1) Digital signature

- Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.
- Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.
- Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

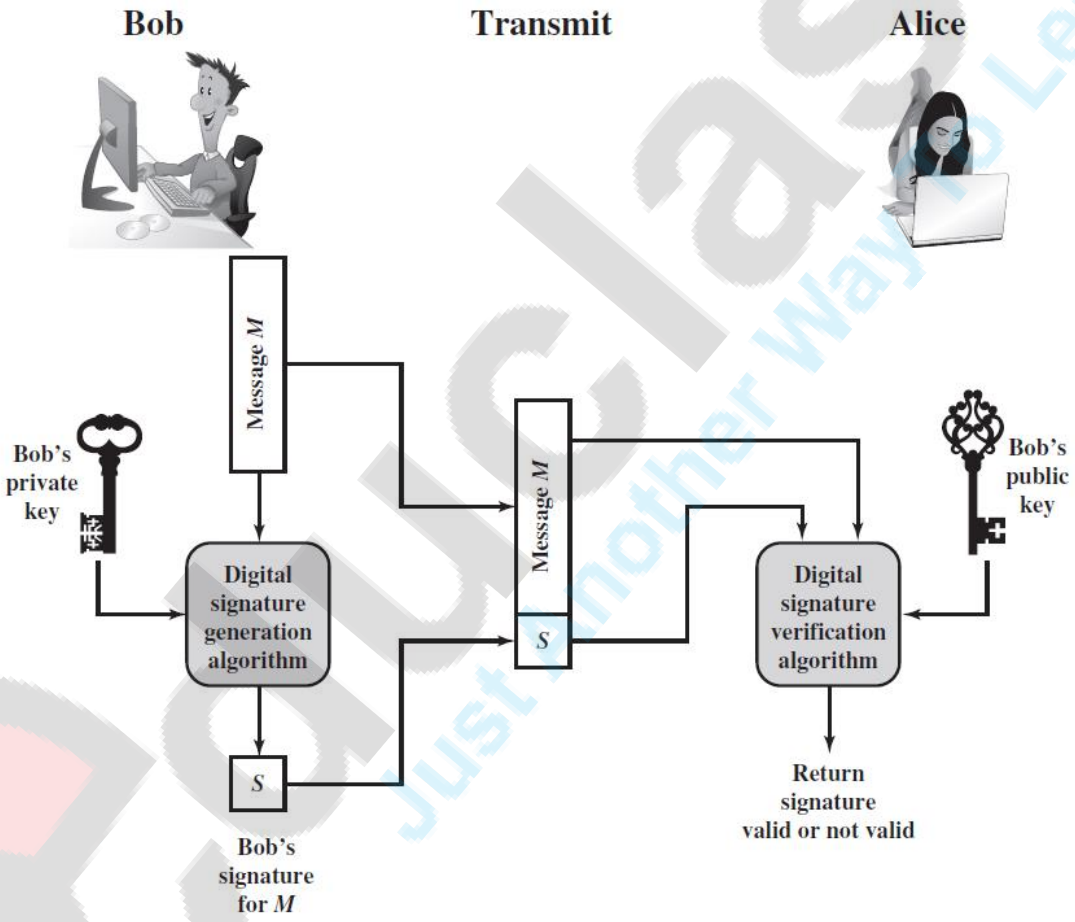


Figure 13.1 Generic Model of Digital Signature Process

The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.

- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

- Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.
- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.
- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

2)What is network security? Discuss various principle of network security.

A)What is network security?

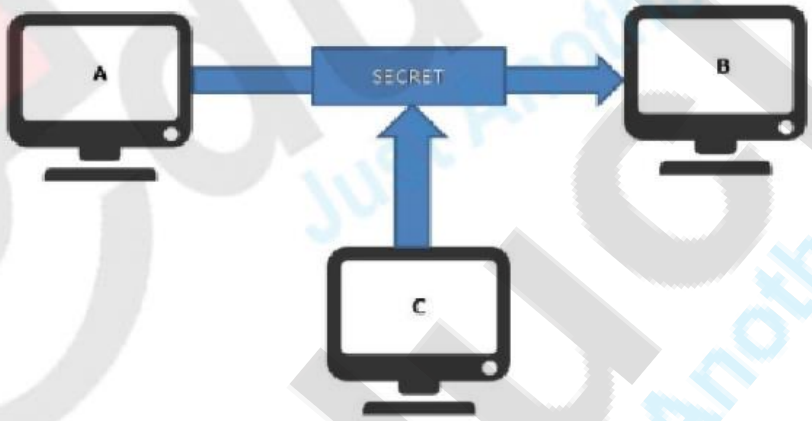
Network security is protection of the access to files and directories in a computer **network** against hacking, misuse and unauthorized changes to the system.

The authorization of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals.

B) services provided by the network security or principles of security

1.CONFIDENTIALITY



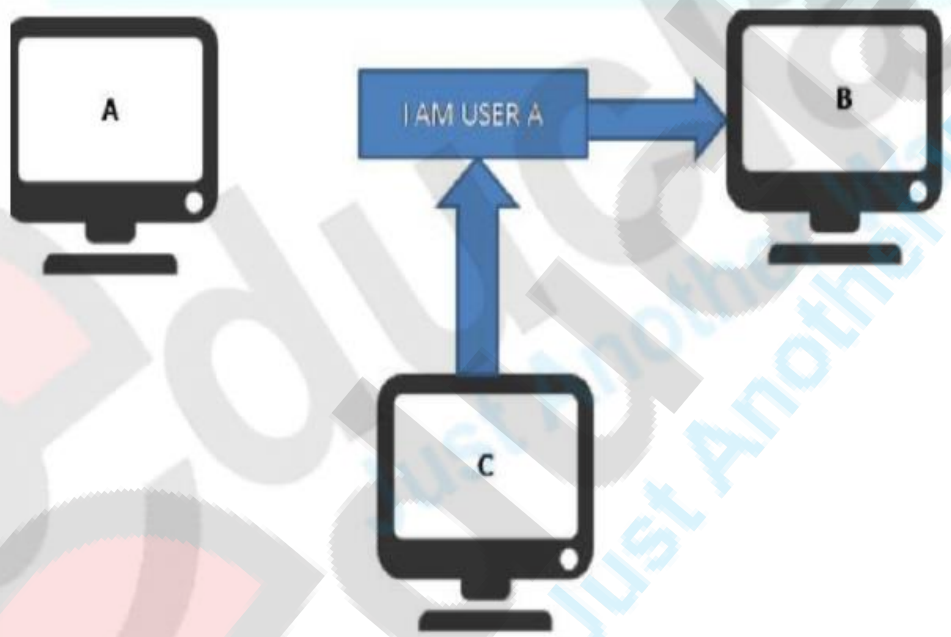
1. The principle of confidentiality specifies that only the sender and intended recipient should be able to access the content of a message.
2. Confidentiality gets compromised if an unauthorized person is able to access message.

3. An example of comprising the confidentiality of message is shown in figure. The user of computer A want to send message to user of computer B. another user C gets access to this message which is not intended to get this message then it defeat purpose of confidentiality.

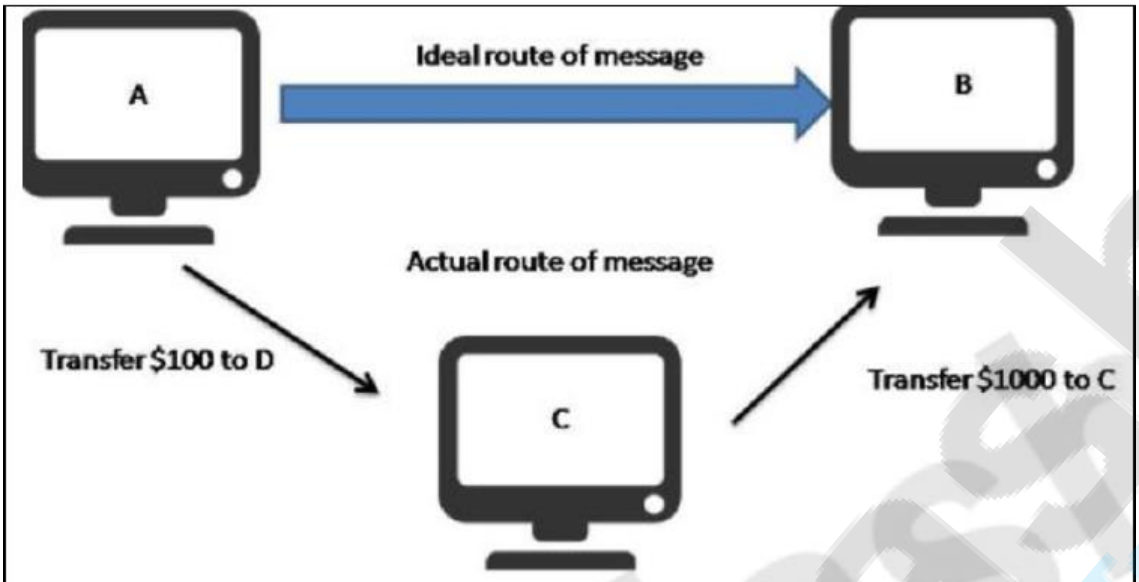
4. If confidential email sent by A to B is accessed by C without permission from A or B then this type of attack is known as interception.

2.AUTHENTICATION

1. Authentication mechanism helps to establish proof of identity.
2. This process ensures that origin of an electronic document or message is correctly identified.
3. If user C posed as user A and sent message to user B then how would user B will come to know that this message came from user C not from user A.
4. If user C posed as user A and sent request of fund transfer to user B then user B might will think that request came from user A and he might transfer funds to user A. This type of attack is known as fabrication.

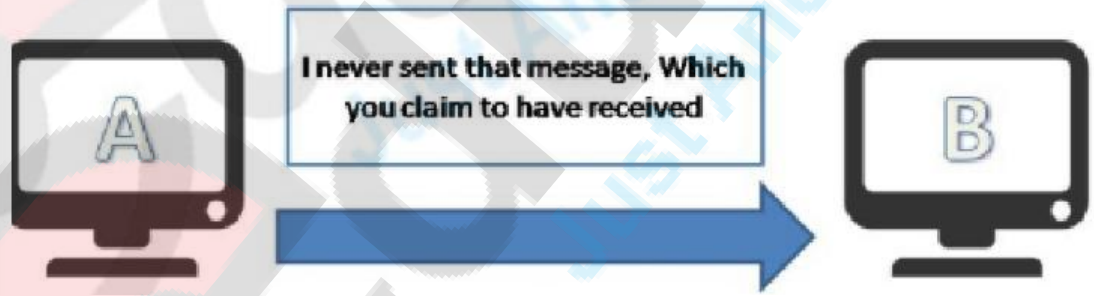


3.Intigrity



1. When content of message change after sending the message by sender but before receiver receive it then we can say that integrity of message is lost.
2. For example if user A sent message to user B but somehow user C managed to access that message and change content of message. User B have no way to knowing that message is tampered after user A sent that message. User A also does not know that message is tampered.
3. This type of attacks is known as modification

4.NON-REPUDIATION



5.ACCESS CONTROL

The principle of acssec control determines who shold be able to acessce what.

For instance we should be able to specify that user A can view the records in a database but cannot update them. However user B might be allowed to make upadates as well .

An acesse control is broadly realated to two areas

1.role management

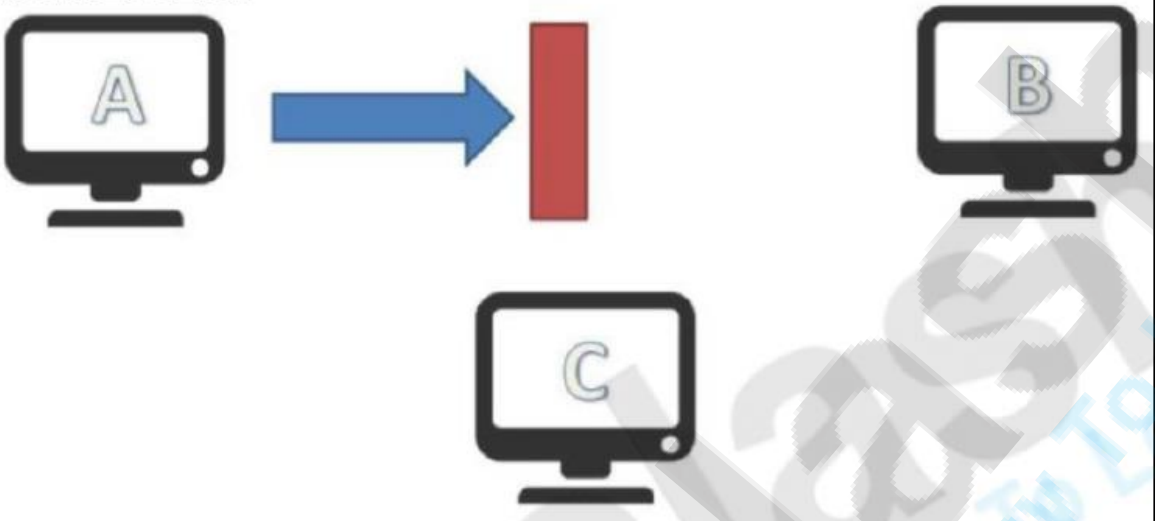
Role management concentrated on user side

2. rule management

rule management focuses on recourse side.

Based on this decisions taken here an access control matrix is prepared, which lists the users against a list of items they can access . an acess conrol list is a subset of an access control matrix.
Acess control specifies and controls **who** can access **what** .

6.AVAILABILITY

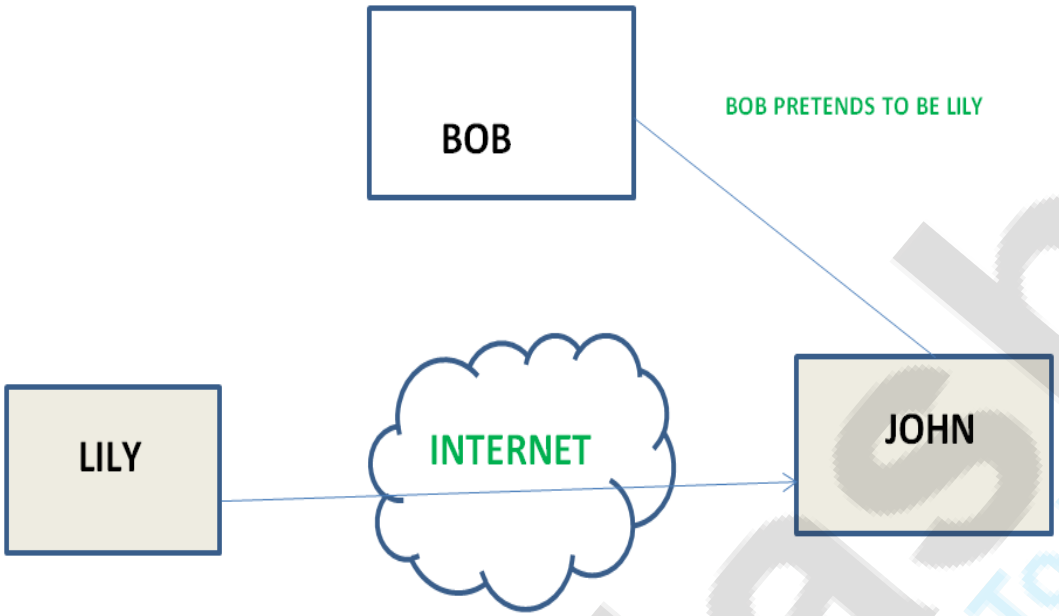


1. The principle of availability states that information should be available to authorized user at all the time.
2. Example :- due to intentional action of unauthorized user C, an authorized user A may not be able to contract a server computer B, as shown in diagram.
3. This would defeat the principle of availability. Such attack are known as **interruption.**

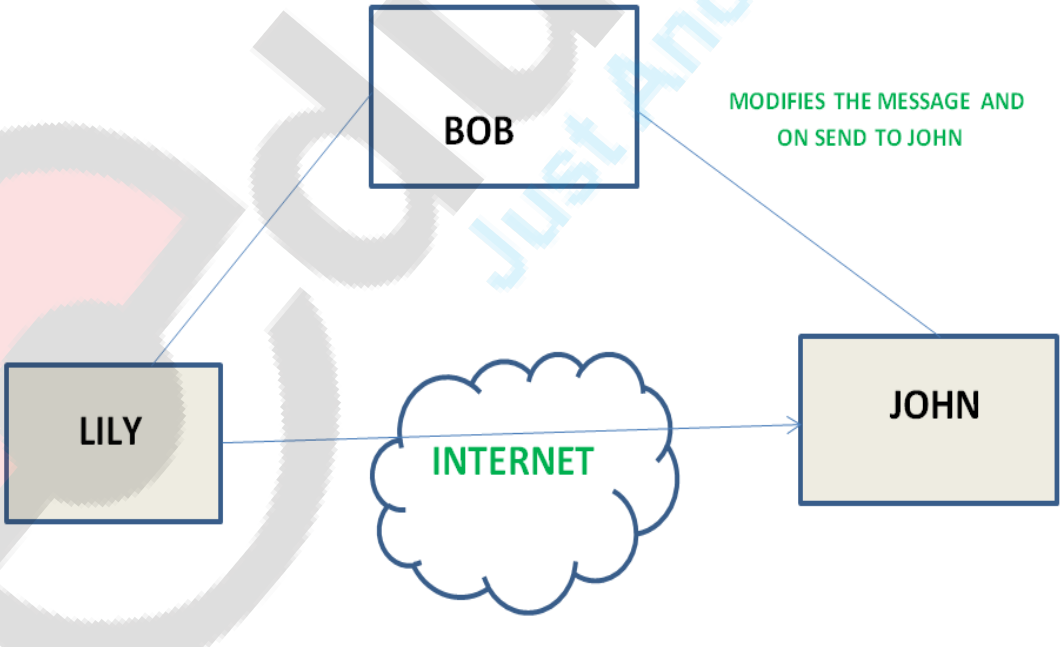
3)Security attacks & it's types

Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

1. **Masquerade –**
   Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



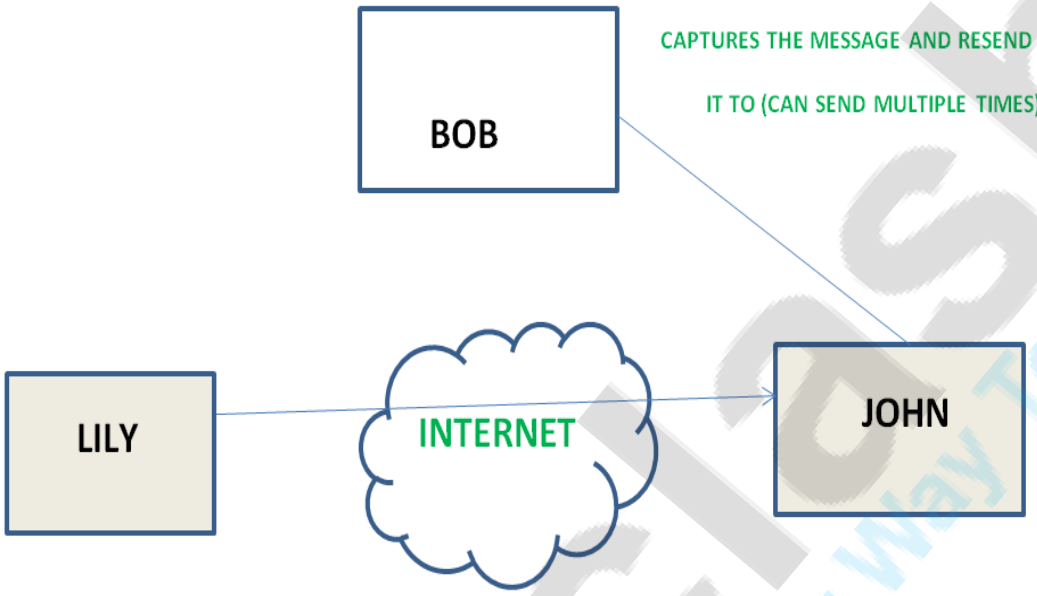
2. **Modification of messages –**
   It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



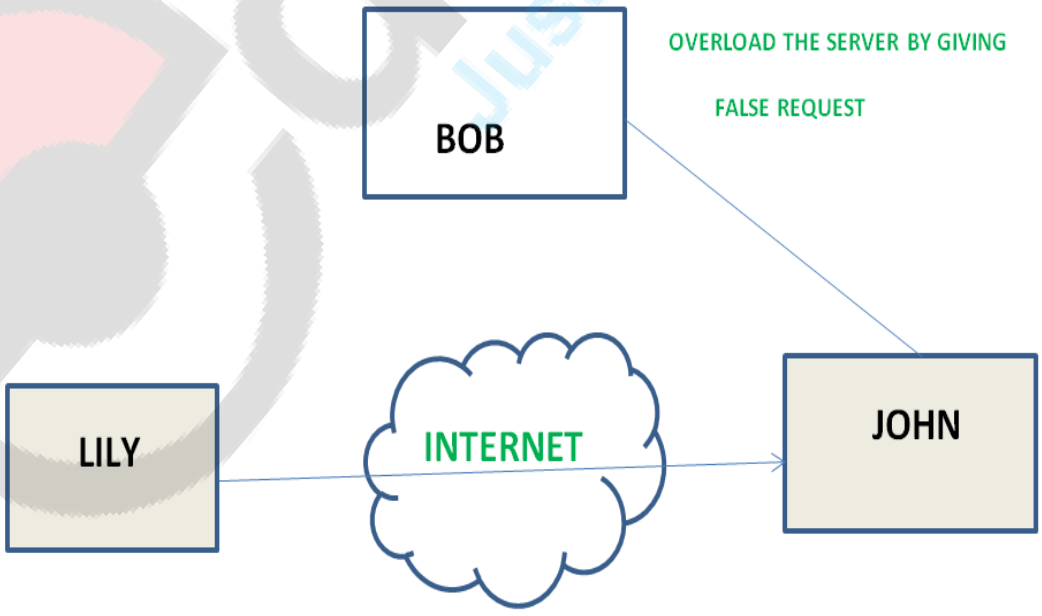
3. **Repudiation –**
   This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank "To

transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.

4. **Replay –**
   It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.

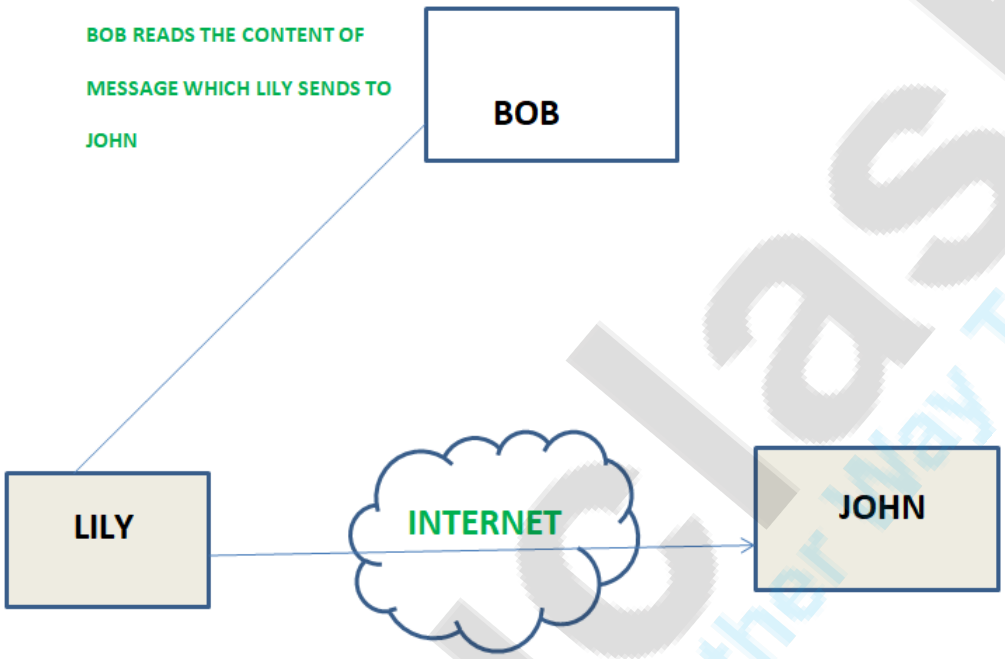


5. **Denial of Service –**
   It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content –**
   Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



2. **Traffic analysis –**
   Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.