SOME BASIC TERMINOLOGIES:

1. THREAT:

Anything (object, human or substance) that has the tendency that could damage or destruction or a possible danger that might exploit a vulnerbility.

2. ATTACK:

Unauthorized actions on the digital assets. The use of threat to exploit a vulnerability and cause harm to the system. An attack is done delibrately.

3. VULNERBILITY:

A weakness in a control or a system that can be exploited by a threat.

4. ASSET:

Anything of value. The entire property of an entity (Person, Organization, Government).

5. CONTROL:

An action implemented to counter a potential threat and protect our asset and thus reducing the risk.

6. RISK:

The likelihood of a threat exploiting a vulnerability in a control to cause damage to the asset.

a. INHERENT RISK:

This type of risk is any that occurs naturally due to a factor other than a failure of internal control.

b. RESIDUAL RISK:

The risk remaining after efforts have been made to reduce the inherent risk.

7. EXPLOIT:

An exploit is a program that is designed to take advantage of vulnerabilities or exploits are the tools used by hackers to break into a computer. Expoit is a threat.

8. BUG:

A bug is any mistake in a program that causes it to behave in a way that is not intended by the developer or not welcome by the user.

DIFFERENCE BETWEEN BUG AND VULNERABILITY:

A bug is any mistake in a program that causes it to behave in a way that is not intended by the developer or not welcome by the user while a vulnerability is bug that can be exploited by the attacker to compromise the security of the system or gain access to the system.

9. CRYPTOGRAPHY:

The science of secret writing. Or converting the intelligible message to unintelligible message to make it unreadable to attacker on the internet.

10. CRYPTANALYSIS:

The breaking of secret writing. It is the study of breaking the ciphers by finding loopholes or bugs in the encryption or decryption algorithms used in

cryptography.

11. CRYPTANALYST:

Person performing cryptanalysis.

THE OSI SECURITY ARCHITECHTURE:

The OSI security architechture deals with three things:

1. Security Attacks
2. Security Services
3. Security Mechanisms

- Security Attacks
  - Cryptanalytic Attacks
    1. Ciphertext only Attack
    2. Known Plaintext Attack
    3. Chosen Ciphertext Attack
    4. Chosen Plaintext Attack
    5. Chosen Text Attack
  - Non Cryptananlytic Attacks
    1. Active Attacks
       - Threats to Integrity
         a. Modification
         b. Masquerade
         c. Replaying
         d. Repudiation
       - Threats to Availability
         a. DOS Attacks
    2. Passive Attacks
       - Threats to confidentiality
         a. Snooping
         b. Traffic Analysis

- Security Services
  1. Data Confidentiality
  2. Data Integrity
  3. Access Control
  4. Non Repudiation
  5. Authentication

- Security Mechanisms
  1. Specific Security Mechanisms
     a. Encipherment
     b. Data Integrity Mechanisms
     c. Notarization
     d. Digital Signature
     e. Authentication Exchange
     f. Access Control Mechanisms
     g. Routing Control
     h. Traffic Padding
  2. Pervasive Security Mechanisms
     a. Trusted Functionality
     b. Security Label
     c. Event Detection
     d. Security Audit Trial
     e. Security Recovery

SECURITY ATTACKS:

Any action that compromises the security of the system.

CRYPTANALYTIC ATTACKS:

Attacks that involves cryptanalysis or attacks that are performed by cryptanalysts using cryptanalysis. These attacks focusses of finding the key to get the plain text. In case of hashing, other approaches are applied to get the plain text as hashing donot involve any key and is a one way function. Cryptanalytic attacks are categorized on the basis of information available to the cryptanalyst.

I. CIPHERTEXT ONLY ATTACK:

Ciphertext-only attacks occur when the attacker only has access to one or more encrypted messages but knows nothing about the plaintext data, the encryption algorithm or hashing algorithm being used or any data about the cryptographic key being used. This is the type of challenge that intelligence agencies often face when they have intercepted encrypted communications from an opponent.

This is the most difficult attack because in this attack there is only cipher text available to the cryptanalyst. Here the attacker uses 3 approaches to decrypt the ciphertext.

Bruteforce Attack - Cryptanalyst tries to decrypt the ciphertext with every possible key in the key domain until the plain text makes sense which is not a good option because if the key domain is large or especially the key size is large, it become difficult to perform these attacks and check every possible key. But as we know the attacker also not know anything about the encryption algorithm, so he has to try every possible key in the key domain on every encryption algorithm.

Statistical Attack - A better approach is statistical attack. In this attack, the attacker uses some inherent (Inherent means existing in someone or something as a permanent and inseparable element, quality, or attribute.) characteristics of the plaintext. For example “E” is the most frequently used letter in english language. So the attacker assigns the most frequently appearing character in the ciphertext as “E” and applies the same transformation logic to other alphabets and tries to decrypt the

message and find the key. To prevent from such attack, the ciphertext must hide characteristics of the language for example using compression we can do this.

Pattern Attack - Some ciphers create patterns in the cipher text. For example: In an html code everything is surrounded by a tag and when such a pattern is converted to ciphertext we get a similar pattern in the ciphertext. Cryptanalyst uses this pattern to break the cipher as they know an html code is always surrounded by an html tag. Once that tag is decrypted the whole code can be decrypted using the same logic.

II. KNOWN PLAINTEXT ATTACK:

In a known-plaintext attack, the attacker has access to both the data's encrypted form (ciphertext) and its corresponding plaintext copy of the data's original (unencrypted form). The attacker attempts to determine the encryption key or algorithm by examining the relationship between the plaintext and ciphertext. For example, if "HELLO" is encrypted as "XUZZA," knowing this pair could enable the attacker to decode other parts of the message that are also encrypted with the same substitution key. This demonstrates how, with some encryption algorithms, even a tiny amount of knowledge can result in broader decryption.

Attackers can obtain these pairs in various ways:

- Intercepting Communication: They might capture unencrypted data before it gets encrypted.
- Public Sources: Some plaintext and ciphertext pairs might be publicly available or leaked.
- Inside Knowledge: They could have access due to insider knowledge or compromised security.

III. CHOSEN CIPHERTEXT ATTACK:

In a chosen ciphertext attack, the cryptanalyst collects information by selecting a ciphertext and obtaining its decryption under an unknown key. The opponent can input known ciphertexts into the system, aiming to conclude the hidden secret key used for decryption.

IV. CHOSEN PLAINTEXT ATTACK:

In a chosen-plaintext attack, the attacker chooses plaintexts amd feeds them into the encryption system. The system then returns the corresponding ciphertexts with every different key. These pairs of plaintexts and ciphertexts are analyzed to find patterns or weaknesses in the encryption process. The steps involved in a chosen-plaintext attack typically include:

1. The attacker selects a set of plaintexts.
2. The chosen plaintexts are input into the encryption system, which is known to the attacker.
3. The system generates corresponding ciphertexts according to the key (Every time a new key is tried).
4. The attacker studies the relationship between the plaintexts and ciphertexts to discover patterns or guess the encryption key,

V. CHOSEN TEXT ATTACK:

Chosen Text Attack: This isn't a standard term in cryptography, but it might refer to a mix of chosen plain text and chosen cipher text attacks.

NON-CRYPTANALYTIC ATTACKS:

These attacks does not involve any cryptanalysis. These attacks threatens the 3 security goals i.e : The CIA.

I. PASSIVE ATTACKS:

Attacks that involves unauthorized reading or monitoring of transmissions. In simple words eavesdropping the conversation or messages. It involves attempts to learn or make use of the information from the system and these attacks does not affect system resources. The goal of passive attacks is to get information that is being transmitted without directly interacting with the target. These attacks does not involve any modification of data and are hard to detect. These attacks threatens the cofidentiality of the data.

TYPES OF PASSIVE ATTACKS:

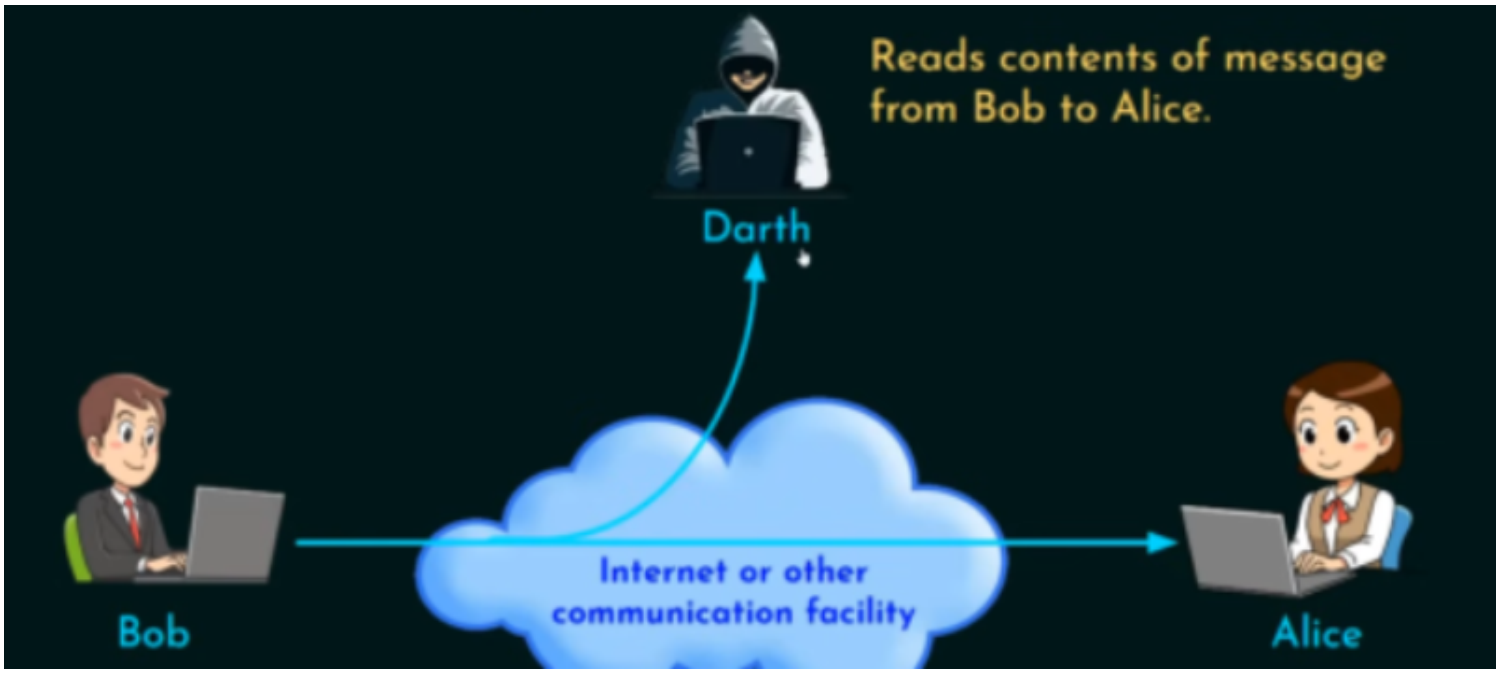
Passive attacks are threats to confidentility which are:

THREATS TO CONFIDENTIALITY:

- Snooping (Release of Message Contents)
- Traffic Analysis

SNOOPING:

The general meaning of snooping is to secretly sneak or peak into something. In cryptography, snooping means unauthorized access to data. For example: Someone sending data on the internet, since internet is public, attackers can get a copy of the message that we are sending to our intended receiver. Now, the attacker opens the message and see the contents of the message, thus compromising the confidentiality security goal. To prevent snooping, we must encipher (Encryption) our data using encipherment techniques i.e : The sender should encrypt the message before sending the message on the public channel so even if the attacker receives the copy of the message, attacker will not be able to read it contents. And the receiver will able to read its contents, since the receiver has the secret key to decrypt the message, thus preserving the confidentiality goal.



TRAFFIC ANALYSIS:

In this attack, attacker obtain information by monitoring online traffic.
It is performed as:
1. The sender sends the encrypted message to the receiver.
2. The attacker gets the encrypted copy of the message.
3. Then the receiver responds with a message to the sender.
4. Attacker also keeps the encrypted copy of the message send from receiver to sender.
5. He then analyze both the request response messages or more precisely request response pair to guess the secret key to obtain the plain text.

Also from traffic analysis, we can find the identity of the communicating host, or the location or the length of the message that is tranferred from sender to receiver. This information can be helpful in guessing the nature of the comunication based on the traffic.

To avoid traffic analysis, avoid using special characters like question mark as it may reveal that a question is asked. Secondly, use longer texts because shorter replies will make the ciphertext get prone to brute force attacks and the plain text might get guessed easily. Thirdly, use strong encyption algorithms, to make the attacker hard to guess the plain text.

II. ACTIVE ATTACKS:

These attacks involves the modification of data or creation of false data or insertion of false data in the real data. These attacks threatens the integrity and availability security goals and are easy to detect.

TYPES OF ACTIVE ATTACKS:

The types of active attacks are:

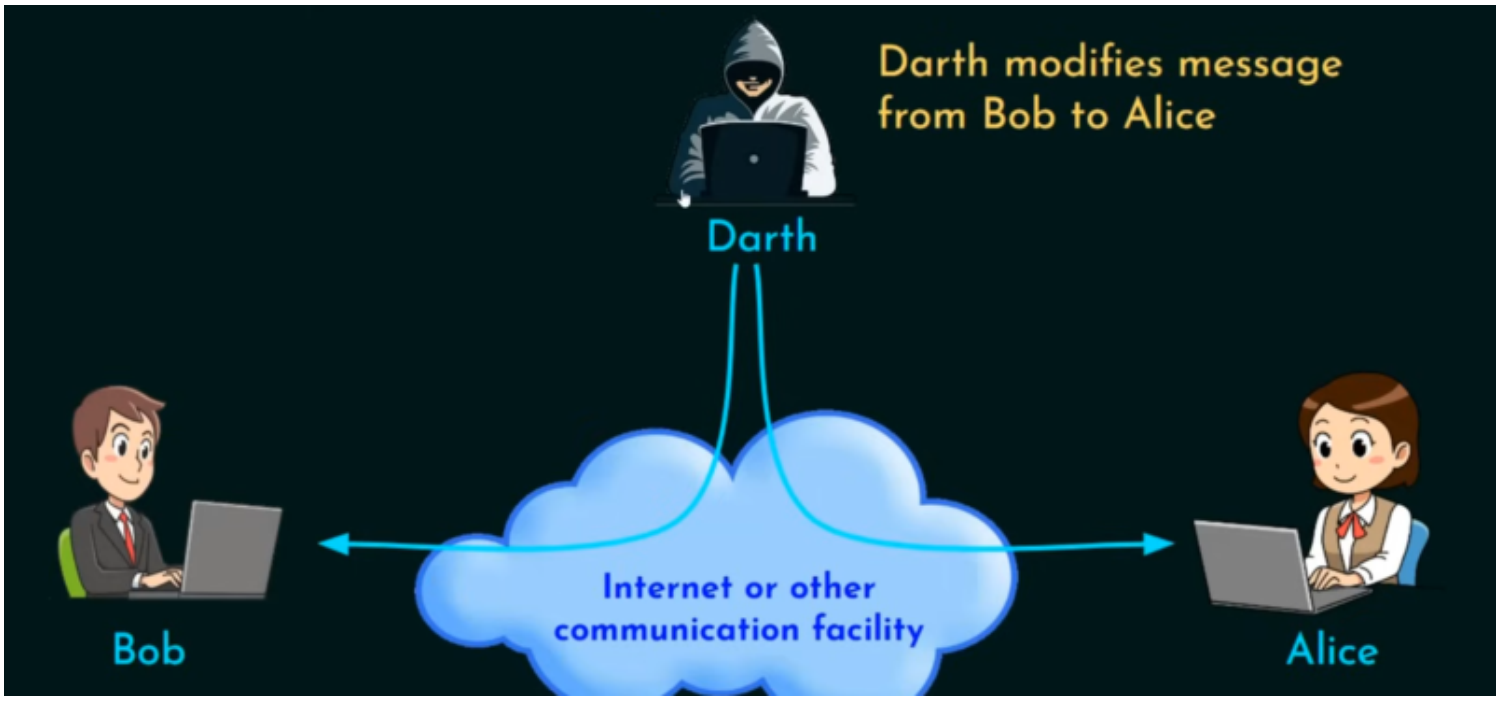
THREATS TO INTEGRITY:

Active attacks that threatens intergrity are:

- Masquerade
- Replay
- Modification
- Repudiation

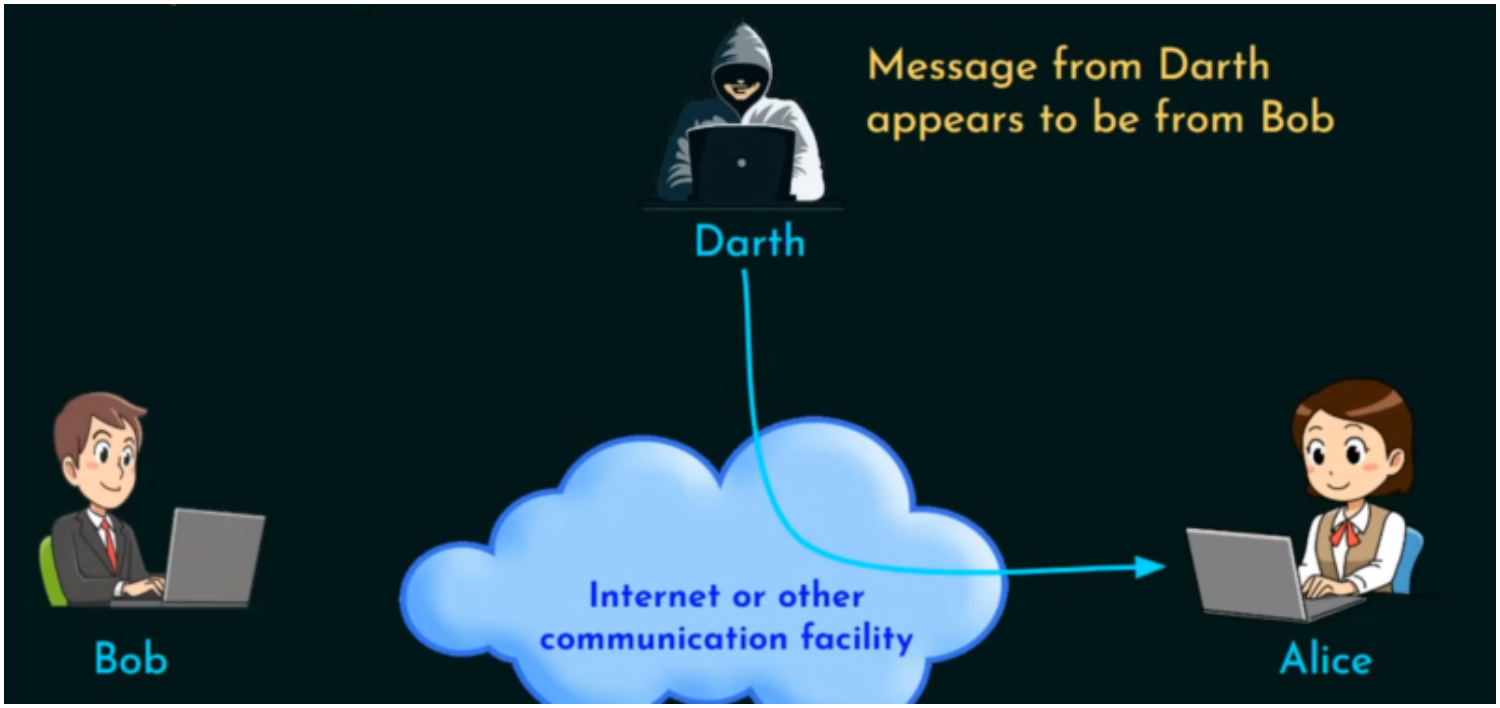
MODIFICATION:

In this attack attacker modifies the data. Inthis attack attacker aims to get benefits from modification. For example bob send message to alice to allow john to access confidential files but the message is modifed on its way to alice and alice receives the message to allow darth to access confidential files. In this way, darth will be able to access confidential files by modification of message.



MASQUERADING:

In this attack, the attacker pretends to be someone else. This attack is also known as spoofing. For example: Darth makes some connection with alice and pretends that he is bob and send message to alice that allow darth to access confidential files, or darth might gain some other benefits from this impersonation. Similarly, darth can also pretend to be alice. So bob sends the message to darth, who in this case is now pretending to be alice, which might contain some sensitive information like OTP or something like that. Second more realistic example would be that if someone stole the username and password of another person and use that credentials to login to second person's account. This process is called masquerading and the person who used the credentails of another person is called a masqeurader.



REPLAYING:

In this attack, the attacker replays the communication with the copy of the message. For example bob sends a message to alice. Darth also receives the copy of the message. Suppose the message from bob to alice was to unlock database for testing purposes. Now darth waits for some time and send the captured message to alice, alice thinks that the message is from bob because it might contain some source information, and darth can now take benefits from the unlocked DB.

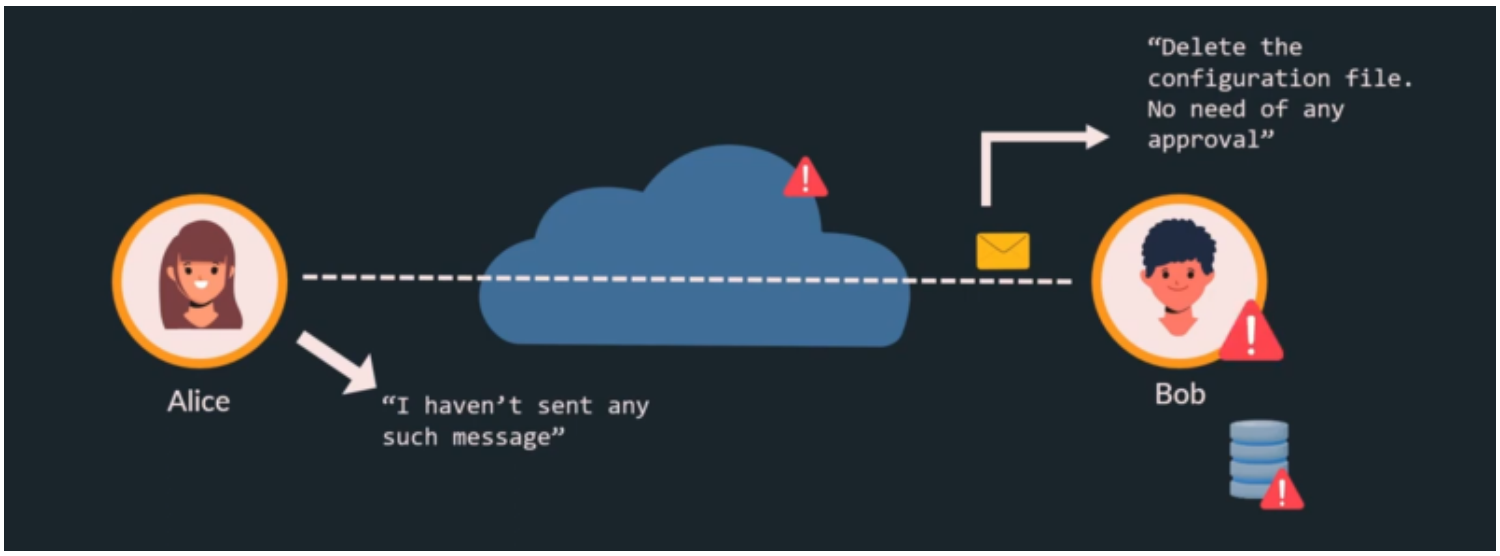
REPUDIATION:

This is different kind of attack, which is done by one of both the paties involved in the communication. It has 2 types.

TYPES OF REPUDIATION:

The 2 types of repudiation are:
- Denial from sender
- Denial form receiver

DENIAL FROM SENDER:



In this type of repudiation the sender denies their actions in case of any trouble. For example: Alice sends message to bob as shown in the above picture. In database, we have a configuration file which is also called config file in short. This file has all the configuration information of the DB so bob deletes this file as told by alice but after the deletion, the DB runs into an error and all blame goes to bob. When bob tells that alice said him to do this, alice denise by saying as shown in the picture. Now bob gets into trouble.

DENIAL FROM RECEIVER:

In this type of repudiation the receiver denies their actions in case of any trouble. For example: Alice send message to bob as shown in the above picture. Since the password is compromised, the DB can go under attack. For some reason, bob doesn't change the password and the information gets leaked which results in the big loss for the organization. Now the blame is on alice. Alice tells that she has send the message to bob regarding a password change. Bob denies this by saying as shown in the picture. Now alice is in
trouble.

THREAT TO AVAILABILITY:

Active attack that threatens availability is:

- Denial of service (DOS) attack

DOS ATTACK:

In this type of attack, the attaker sends many bogus requests to the server. It may slow down or totally interrupt the service of the server. For example, the attacker send many bogus, unwanted requests to the server. The server got crashed. Now a user sends a request to the server. Since the server is crashed, it is not able to provide the service to the user thus threatning the availability security goal, i.e: The user is denied from the service or the service is not available to the user due to server crash. DOS is done in a way that the server consider these requests are from different users.

SECURITY SERVICES:

Services that protect the system from security attacks. Security services answer the question what to implement to achieve the security goals. i.e CIA. Data confidentiality and authentication provide confidentiality security goal or helps to us achieve it, Data integrity and Non repudiation provides integrity security goal and the access control provide availability. However,

this is not a strict mapping, all the security services work mutually to achieve the security goals. The security services are:

DATA CONFIDENTIALITY:

The protection of data from unauthorized disclosure.

AUTHENTICATION:

Proving an identity of oneself. The best example of authentication is a fingerprint. Sice every person havs a different fingerprint, we can prove our identity. Now authentication service is provides authentication of the parties, that are the parties legit involved in the communication. It is the process of verifying the identity of a user or device in order to grant or deny access to a system or device. This can be done using basic password protection.

TYPES OF AUTHENTICATION:

Authentication is of 2 types namely :

Peer entity authentication
Data origin authentication

PEER ENTITY AUTHENTICATION:

This service provide authentication of both the sender and the receiver.

DATA ORIGIN AUTHENTICATION:

Here the service provide authentication of the origin only i.e : The sender.

DATA INTEGRITY SERVICE:

This service protects the data from modification, insertion, deletion and

replaying.

NON REPUDIATION:

This service protects against repudiation by either parties.

TYPES OF NON REPUDIATION:

Non repudiation is of 2 types:

PROOF OF DELIVERY:

Here sender of the data can prove that the data was delivered to the intended recipient.
Sender has a delivery proof that I have send the data.

PROOF OF ORIGIN:

Here the receiver of the data can prove the identity of the sender if denied.

ACCESS CONTROL:

In an organization, various levels of employees have various levels of access to the system. For example, in a company, a software engineer has limited access to the system as compared to the product manager and the product manager has limited access as compared to the CTO of the company. It also prevents from DOS attacks. For example, a server is configured in such a way that it can only accept requests from authenticated users, non authenticated users have no access to the server, neither it will accept any request from unauthenticated user so in case if a person tries to perform DOS attack, the attacker being non authenticated user, the server will drop his packets thus providing availability security goal.

SECURITY MECHANISMS:

A process that is designed to detect, prevent or recover from security attack. Security Mechanisms answer the question how to implement the security services which will help us achieve the security goals. Security Mechanisms can be pervasive or specific.

SPECIFIC SECURITY MECHANISMS:

These are security measures used to protect specific parts of a system or data. Specific mechanisms focus on specific vulnerabilities. The specific security mechanisms are

1. ENCIPHERMENT:

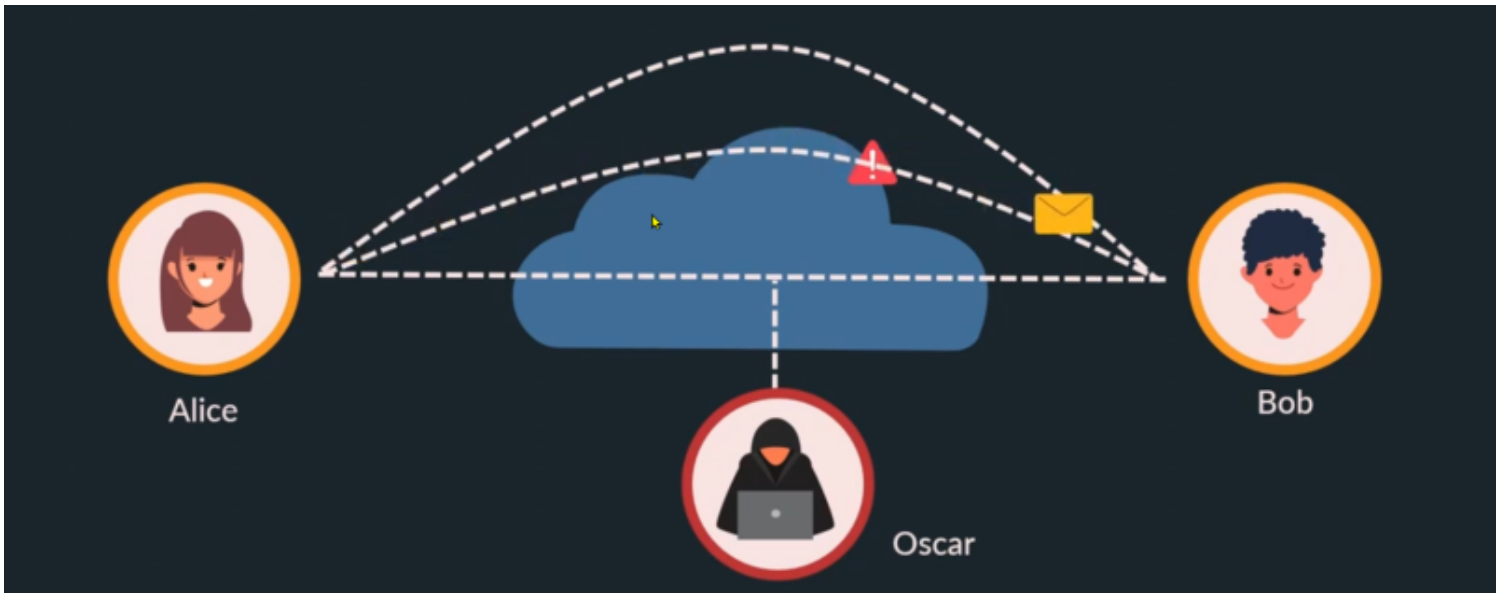
One of the most popular security mechanisms is encryption. It involves 2 things i.e the key and the encryption algorithm/decryption algorithm. The message/data sent from the sender to the receiver is usually is not understandable so that even if the message is stolen, cannot be decrypted easily by the attacker. Some of the popular encryption algorithms are AES, RSA, Triple DES, etc.

2. TRAFFIC PADDING:

In traffic padding, we insert some bogus data into the data traffic. First the "cryptography is cool" to its encrypted form, then we remove the spaces and add dummy data before and after the encrypted text which has not any regular order. So it will confuse the attacker which blocks are of the dummy data and which one is actual data.

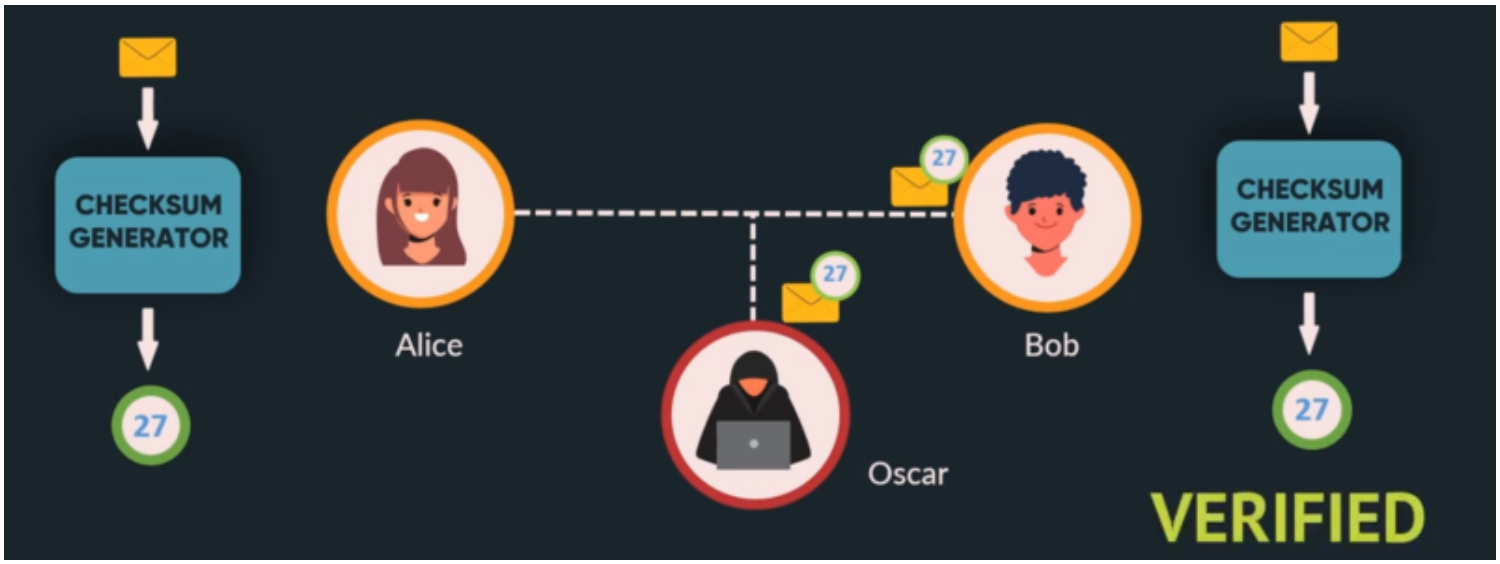
3. ROUTING CONTROL:

In routing control, sender and receiver continuously change the paths of communication to avoid the use of the path on which the attacker is eavesdropping or might be eavesdropping or to confuse the attacker which data is sent on which path thus preserving confidentiality so that to give the attacker a hard time to find the desired data.

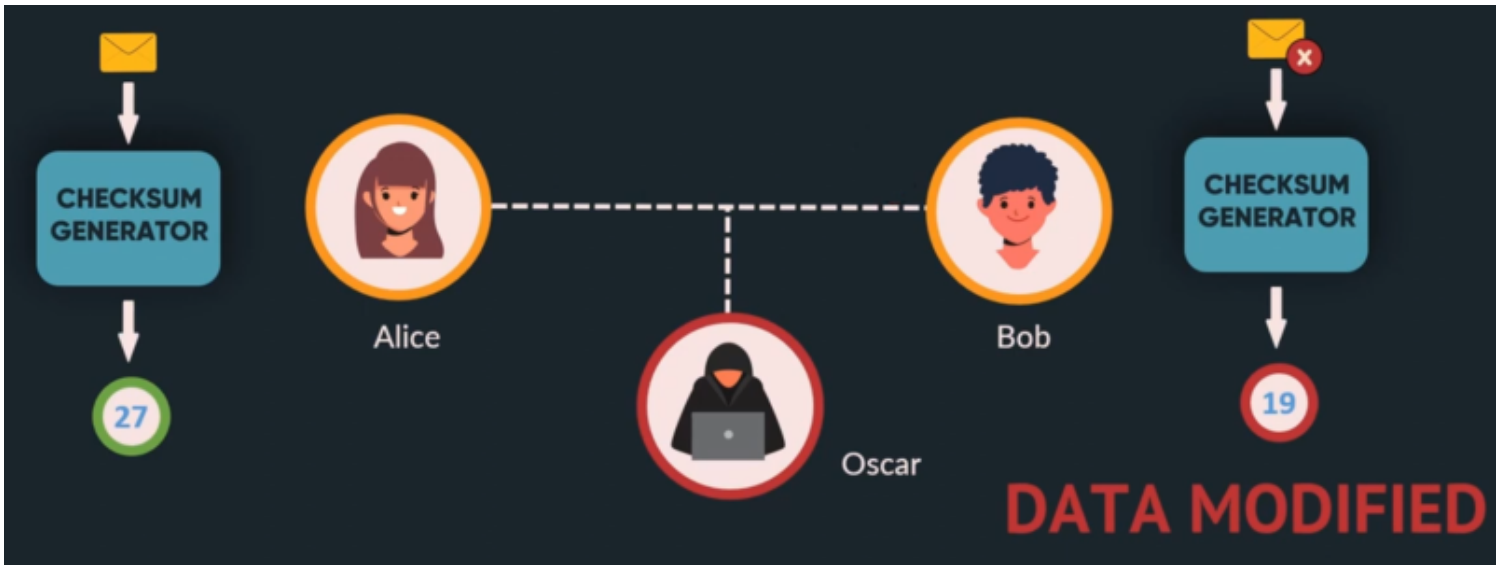


4. DATA INTEGRITY:

In data integrity, a checksum value is generated using a specific process from the data itself. It ensures integrity.



☐ Here alice generated a checksum value from the data using a checksum generator.
☐ She then attaches the checksum value with the data and sends it to bob.
☐ Bob also pass the data from checksum genrator and gets the checksum value.
☐ Now he compares the checksum value attached with the data send by alice and his own calculated checksum value.
☐ If both the values match, it means the data is not modified.



Suppose, on the way to bob, oscar modified the data and bob received the data.

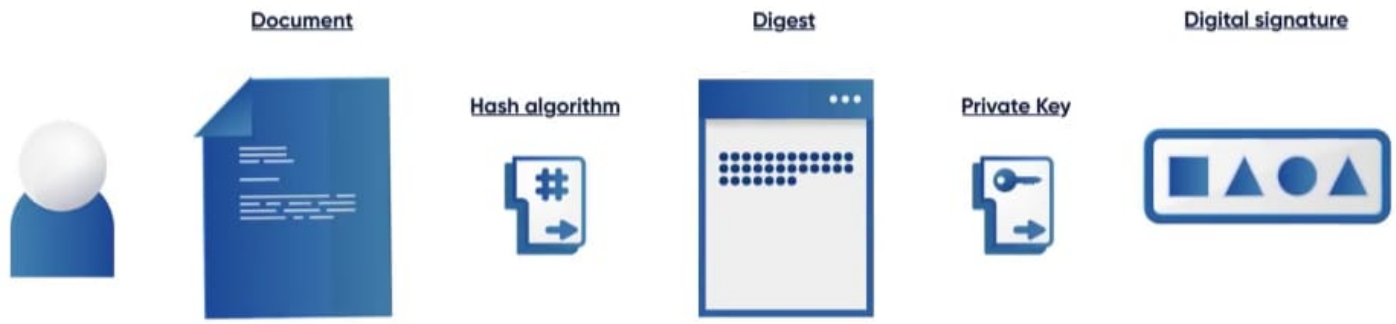
He calculates the checksum which was 19, but the checksum calculated by alice attached with the data is 27.
So these both don't match which means the data is modified and bob drops the data packet.

5. DIGITAL SIGNATURE:

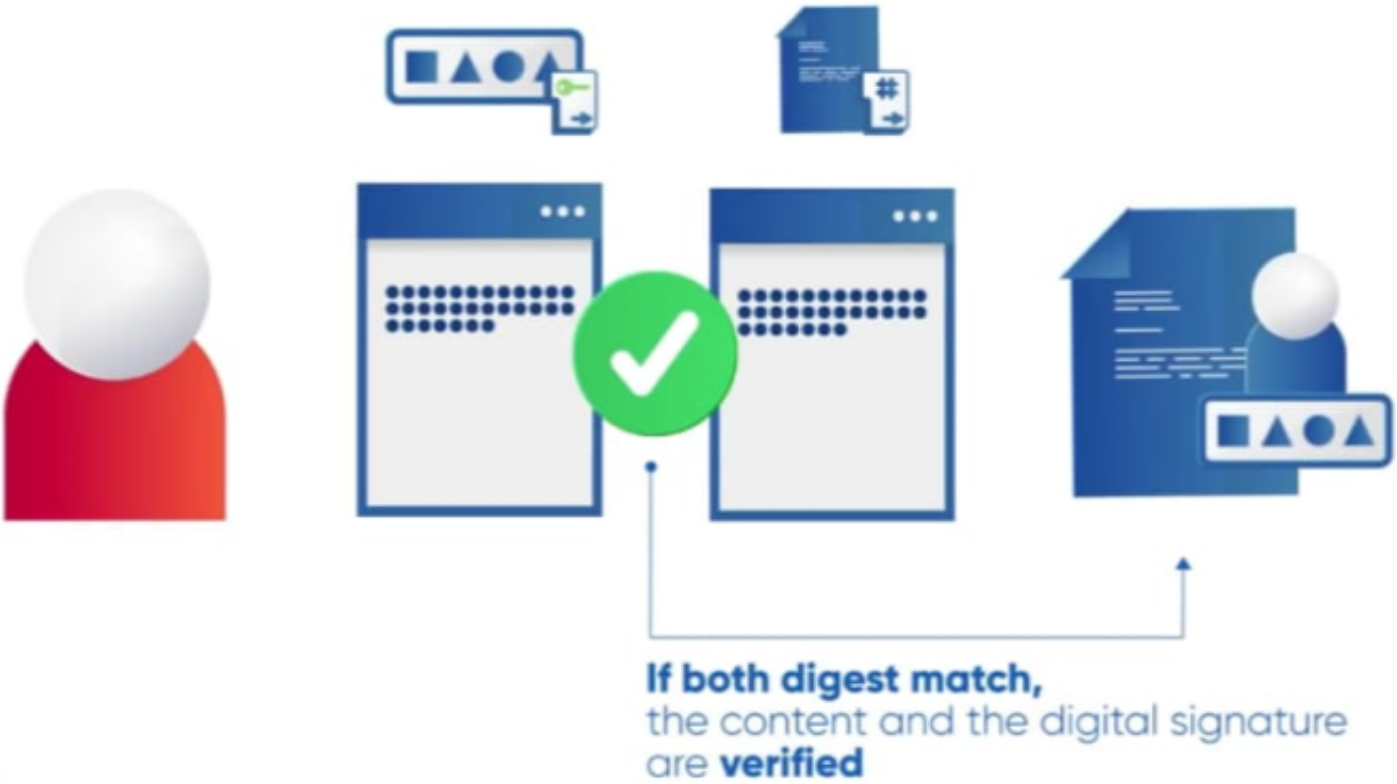
A digital signature is the combination of the document and the sender's private key. It works as follows.

☐ In digital signature, a copy of the message or the document we want to send to the receiver is passed throught a hashing algorithm. The output of this process is called a hashed file or digest.
☐ Then this hashed document is encrypted by taking this hashed document as an input plus the private key of the sender.
☐ The output of this encryption step will be the digital signature.
☐ Sender attaches this digital signature to the actual document and sends it to receiver.
☐ The receiver first decrypt the digital signature using the public key of the sender to get the hashed form of the document.
☐ He then passes the copy of the actual document from the hashing algorithm from which the sender passed the document to get a digest.
☐ He then compares this digest and the decrypted digital signature which is also a digest.
☐ If both digests match, it means the receiver received the message without any modification thus ensuring integrity.

- ON SENDER SIDE :



- ON RECEIVER SIDE:



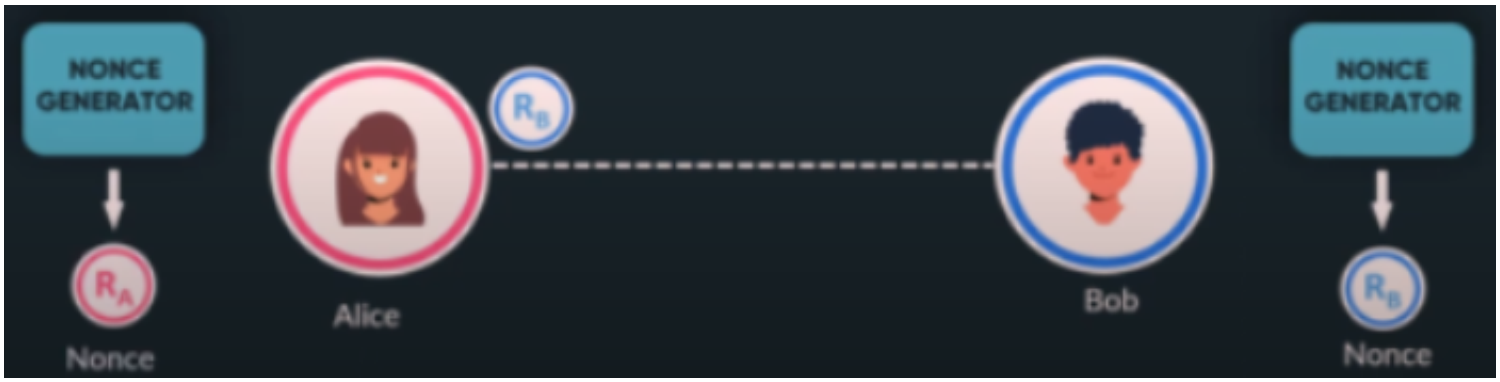
6. AUTHENTICATION EXCHANGE:

In authentication exchange entities exchange some messages to prove their identity. Authentication Exchange works as:

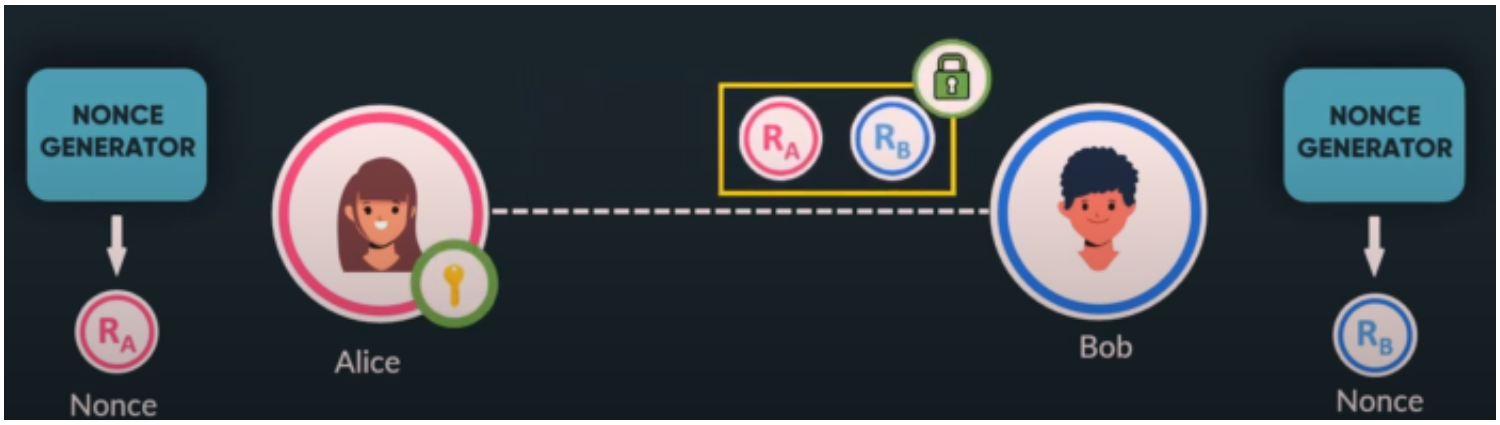
Alice first gives her address to bob.

After receiving alice's address bob generates a nonce (nonce is a time varying random number that is used only once)
So bob uses a nonce generator to generate a one-time nonce now bob sends this nonce to alice.

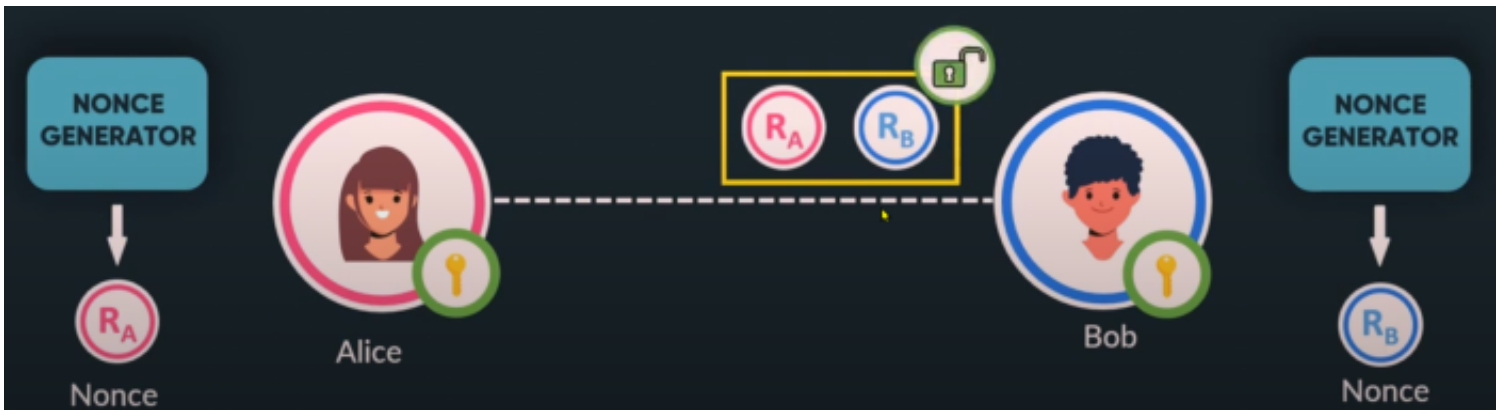
After receiving bob's nonce alice generates her own nonce



Now alice prepends her nonce after bob's nonce and using her secret key encrypts the message and send it to bob.

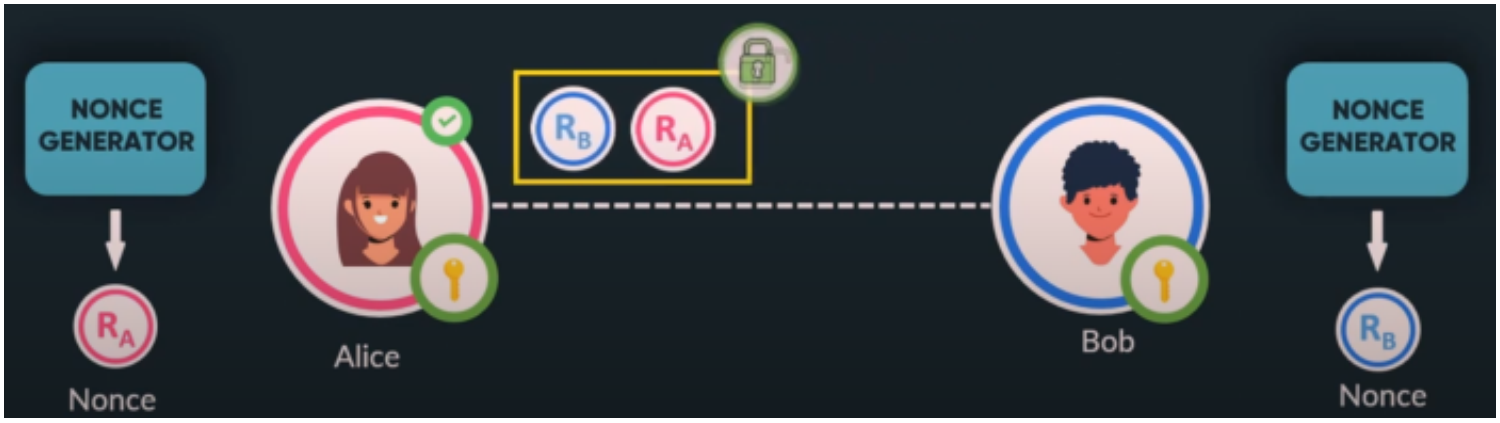


Now bob uses his secret key to decrypt the message.

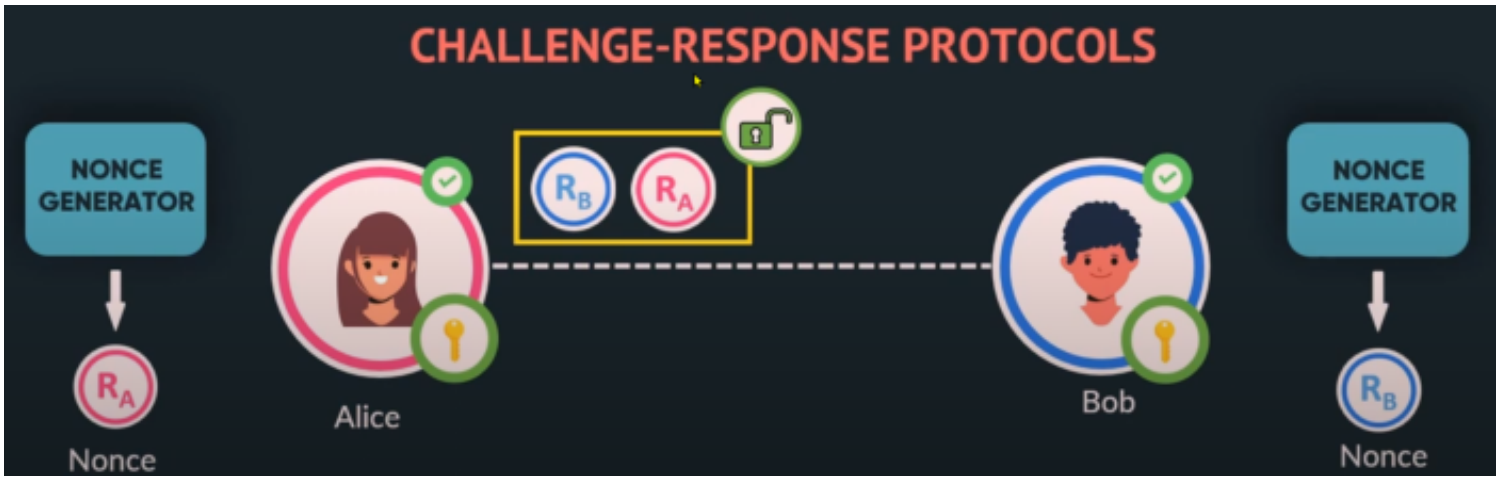


Since bob received his own nonce which he had sent, alice is now authenticated.
Now bob shuffles the messages and prepends alice's nonce after his nonce

and sends it to alice.



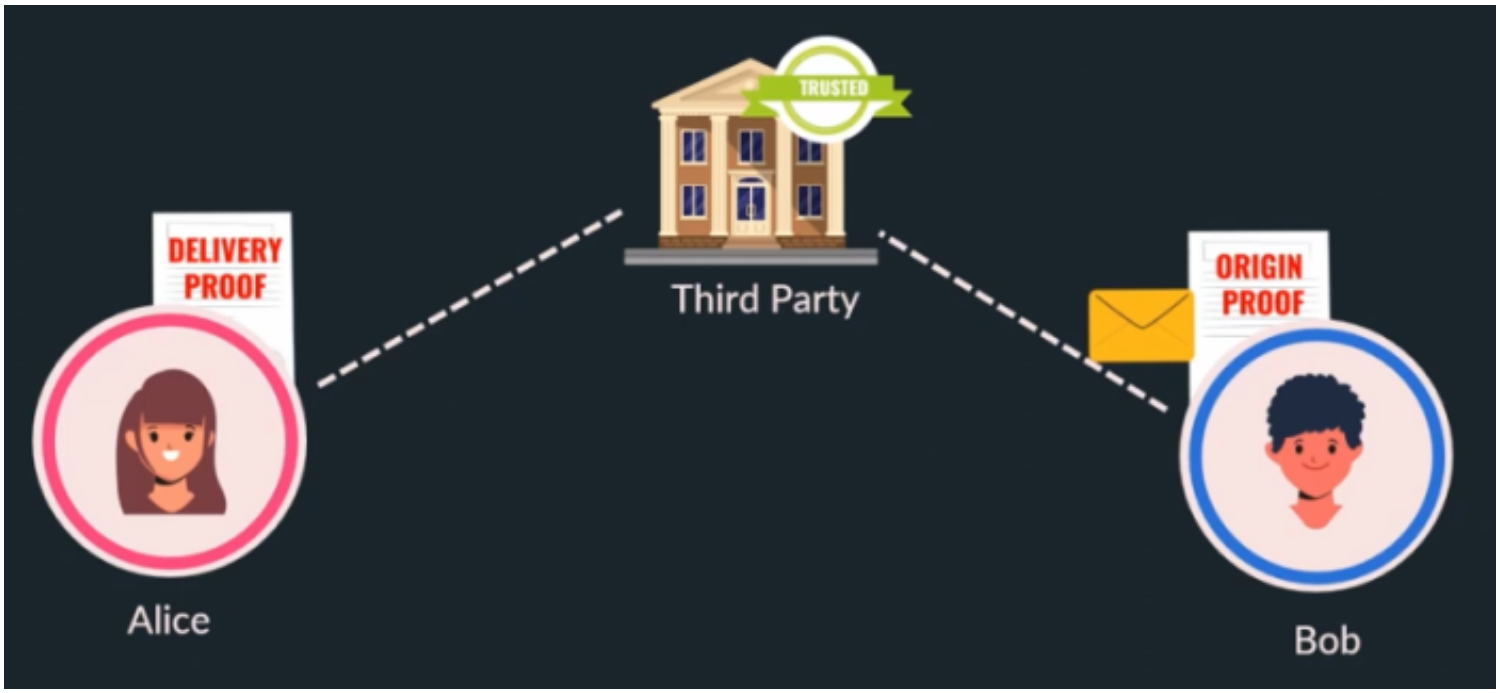
Alice decrypts it and verifies the nonce with this bob is also authenticated so we can see that by exchanging some messages alice and bob have authenticated each other such kind of systems are called challenge response protocols.



7. NOTARIZATION:

In notarization we select a trusted third party to control communication between two parties. Let's call our alice bob example back to understand it better here we have a trusted third party which acts as a mediator between alice and bob so whenever alice wants to send a message to bob, she sends a message to the third party and the third party forwards the message to bob once the message is delivered, the third party generates a delivery proof of the message and sends it to alice. Similarly it generates

an origin proof for bob since both alice and bob have their respective proofs. In the future neither of them can deny sending or receiving the messages hence notarization avoids repudiation security attack.



8. ACCESS CONTROL MECHANISMS:

In access control we enforce access rights to resources. let's call alice bob example back, so here bob has a server that receives messages. So here in the access control mechanism we can use any authentication system such as passwords or pin to authenticate the user and then provide access to the authenticated user. So alice sends her credentials to the server to authenticate her once her credentials are validated, the server provides access to her. Since alice has the access she can now send messages to the server so we can see that the server allows only messages from authenticated entities thus avoiding dos attacks.

PERVASIVE SECURITY MECHANISMS:

These are overall security measures that apply to the entire system, not just specific parts. It is the overall protection. Pervasive mechanisms provide overall protection.

1. TRUSTED FUNCTIONALITY:

Trusted functionality ensures that a system or device works correctly and follows security rules. For example: Your smartphone's fingerprint scanner only unlocks for your fingerprint, keeping your data safe.

2. SECURITY LABEL:

A security label is a tag or marker that shows the security level of information or a resource that how much is the information sensitive or private. For example: Classifying documents as "Public," "Confidential," or "Top Secret" helps ensure they're handled properly.

3. EVENT DETECTION:

Event detection identifies potential security threats or incidents. For example: Anti-virus software detects malware on your computer, alerting you to take action.

4. SECURITY AUDIT TRIAL:

A security audit trail collects data to investigate security incidents or what happens for review. In the term "security audit trail," "audit" and "trail" have different meanings:

Audit: This refers to a careful check or review of how things are done. In a security context, it means examining systems to ensure they are safe and working properly.

Trail: This refers to a record or path of actions that have taken place. In this case, it’s a log that shows what has happened in the system, like who accessed it and what they did.

So, a "security audit trail" is a record that helps check and ensure the security of a system by showing all the actions taken within it. For example: Website login history helps find unauthorized access attempts.

5. SECURITY RECOVERY:

Security recovery fixes issues caused by security breaches or failures. For example: Restoring your phone from a backup after a virus attack.