Unit 1

(Q) Principles of Security

Key principles of security include

1) Confidentiality
2) Authentication
3) Integrity
4) Non repudiation
5) Access control
6) Availability.

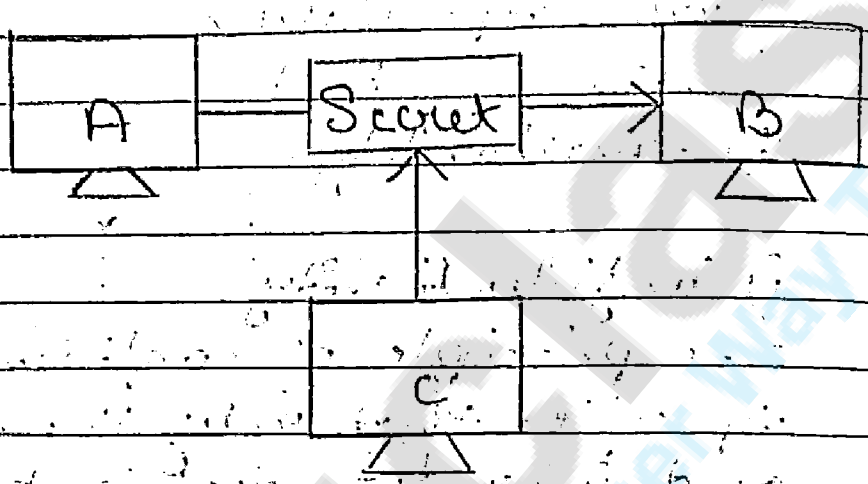
1) Confidentiality

The principle of confidentiality specifies that only the sender and intended recipient should be able to access the control of a message.

Confidentiality gets compromised if an unauthorized person is able to access message.

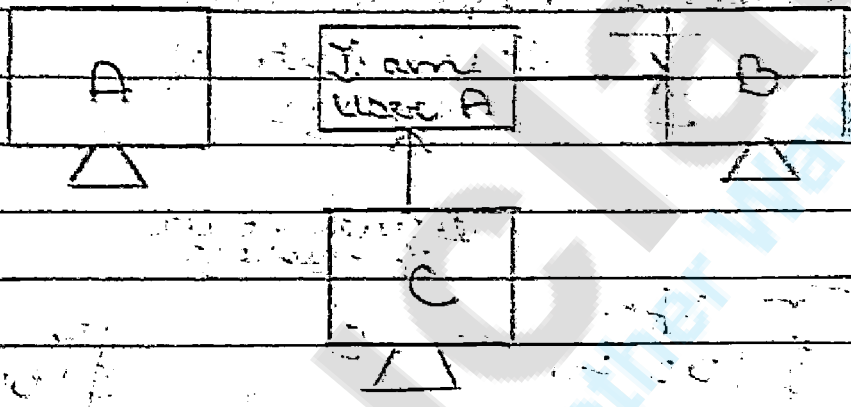
An example of compensing the confidentiality of message is shown in diagram. The user of computer A want to send message to user of computer B. Another user C gets access to this message which is not intended to get this message then it defeat purpose of

confidentiality.
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
Authentication mechanism helps to establish proof of identity.
This process ensures that origin of an electronic document or message is correctly identified.
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.

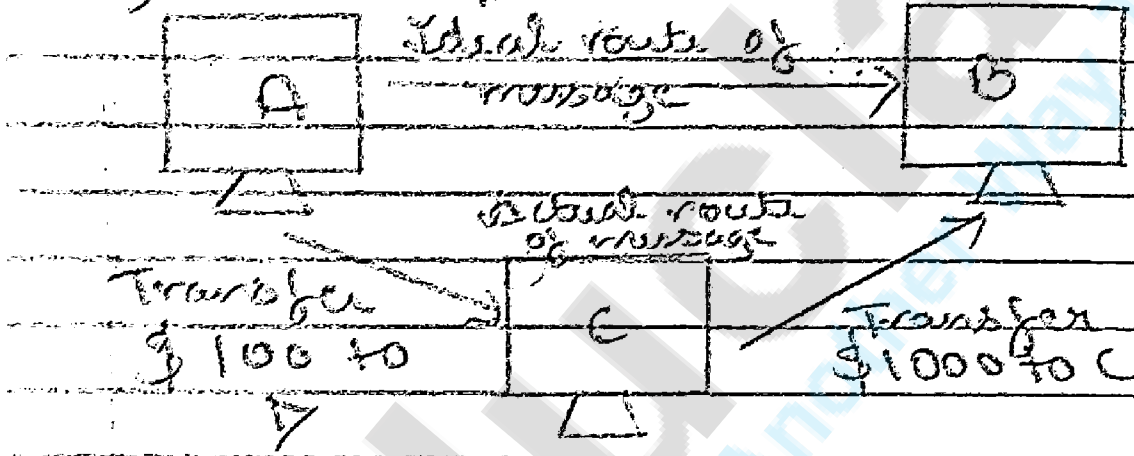
If user C posed as user A and sent request of fund transfer to user B then user B might will think that request came from user A and he might transfer funds to user A. This type of attack is known as fabrication.

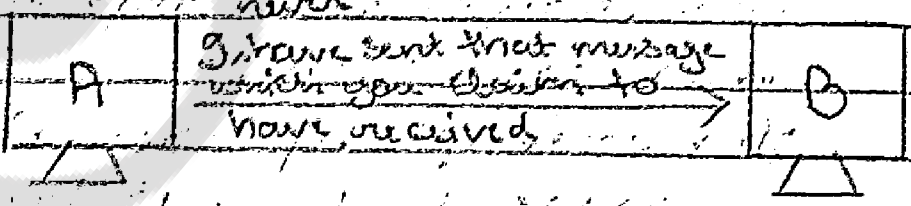


3) Integrity

When content of message change after sending the message by sender but before reciever recieve it, then we can say that integrity of message is lost.

for example if user A sent message to user B but somehow user C managed to access that message and change content of message.





5) Access control

The principle of access control

determines who should be able what for instance we should be able to specify user A can view the records in a database but cannot update them however user B might be allowed to make updates as well. An access control is broadly related to two areas

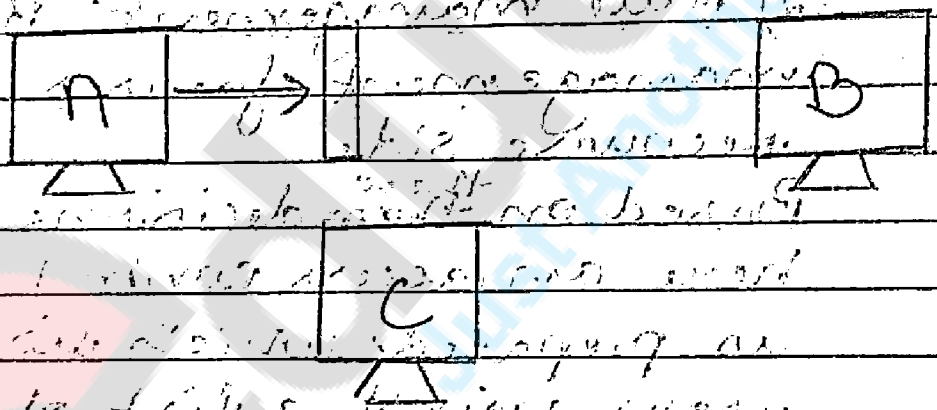
1) Role management: Role management is concentrated on user side

2) Rule management: Rule management focuses on resource side.

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

b) Availability

The principle of availability states that information should be available to authorized user at all the time.
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.
This would defeat the principle of availability. Such attack are known as 'interruption'.

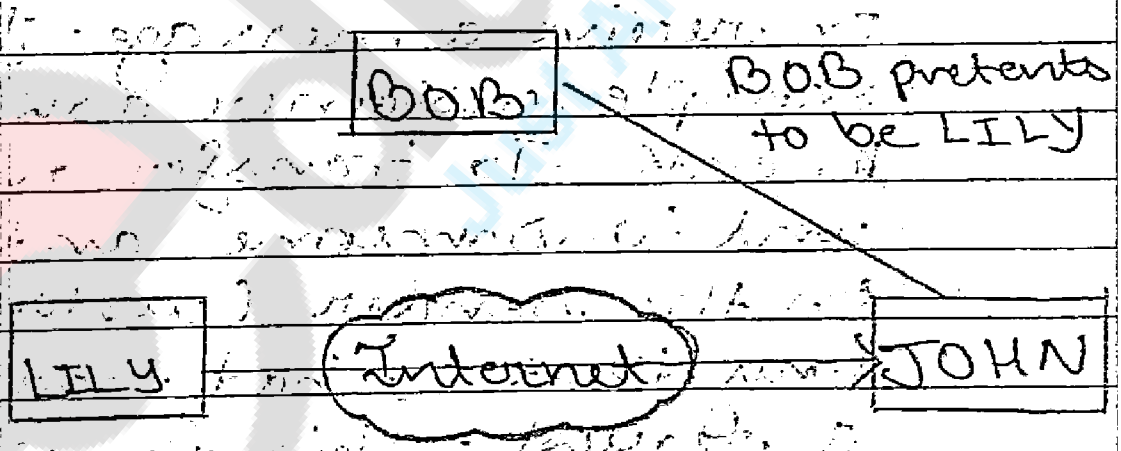


9) Attacks
Attacks are classified into two. They are 1) Active Attacks
2) Passive Attacks

1) Active Attacks: An Active

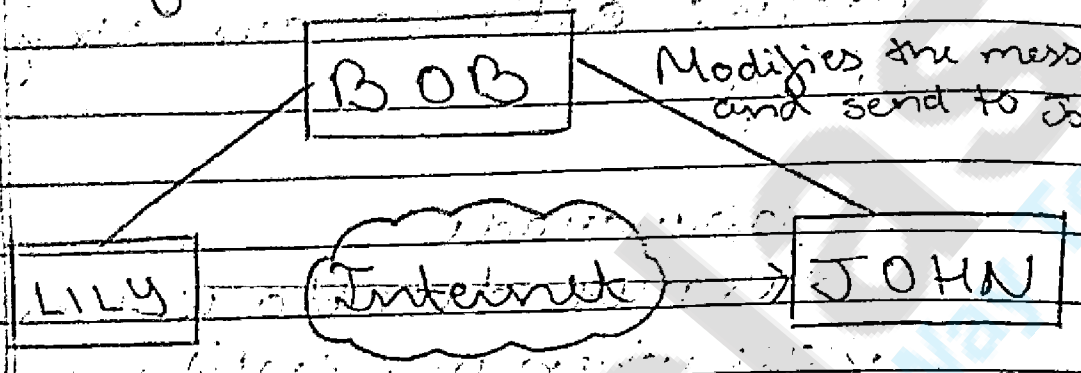
attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:-

1) Masquerade:-
Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other forms 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

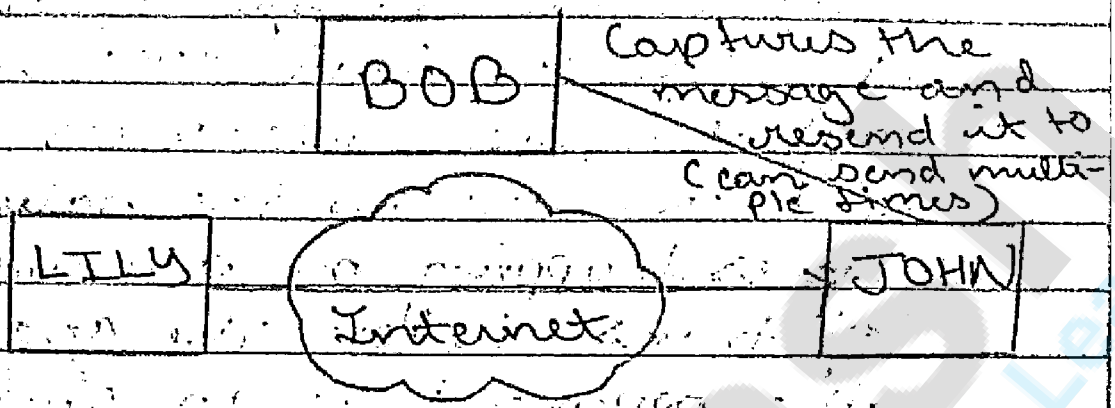
an unauthorised effect. For example, a message meaning "Allow JOHN to read confidential file X" is modified as "Allow Smith to read confidential file X".



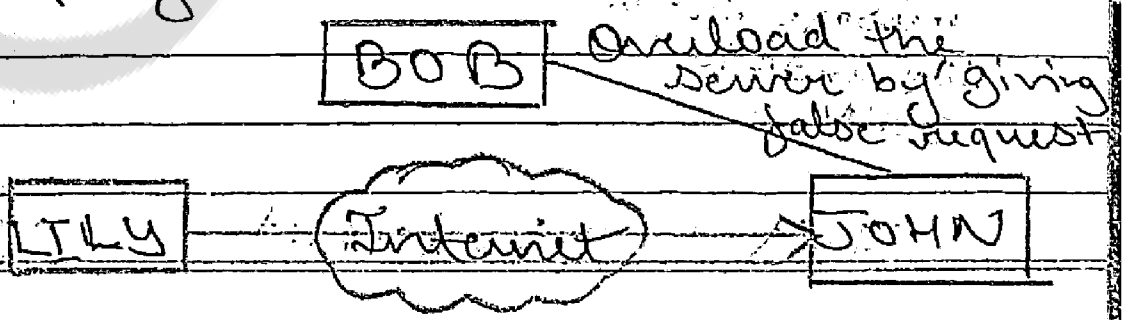
3) Repudiation:-
This attack is done by either sender or receiver. The sender or receive a message. For example, customer ask his bank "To transfer an amount to someone" and later on the sender (customer) deny that he had made such a request. This is repudiation.

4) Replay:-
It involves the passive capture of a message and its subsequent transmission to

produce an authorized effect.

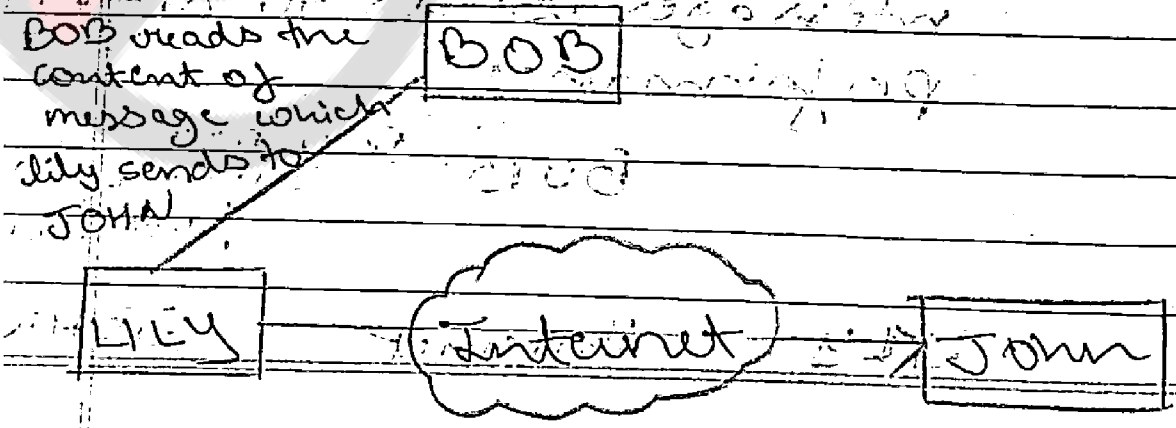


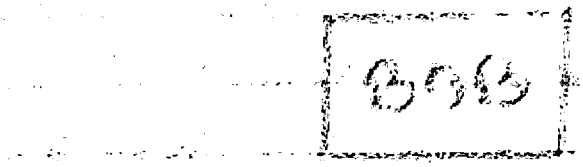
B) Denial of Service:
It prevents normal use of communication facilities. This attack may have a specific target: for example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network either by disabling the network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

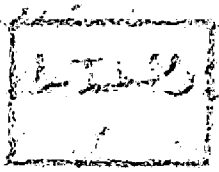


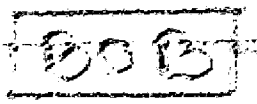
2) Passive attacks :- A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types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

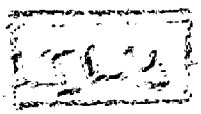
1) The release of message content- Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

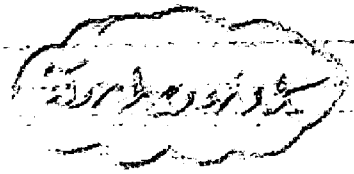


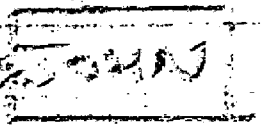






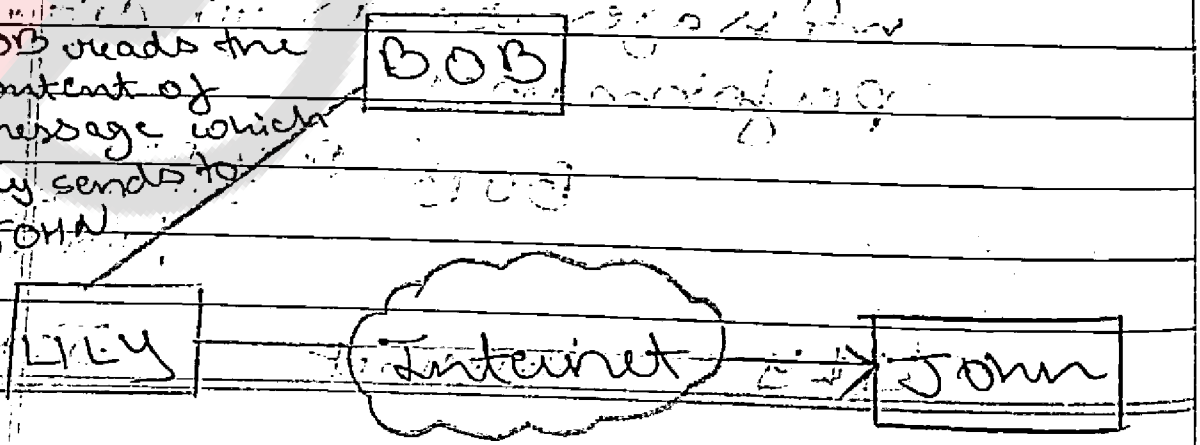






2) Passive attacks :- A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types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

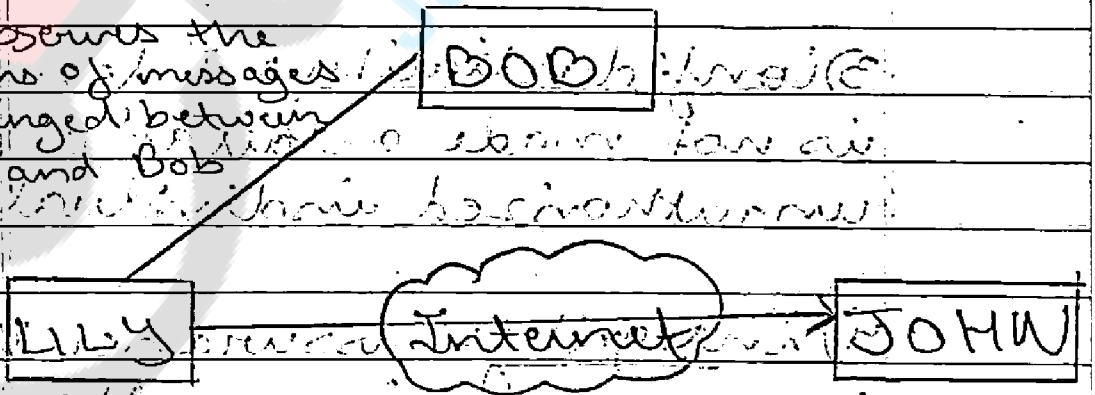
1) The release of message content- Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



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.



9) Services and Mechanisms

ITU-T provides some

security services and some mechanisms to implement these services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

Security services:-

1) Authentication: assures recipient ~~can have access~~ that the message is from the source that it claims to be from.

2) Access control:- controls who can have access to resource under what condition.

3) Confidentiality:- Information is not made available to unauthorized individual

4) Integrity:- assurance that the message is unaltered

5) Non-Repudiation:- protection against denial of sending

or receiving in the communication

Security Mechanisms

- Encipherment
- Data integrity
- Digital signature
- Security Mechanisms
  - Authentication exchange
  - Traffic padding
  - Routing control
  - Notarization
  - Access control

Relation between Security services and mechanisms

Security Service	Security Mechanism
Data confidentiality	Encipherment and routing control

Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity and notarization
Access control	Access control mechanisms

Q) Integrity check

Integrity checking is the process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes (and so it sometimes called change detection)

Generally the state information that gets used in the comparison is in the form of a hash of some kind and ideally the baseline state that the

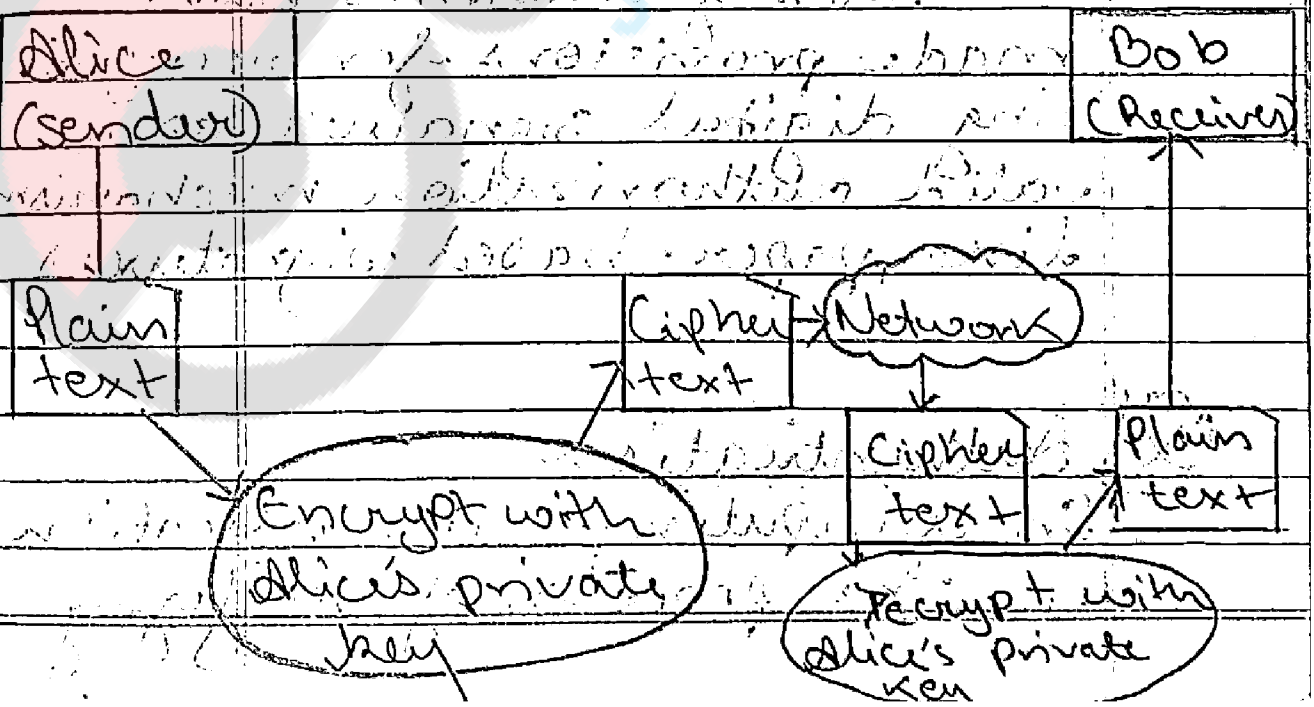
current state is compared to was generated when there was nothing wrong with the system.

The reasoning behind this technique is that for anything bad to happen on a system something on that system must change, so then detecting when something bad has happened simply requires detecting changes that should-n't have happened.

Integrity checking is generally considered one of the strongest anti-malware controls since it has the potential to detect and locate all persistent malware intrusions along with any additional persist-ent changes to the system that malware could have made. Unfortunately it is a detective rather than a preventative control - it can only detect when prevention has failed and so is only good after the

the receiver. The receiver receives the message and the signature and applies the verifying algorithm to the combination. If the result is true, the message is accepted otherwise it is rejected.

A conventional signature is like a private key belonging to the signer of the document. The signer uses it to sign documents. The copy of the signature on a file is like a public key so anyone can use it to verify a document to compare it to the original signature.



In digital signature the signer uses her private key applied to a signing algorithm to sign the document. The verifier uses the public key of the signer applied to verifying algorithm to verify the sign. When a document is signed anyone including Bob can verify it because everyone has access to Alice's public key. Alice must never use her public key to sign the document because anyone could forge her signature. Digital signatures have assumed great significance in the modern world of web-commerce. Many countries have made provisions for recognizing digital signature as a valid authorization mechanism like paper-based signatures.

5) Authentication

In computing, authentication is the process of verifying

The identity of a person or device. A common example is entering a username and password when you log in to a website. Entering the correct login information lets the website prove to you and you to it that it is actually you accessing the website. While a username/password combination is a common way to authenticate your identity, many other types of authentication exist. For example, you might use a four- or six-digit passcode to unlock your phone. A single password may be required to log on to your laptop or work computer. Every time you receive or send email, the mail server verifies your identity by matching your email address with the correct password. This information is often stored by your web

PAGE NO.
DATE: / /

browser or email program so you do not have to enter it each time.

Biometrics may also be used for authentication for example, many smartphones have a fingerprint sensor that allows you to unlock your phone with a simple tap of your thumb or finger. Some facilities have retinal scanners, which require an eye scan to allow authorized individuals to access secure areas. Apple's Face ID (introduced with the iPhone X) authenticates users by facial recognition.

Two-factor authentication

Authentication is a part of everyday life in the digital age. Until it helps keep your personal information private, it is not foolproof. For example, if someone knows your email address, he or she could gain access to your account by simply guessing your

password. This is why it is important to use uncommon, hard-to-guess passwords, especially for your email accounts. It is also a good idea to use two-factor authentication when available, as this provides an extra security check when accessing your account.

Two-factor authentication (2FA) typically requires a correct login plus another verification check. For example, if you enable 2FA for your online bank account, you may be required to enter a temporary code sent to your phone or email address to complete the login process. This ensures that only you (or someone with access to your account) can gain access after entering the correct login information.

Note:- On many websites you can select the "Remember me" checkbox when logging

in to a secure website. This will store a cookie on your device which indicates the device is trusted/or previously authenticated for that website. The cookie may keep you logged in over multiple browser sessions or may prevent the need for two-factor authentication when using that device in the future.