
Email
service
security

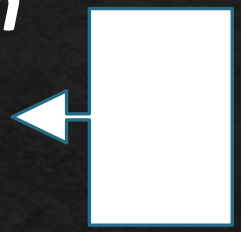
Email Security

Email security can be defined as the use of various techniques to secure sensitive information in email communication and accounts against unauthorized access, loss, or compromise. In simpler terms, email security allows an individual or organization to protect the overall access to one or more email addresses or accounts.

Email Security Requirements:

- ***Confidentiality***
- ***Authentication***
- ***Integrity***
- ***Non repudiation(***Nonrepudiation ensures that no party can deny that it sent or received a message via encryption and/or digital signatures or approved some information.***)***

- ***Integrity***
- ***Confidentiality*** ***Message Encryption***
- ***Authentication***
- **Non-Repudiation** ***Digital Signature***

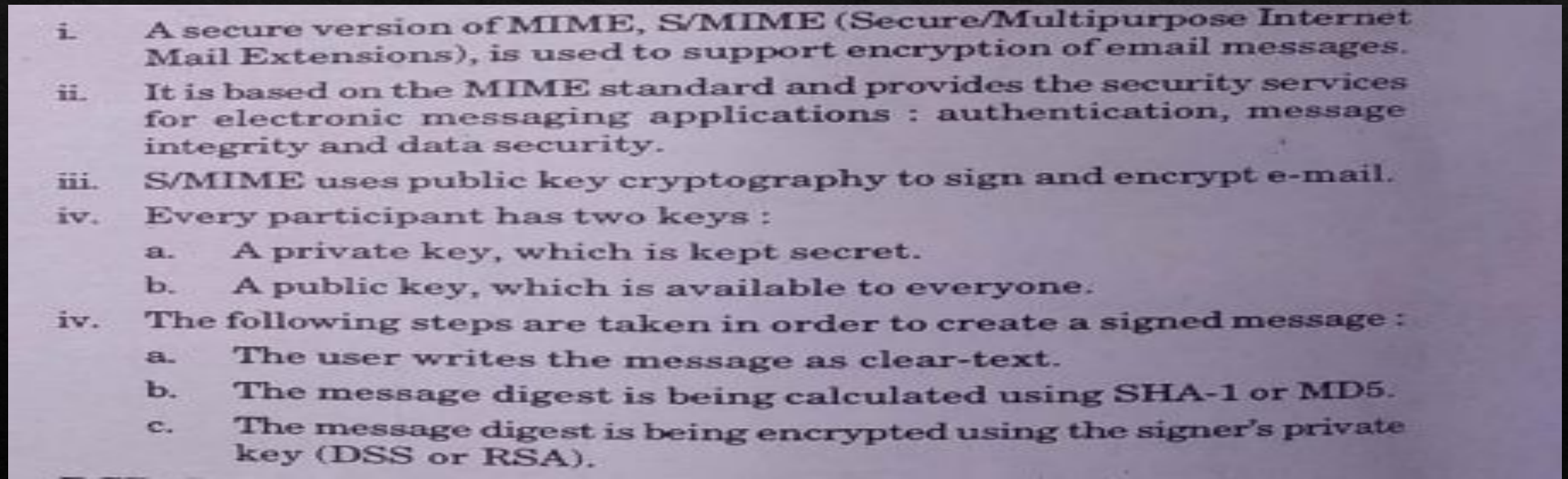


Email security certificates(S/MIME,PGP)

- SSL,TLS protocols refers to the standard protocol used to secure email transmission.
- Transport Layer Security provides a way to encrypt a communication channel between two computers over the internet.

Email Certificate

Email certificates, also known as SMIME (secure/multipurpose internet mail extension)certificates, are digital certificates that can be used to sign and encrypt email messages. When you encrypt an email using an email certificate, only the person that you sent it to can decrypt and read the email. The recipient can also be sure that the email hasn't been changed in any way.



i. A secure version of MIME, S/MIME (Secure/Multipurpose Internet Mail Extensions), is used to support encryption of email messages.

ii. It is based on the MIME standard and provides the security services for electronic messaging applications : authentication, message integrity and data security.

iii. S/MIME uses public key cryptography to sign and encrypt e-mail.

iv. Every participant has two keys :

   a. A private key, which is kept secret.

   b. A public key, which is available to everyone.

iv. The following steps are taken in order to create a signed message :

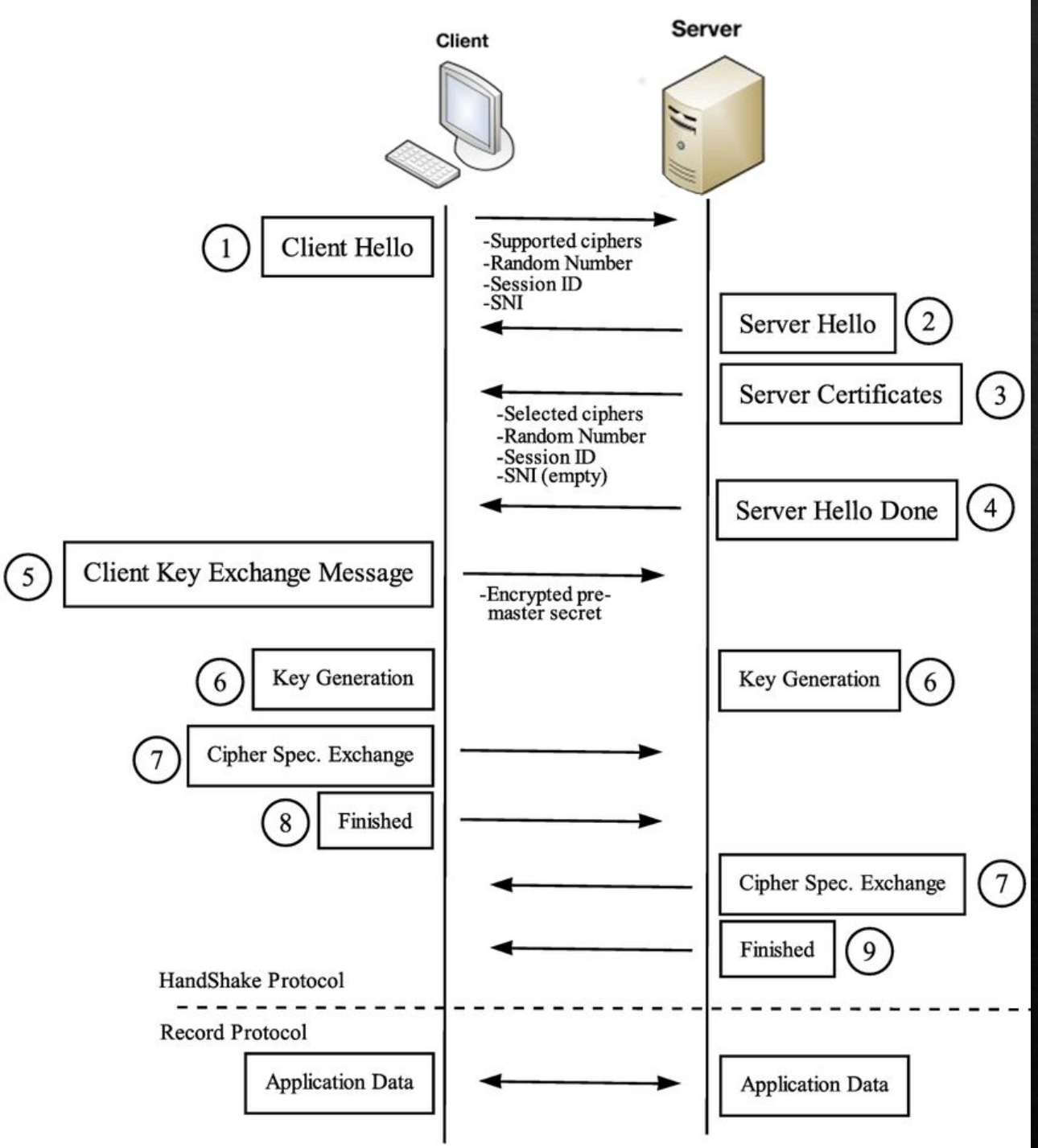
   a. The user writes the message as clear-text.

   b. The message digest is being calculated using SHA-1 or MD5.

   c. The message digest is being encrypted using the signer's private key (DSS or RSA).

TLS(Transport Layer Security)

- TLS is a cryptographic protocol built to provide a secure connection protecting the security and privacy between two communicating parties.
- TLS operates below the Application layer and above Transport layer.
- It is used extensively in applications, as HTTP, FTP, SMTP and VoIP, where security and privacy are needed.
- HTTP Secure (HTTPS) is technically not a protocol by itself, as it simply HTTP used on top of TLS.
- When a client and server connect over HTTPS, they first complete a TLS handshake .



SNI - Server name indication extension