CS253 HW9

a. Yes. The client application checks if the server domain name specified in the server certificate is the same as the actual domain name.
b. Yes. Key-management is based on short-term session keys that generated by random hash number. Each direction of communication generates independent keys for the connection as well as for each instance of the connection.
c. Yes. If the server requests client authentication, the SSL protocol requires that the client create a digital signature by creating a one-way hash from randomly generated data during the handshake and known only to the client and server. The hash data is encrypted with the client's private key that corresponds to the public key in the certificate received by the server.
d. Yes. SSL uses HMAC which is a hash-based construction. Authentication can be requested during the connection in order to protect the confidential nature of data being passed.
e. Yes. The source of the message has to be authenticated before generating a response. The messages that are continuously sent, can be removed if the source of the requests are considered invalid.