protocol action.

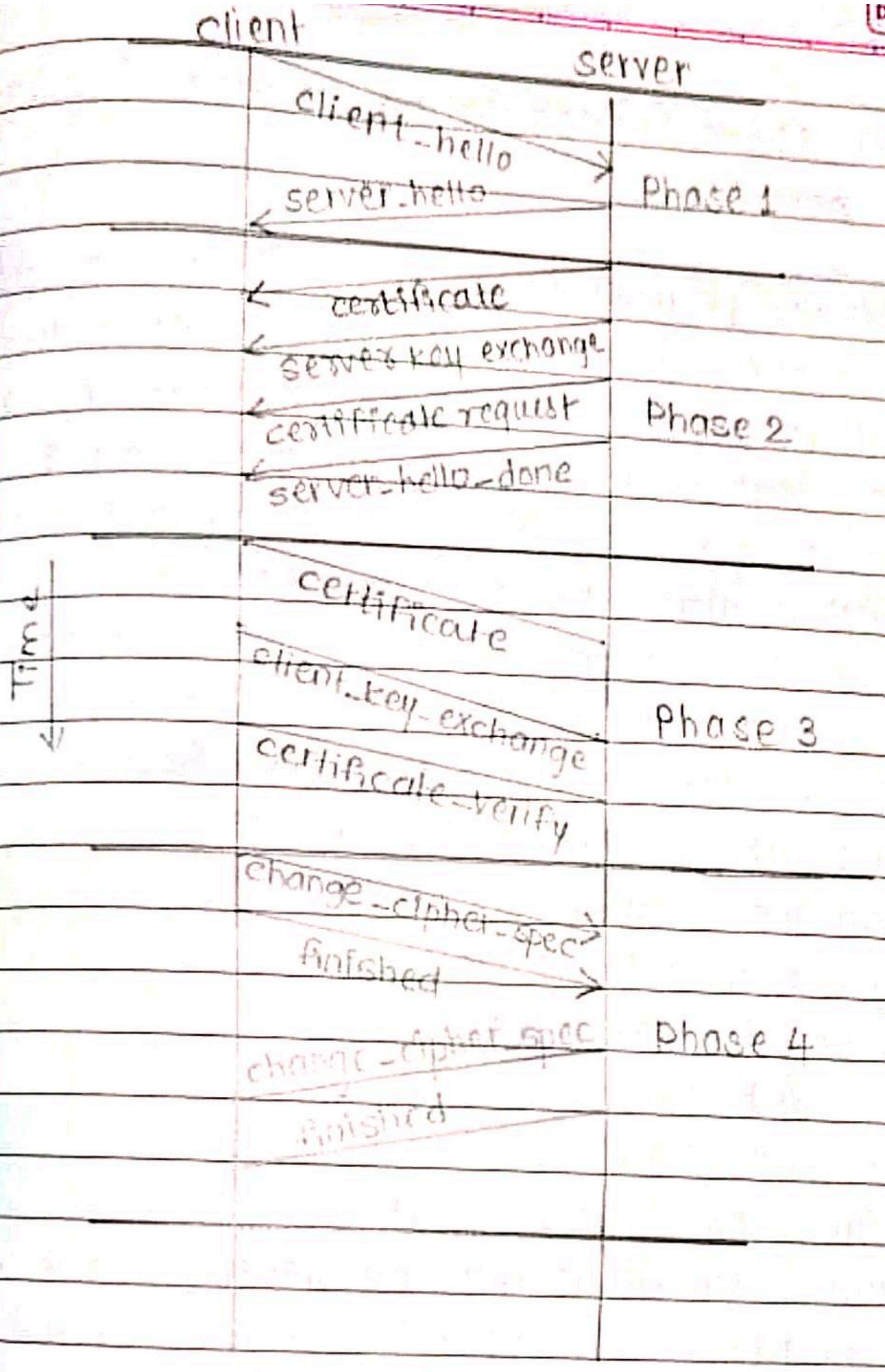
- Handshake protocol allows the server & client to authenticate each other and to negotiate an encryption and MAC algorithm.
- It consist of a series of messages exchanged by client and server.

Phase 1 =

Establish security capabilities, including protocol version, session ID, cipher suite, compression method & initial random numbers.

Phase 2 =

Server may send certificate, key exchange, & request certificate. Server signals end of hello message phase.



Handshake Protocol Action

Phase 3 =

Client send certificate if requested. Client send key exchange. Client may send certificate verification.

Phase 4 =

Change cipher suite & finish handshake protocol.

1) PGP message generation:

a) Signing the message:

- PGP retrieves the sender's private key from the private-key-ring using your userid as an index. If your user-id was not provided in the command, the first private key on the ring is retrieved
- PGP prompts the user for the passphrase to recover the unencrypted private key.
- The signature component of the message is constructed.

b) Encrypting the message:

- PGP generates a session key & encrypts the message.
- PGP retrieves the recipients public key from the public-key ring using her-userid as an index.
- The session key component of the message is constructed.

2) PGP message reception

a) Decrypting the message:

- PGP retrieves the receivers private key from the private key using key ID in the session key component of the message as an index.
- PGP prompts the user for the passphrase to recover unencrypted private key.
- PGP then recovers session key and decrypts. the message.

b) Authenticating the message:

- PGP retrieves the sender's publickey from public-key ring using key ID.
- PGP recovers the transmitted message digest.
- PGP computes the message digest for the received message and compares it to the transmitted message digest to authenticate.

Secure/Multipurpose Internet Main Extension (S/MIME) is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security.

- To understand S/MIME, we need to have general understanding of MIME and RFC 5322.

1) RFC 5322-

- RFC 5322 defines a format for text messages that are sent using electronic mail.

PAGE NO.:

DATE / /

- In the RFC 5322 context, messages are viewed as having an envelope and contents.
- The envelope contains whatever information is needed to accomplish transmission and delivery.
- The contents compose the object to be delivered to the recipient.
- The RFC 5322 standard applies only to the contents.

2) MIME -

- Multipurpose Internet Mail Extension (MIME) is an extension to the RFC 5322 framework that is intended to address some of the problems and limitations of the use of SMTP, defined in RFC 821.

- Following are the limitations of SMTP-

1) SMTP cannot transmit executable files or other binary objects.

2) SMTP cannot transmit text data that includes national language characters because these are represented by 8-bit codes with values of 128 decima

3) SMTP servers may reject mail message over a certain size.

(ESP) service.

- ESP can be used to provide confidentiality, data origin authentication. connectionless integrity, an anti-replay service and traffic flow confidentiality
- ESP can work with a variety of encryption & authentication algorithms. including authenticated encryption algorithm such as GCM
- Services depend on options selected when establish security Association (SA), net location.
- ESP packet contains the following fields-

1) security Parameters Index (32 bits)
2) Sequence number (32 bits)
3) Payload data (variable)
4) Padding (0-255 bytes)
5) Pad length (8 bits)
6) Next header (8 bits)
7) Integrity check value (variable)

- Two additional fields may be present in the payload. An IV or nonce, is present if this is required by the encryption or authenticated encryption algorithm used for ESP.
- If tunnel mode is being used, then the IPsec implementation may add traffic flow confidentiality (TFC) padding after the payload Data & before the padding field, as explained subsequently.