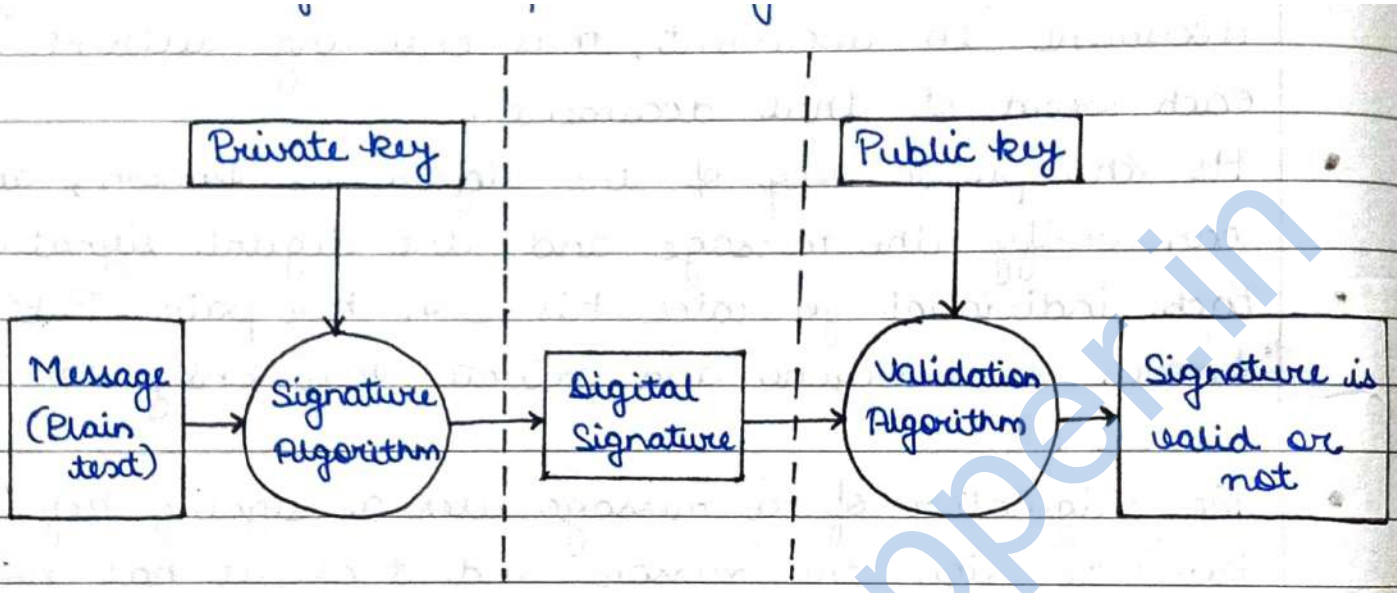
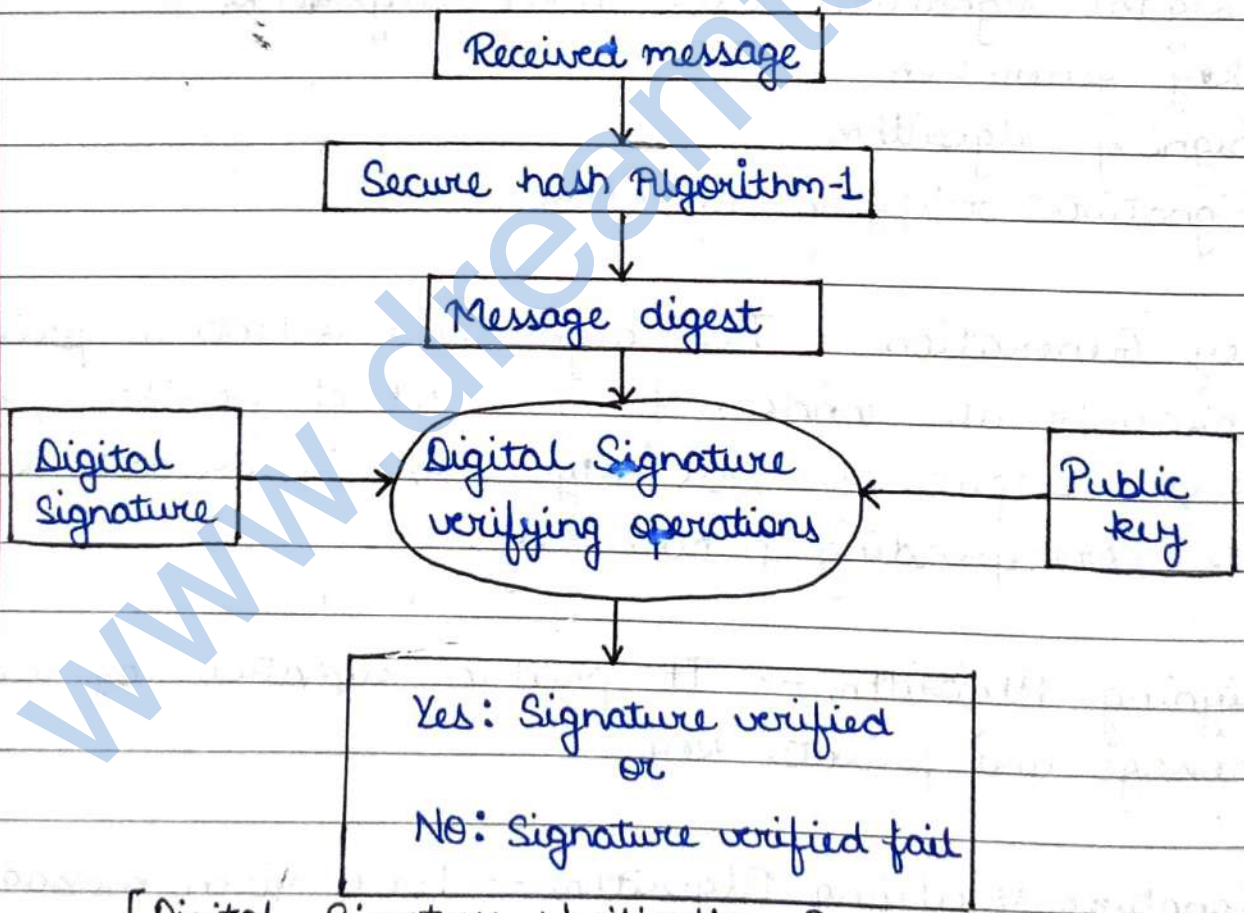




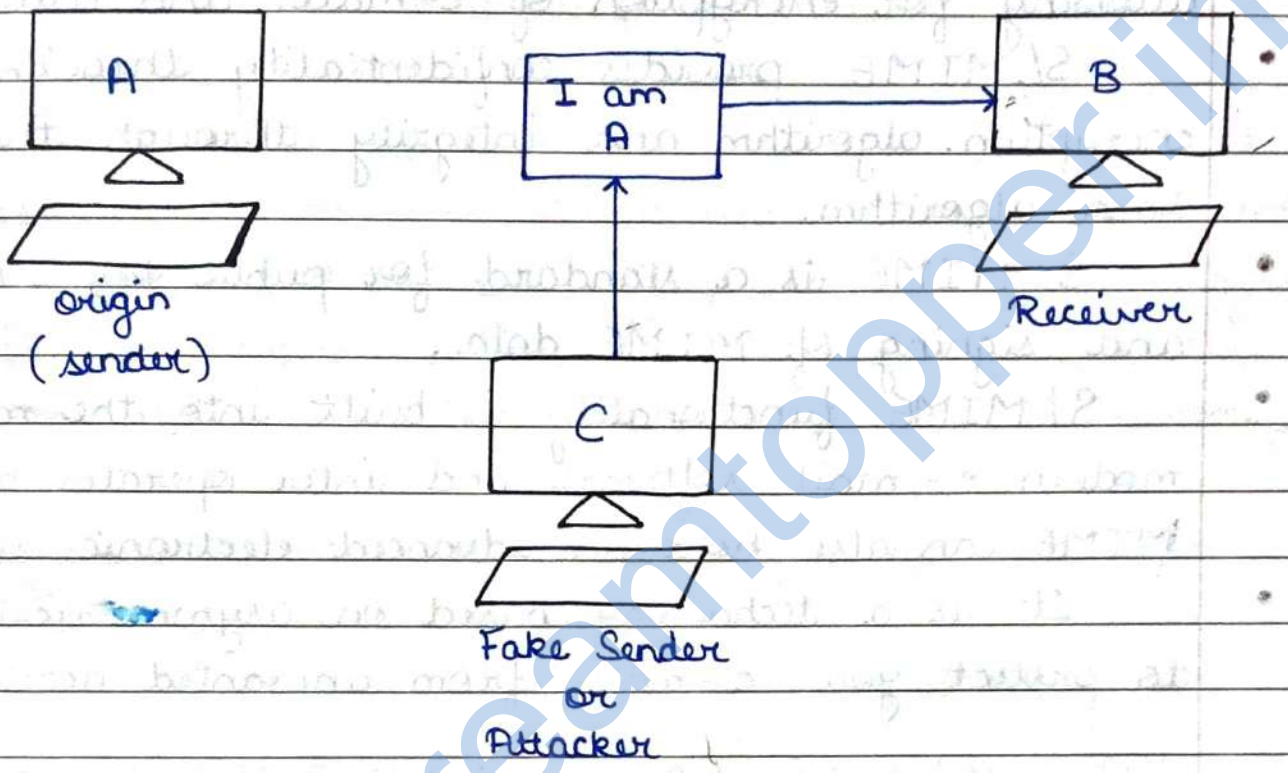
[Digital Signature Verification Process]

today for safe business - transaction online.

Authentication - Authentication helps in proof of identities. It ensures that the origin (sender) of an electronic message or document is correctly identified.

For example:

In absence of Authentication



* **MIME (Multipurpose Internet Mail Extension):-**

This is a technical specification indicating how multi-media data and e-mail attachments are to be transfered.

Internet has e-mail standards that dictate how a mail is to be formatted, encapsulated, transmitted and opened.

If a message or document contains a multimedia attachments, MIME dictates how that portion of the message should be handled.

★ S/MIME (Secure Multipurpose Internet Mail Extension):-

- It is a standard for encryption and digitally signing e-mails that contains attachments and providing secure data transmission.
- S/MIME extends the MIME standard by allowing for encryption of e-mails and attachments.
- S/MIME provides confidentiality through the user's encryption algorithm and integrity through the user's hash algorithm.
- S/MIME is a standard for public key encryption and signing of MIME data.
- S/MIME functionality is built into the majority of modern e-mail software and inter operates between them. MIME can also hold an advanced electronic signature.
- It is a technology based on asymmetric cryptography to protect your e-mails from unwanted access.

★ Authentication Application : Kerberos :-

- Kerberos provides a centralised authentication server whose function is to authenticate users to servers and servers to users.
- Kerberos relies exclusively on conventional encryption, making no use of public key encryption. The following are the requirements of Kerberos -

Secure

1- Secure - A network eaves-dropper should not be able to obtain the necessary information to impersonate a user. More generally kerberos should be strong enough that a potential opponent does not find it to be the weak link.

2- Reliable — For all services that relie on kerberos for access control, lack of availability of the kerberos service means lack of availability of the supported services. Hence, kerberos should be highly reliable and should employ a distributed server architecture with one system able to backup another.

3- Transparent, 4- Scalable

- Kerberos is a network authentication protocol. It is designed to provide strong authentication for client-server applications by using secret key cryptography. A free implementation of this protocol is available from the MIT (Massachusetts Institute of Technology).

- Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice-versa), across insecure internet connection.

- Kerberos is freely available from MIT under copyright permission very similar those used for the BSD operating system.

Kerberos works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one-another in a secure manner. It provides mutual authentication — both the user and the server verify each other's identity.

Kerberos uses UDP port 88 by default.

★ X.509 :- In cryptography, X.509 is a standard which is used to define the format of public key certificates. X.509 certificates are used in many internet protocols such as - https.

- It is also used in digital signatures.
- An X.509 certificate contains a public key and an identity (a host name, or an organisation or an individual) and is either signed by a certificate authority or self-signed.
- X.509 is defined by ITU-T (International Telecommunication Union's) Standardisation sector.
- X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

★ Directory Authentication Service :-

- It is an external authentication directory service (also called an enterprise directory or authentication login domain) to provide a single sign-on for group of users instead of maintaining individual local login accounts.
- Each user in a group is assigned the same role (for example - infrastructure administrator). An example of an authentication directory service is a corporate directory that uses LDAP (Light-weight Directory Access Protocol).
- After the directory service is configured, any user in the group can log into the application or appliance. On the login windor the user -

→ Enters their user-name (CN, common name attribute)
→ Enter their password.
→ Selects the authentication directory service. This box appears only if you have added an authentication directory service to the appliance.

When you add an authentication directory service to the appliance, you provide such criteria so that the appliance can find the group by its DN (Distinguished Name)

Q

★ Pretty Good Privacy (PGP) :-

It is a computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting, decrypting e-mails to increase the security of e-mail communications.

PGP is a popular program used to encrypt and decrypt email over the internet, as well as authenticate messages with digital signatures and encrypted stored files.

PGP is based on public key method, which uses two keys - one is a public key that you disseminate to anyone from whom you want to receive a message. The other key is a private key which is used to decrypt messages.

PGP consist five services -

1- Authentication
2- Compression
3- Confidentiality
4- Email compatibility
5- Segmentation

1- Authentication — A hash code of message is created. using SHA-1. This message digest is encrypted using RSA with a sender's private key. and included with the message.

2- Compression — As a default PGP compresses the message after applying the signature but before encryption. This has the benefit of saving space both for email transmission and for file storage.

3- Confidentiality — Message is encrypted using IDEA or 3DES with a one-time session key generated by the sender. The sender key is encrypted using diffiehellman or RSA with a recepient's public key and included with the message.

4- Email compatibility — Email systems only permit the use of blocks consisting of ASCII text. To accomodate this restriction PGP provides the service converting the raw it with binary stream to a stream or printable ASCII characters.

Following

5- Segmentation — To accomodate maximum message size limitations, PGP performs segmentation and re-assembly.

PGP documentation often uses the term secret keys do refer to a key-paired with a public key encryption scheme.