Topics Covered

1. What is Cryptography? (Introduction)
2. Types of Cryptography – Symmetric
   – Asymmetric
   – Hashing
3. CIA Triad | Security Goals and Security Services.
4. Security Attacks in Cryptography.
5. Security Mechanisms in Cryptography.
6. Substitution and Transposition Techniques
   - monoalphabetic cipher
   - polyalphabetic cipher
7. Rail fence & Row Transposition techniques
8. keyless and keyed " "
9. Caesar Cipher
10. Playfair cipher.
11. Vigenere Cipher. method-1

position techniques
- monoalphabetic cipher
- Polyalphabetic cipher

7. Rail fence & Row Transposition techniques
8. keyless and keyed " "
9. Caesar Cipher
10. Playfair cipher.
11. Vigenere Cipher. method-1
12. Vigenere Cipher method-2
13. Hill Cipher (encryption + Decryption)
14. (3x3) example
15. Stream & Block cipher and their difence b/w
16. Shannons Theory of Confusion & Diffusion.
17. fiestel structure | cipher
18. DES in detail
19. key genera[illegible] in DES
20. Vernam Cipher.

Security Goals

CIA triad in crypto

1) CONFIDENTIALITY - It is the most common aspect of info. security.

* It allows authorized users to access sensitive & protected data.
The data sent over the network shouldnot be accessed by unauthorized users/individuals.

Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data so that even if attacker gains access, he/she will not be able to decrypt it.

2) INTEGRITY - [eg] In a bank, when we deposit/withdraw money the balance needs to be maintained.

Integrity means that changes need to be done only

Attacker will try to capture data. To avoid this, various encryption techniques are used to safeguard our data so that even if attacker gains access, he/she will not be able to decrypt it.

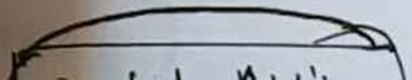
2) INTEGRITY – [eg] In a bank, when we deposit/withdraw money, the balance needs to be maintained.

Integrity means that changes need to be done only by the authorized entities and through authorized mechanisms, and nobody else should modify our data.

3) Availability → data must be available to the authorized user.

Info is useless if we cannot access it.

eg) what would happen if we cannot access our bank accounts for transactions.



withdraw money, the balance needs to be maintained.

Integrity means that changes need to be done only by the authorized entities and through authorized mechanisms and nobody else should modify our data.

---

3) Availability → data must be available to the authorized user.

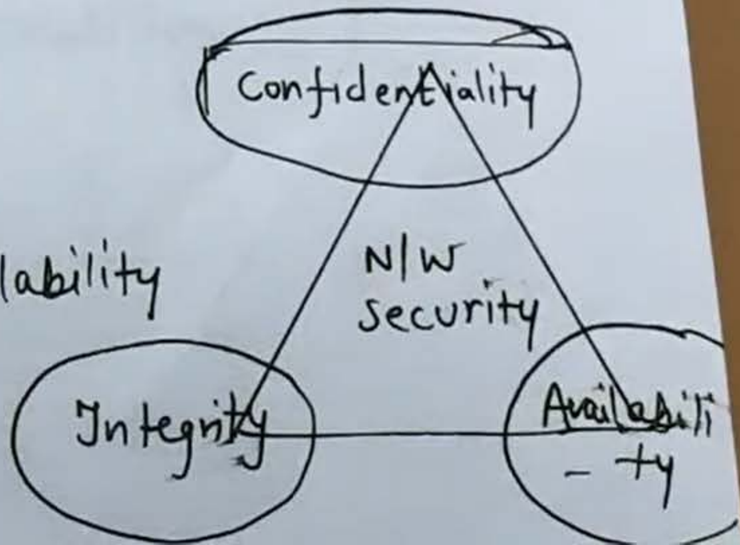
Info is useless if we cannot access it.

eg) what would happen if we cannot access our bank accounts for transactions.

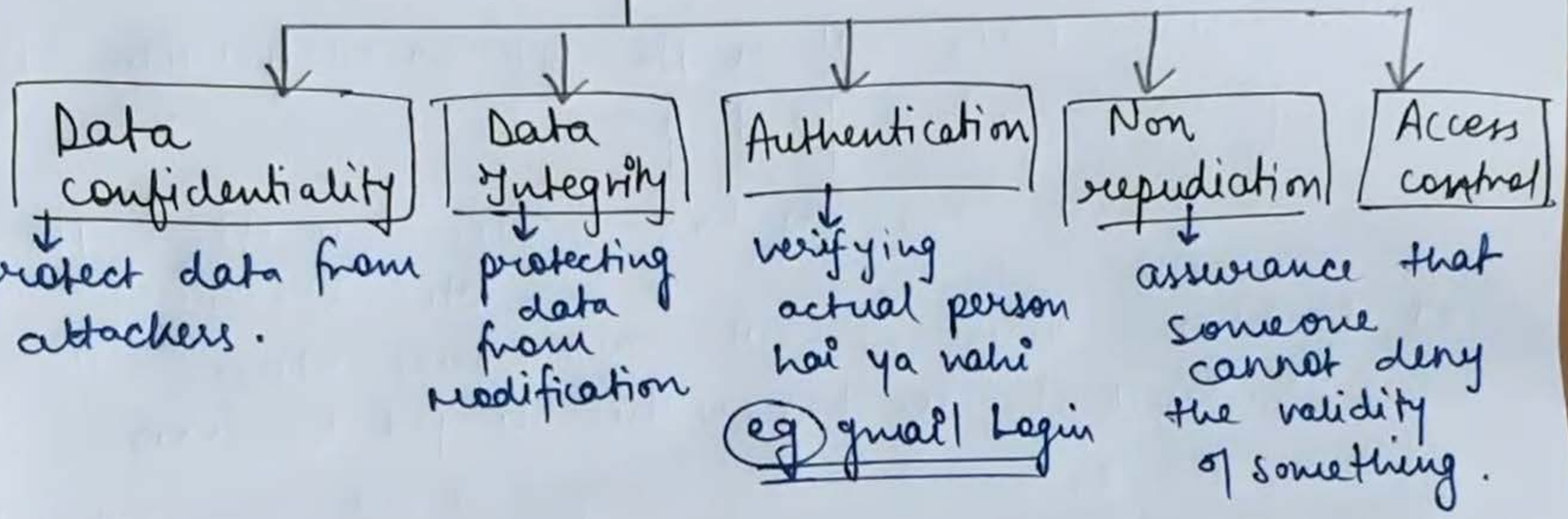
C I A triad in cryptography

↓

confidentiality, Integrity and availability



Security Services



Repudiation → denial of truth or validity of something
ie. act of claiming that something is invalid.

(H) **Non Repudiation** → is a service, which provides proof of the origin of data and the integrity of the data.

claiming that something is invalid.

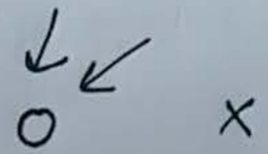
(4) Non Repudiation → is a service, which provides proof of the origin of data and the integrity of the data.

eg A give 1000 Rs check to B. and later B deny it.
It cannot happen b/c A will have its proof.

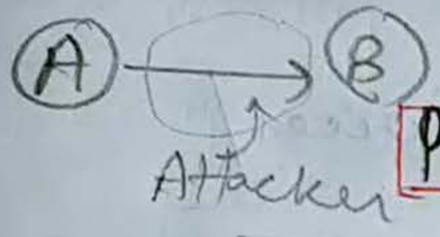
(5) Access control → to whom the access should be given can be decided.

or

The prevention of Unauthorized use of a resource (i.e, this service controls who can have access to our info, under what conditions).



Security Attacks



Passive Attack

Active attack

It attempts to learn or make use of the info from the system but doesnot affect the system resources.

i.e the attacker will only see the data he will not modify it.

We can prevent it using better encryption techniques.

Two types of passive attacks

1) Release of message content → attacker/hacker will easily be able to understand the data/inf

Two types of passive attacks

1) Release of message content → The attacker/hacker will easily be able to understand the data/info.

2) Traffic analysis → If we have encryption protection, an opponent/attacker might still be able to observe the pattern of these messages.

The attacker could determine the location and the identity of communication hosts and could observe the frequency and length of the message being exchanged.

This info might be helpful in guessing the nature of communication that was taking place.

Passive attacks are difficult to detect b/c they do-

Observe the pattern of

The attacker could determine the location and the identity of communication hosts and could observe the frequency and length of the message being exchanged.

This info might be helpful in guessing the nature of communication that was taking place.

Passive attacks are difficult to detect b/c they do not involve any alteration of data.

So, the sender & receiver will not be able to know whether a third person is reading their msg or NOT.

→ he can [see + modify] msg

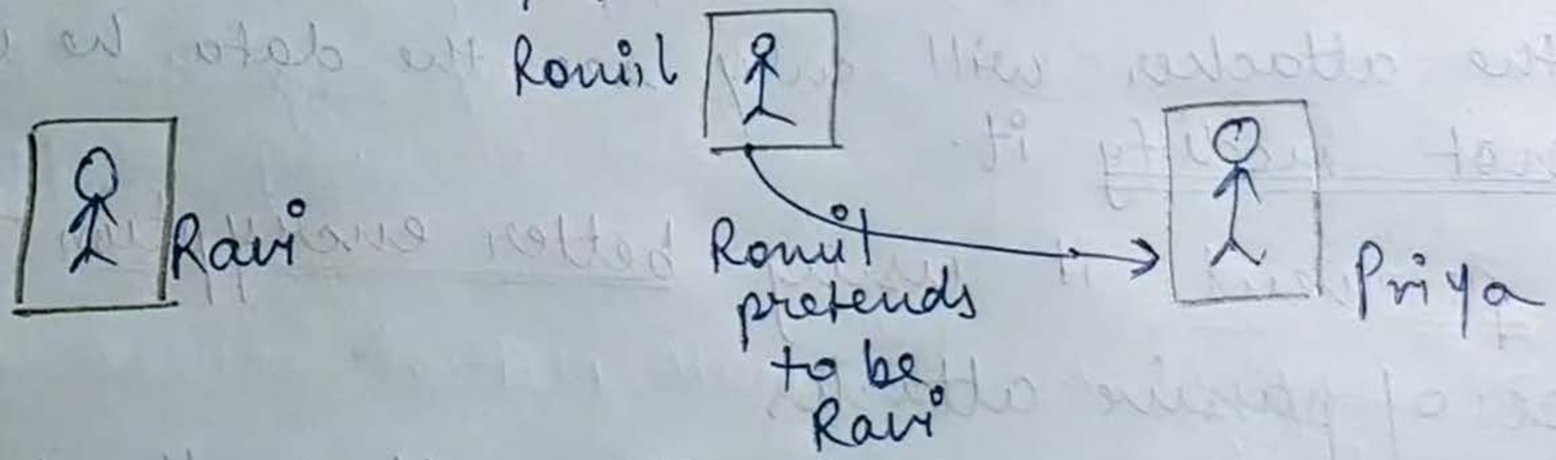
2) ACTIVE attacks

It attempts to alter system resources/ info [redacted].

(i) masquerade

→ when one entity pretends to be another entity.

eg

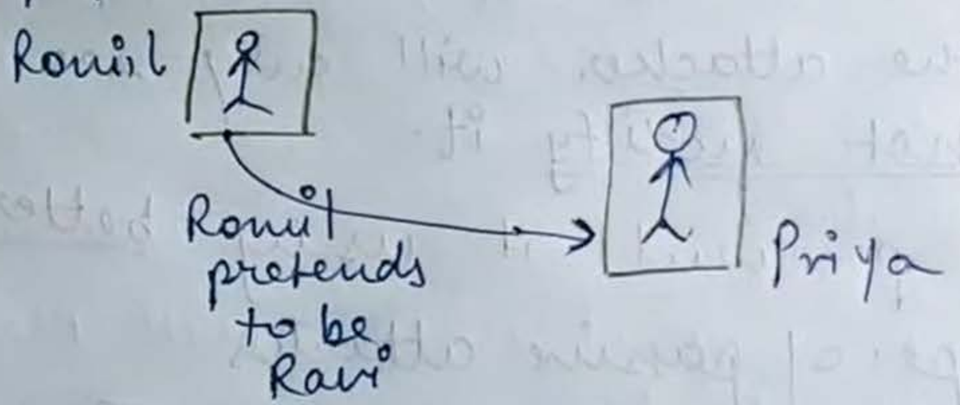


(ii) modification of messages

(iv)

(i) masquerade
→ when one entity pretends to be another entity.

eg



(ii) modification of messages
some portion of the message is altered or the message is delayed or reordered to produce an unauthorized effect.

eg) give 100 Rs to John

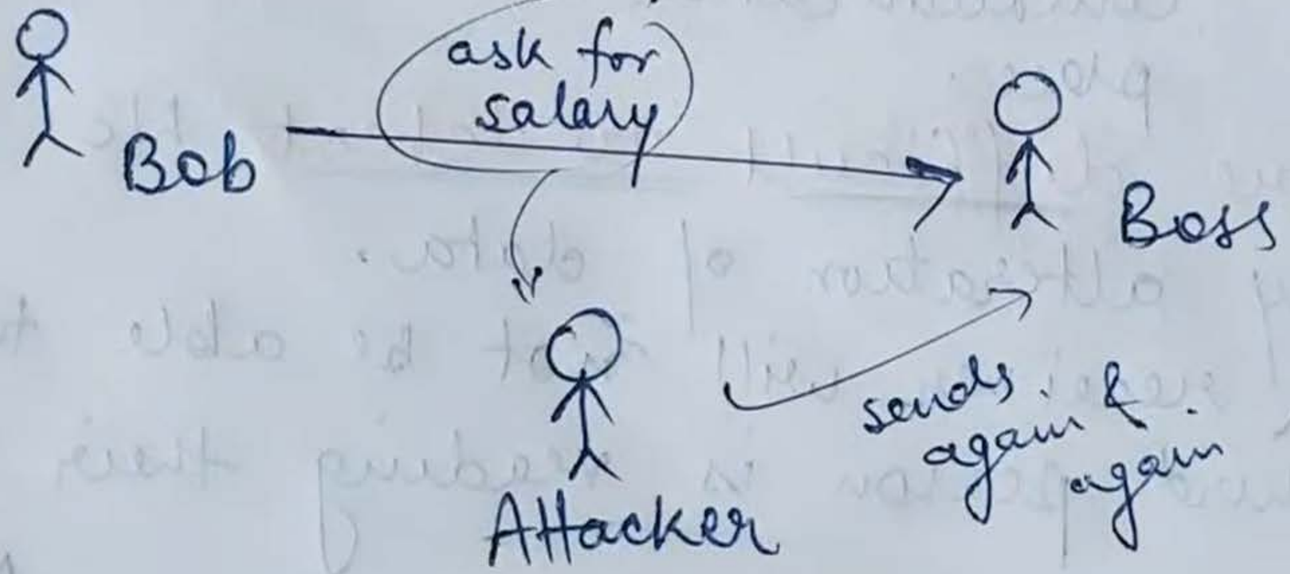
↓

give 500 Rs to Gaurav

give 500 Rs to Gaurav

(iii) ~~Replay~~ → Replay
involves passive capture of a message and its subsequent retransmission to produce an unauthorized effect.

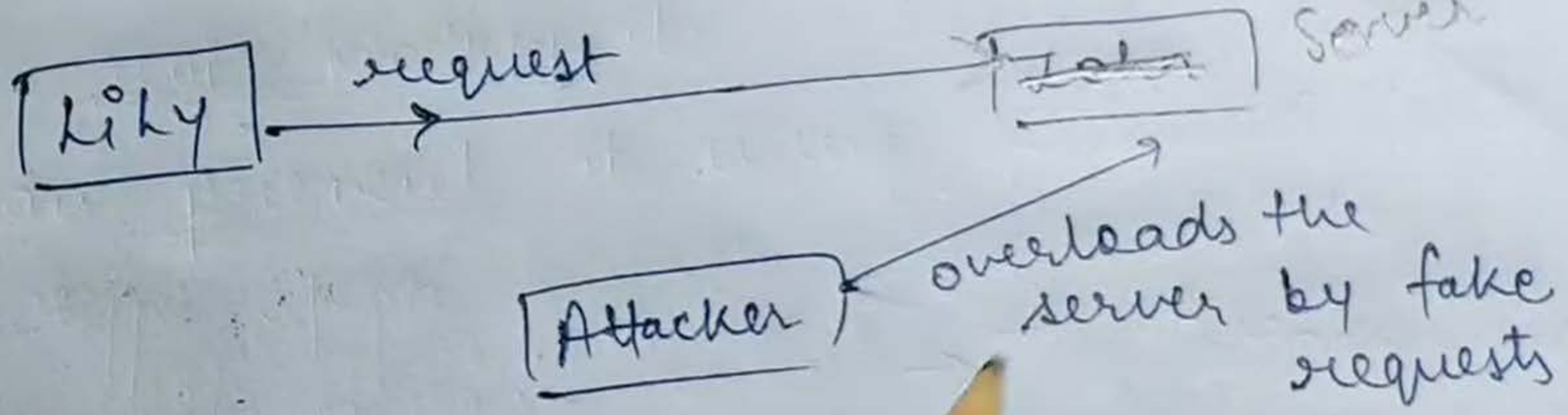
eg)



(iv) Denial of services

It prevents normal use of communication facilities.

eg) disruption of an entire network whether by disabling the network or by overloading it by messages so as to degrade performance.



5th video

Security Mechanisms

Security mechanisms are used to provide security.

1) Encipherment → The use of mathematical algo.s to transform data into a form that is not readily intelligible.

plain text to cipher text

2) Digital Signature → It is a means by which the sender can electronically sign the data and the receiver can electronically verify the

1) A ⟶ B

Plain → encrypt → ci

not readily intelligible.

plain text
to cipher text

2) Digital Signature → It is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

or we can say, it is a mathematical scheme for authentication.

3) Data Integrity →

1) A ⟶ B

Plain → encrypt → ciph

signature.

or we can say it is a mathematical scheme for authentication.

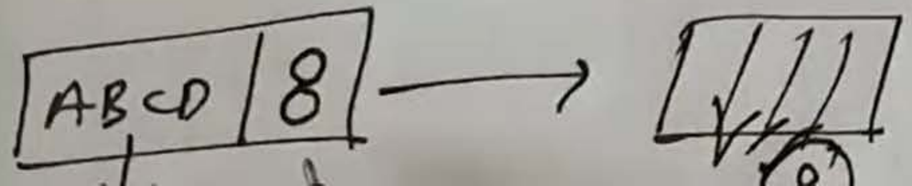
3) Data Integrity →

This mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver creates a new checkvalue from the received data and compares the newly created check-value with the one received.

If both the values are same, the integrity of

1) A ⟶ B

Plain → encrypt → cipher

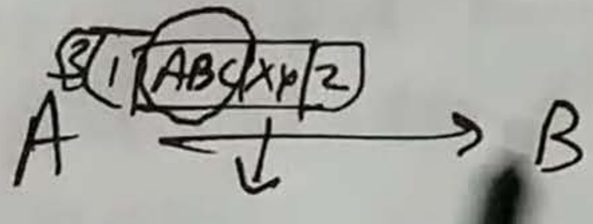


from the received data and compares the newly created check-value with the one received.

If both the values are same, the integrity of the data has been preserved.

4) Authentication exchange –
In this, two entities exchange some messages to prove their identity to each other.

5) Traffic Padding → In this technique, we add some extra/dummy bits with the data while encrypting



6) Routing control

means selecting and continuously changing different available routes b/w the sender & the receiver to prevent the attacker from eavesdropping on a particular route.

↓

पासू सी

ओएसपीएफ

7) Access control -
These methods prove that a user has access right to the data.

8) Notarization → means selecting a trusted third party to control the communication between two entities. This can be done (for eg) to prevent repudiation.