/2023

information using shared keys.

Authentication Method OR Models:-

→ Authentication is simply a verification of users including his password and username.

* Authentication vs Authorization:

→ Authentication is the process of verifying who a user is.

→ Authorization is the process of verifying what they have access to.

Models:-

- Single factor authentication
- Two factor authentication
- Multi-factor authentication

Date: __/__/2023 M T W T F S

Single Factor Authentication:-

→ Single factor usually means password-only authentication. This model applies to any authentication platform that uses only one factor; even biometric falls in it.

→ It leaves a single layer of security between the hackers and their target.

→ It is regarded as the weakest of all authentication models. Passwords can easily be cracked, guessed or stolen.

Two Factor Authentication:-

Two factor authentication (2FA) is a security system that requires two seperate, distinct forms of identification.

Date: __/__/2023

M T W T F S

in order to access something. The first factor is password and second commonly includes a text with a code sent to your smartphone (OTP).

Multifactor Authentication:-

Multifactor authentication (MFA) is a multi-step account login process that requires more information than just a password.

e.g: Along with the password users might be asked to enter a code sent to their email, answer a secret question, captcha or scan a fingerprint.

OS Authentication method:-

→ The user authentication process is used just to

Date: __/__/2023 M T W T F S

identify who the owner is or who the identified person is. Generally, this type of authentication can be performed by using a password.

→ There is no need of physical availibility.

Physical Methods:-

1. Bio-Metric
2. Retina (Eye scan)
3. Facial Expressions
4. voice Detection
5. Signature (e-signature).

Date: __/__/2023

CRYPTOGRAPHY :-

↳ The study of encryption methods is called cryptography.

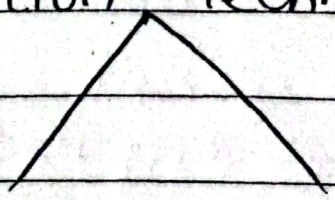
Code Braking :-

The process of decrypting a cipher text is known as code braking.

Cryptology :

The process of cryptology + crypto-analysis of a cipher text is known as cryptology.

Encryption Techniques



Substitution Transposition

Date: __/__/2023 M T W T F S

Substitution:-

The process in which a letter is replaced with another letter.

e.g $\begin{bmatrix} A \rightarrow \pi \\ B \rightarrow Y \\ \text{Ɛ} \rightarrow Z \end{bmatrix}$

Transposition:-

The technique in which letters are arranged.

e.g:

$$NESO \rightarrow \begin{bmatrix} E\ S\ N\ O \\ S\ E\ N\ O \\ O\ N\ E\ S \end{bmatrix}$$

Algorithms:- (Methods)

CEASER CIPHER:-

→ It is a method of substitution, technique of encryption.

→ Introduced by "Julis Ceaser"

→ It allot specific numbers to alphabets from (0 → 25).

0	1	2	3	4	5	6	7	8	9	10	11	12
A	B	C	D	E	F	G	H	I	J	K	L	M
13	14	15	16	17	18	19	20	21	22	23	24	25
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

→ Formula:-

- Encryption of plain text:

$$C = (E(P) + k) \% 26$$

- Decryption of cipher text:

$$P = (E(C) + k) \% 26$$

Example:-

BAG

Encryption: $\left[C = (E(P) + k) \% 26\right]$

→ Addition (3) and take Mode with 26.

$B = 1 + 3 = 4 \% 26 \Rightarrow 4 \rightarrow E$

$A = 0 + 3 = 3 \% 26 \Rightarrow 3 \rightarrow D$

$G = 6 + 3 = 9 \% 26 \Rightarrow 9 \rightarrow J$

Date: __/__/2023 M T W T F S

Decryption:-

EDJ

→ Subtract (3) and take mode with 26.

E = 4 - 3 = 1 %o 26 ⇒ 1 → B

D = 3 - 3 = 0 %o 26 ⇒ 0 → A

J = 9 - 3 = 6 %o 26 ⇒ 6 → G

Encryption formula proof:-

$C = (E + (P) + K) \%o 26$

$C = (E(B) + 3) \%o 26$

$C = 1 + 3 \%o 26$

$C = 4$

Date: __/__/2023 M T W T F S

Play Fair:-

→ Invented by wheatstone.
→ It is invented in 1854.
→ It is called diagraph, encryption algorithm because pairs are replaced at single time.
→ It is mostly used in WW I – WW II.

Rules:-

1. Create a diagram of 5 x 5 matrix.
2. Repeated letter in pair are replaced by x.
3. If pair belongs to some column ↓ Round wrap.
4. If Pair belongs to some Row → Round wrap.
5. If Rectangle is created ⇄ swap.

Date: __/__/2023 M T W T F S

(6) I/J have the same value.

(7) use key of your own choice.

(8) Letters are not repeatedly used in Matrix.

Step 1- create a diagram of 5x5 matrix.

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

key : GOODBOY

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