

1. B
2. B
3. B
4. C
5. D
6. B
7. C
8. C
9. C
10. D
11.
 - Browser accesses the server's secured page and sends SSL version number
 - The server sends its certificate
 - Browser obtains the server's public key by decrypting the certificate using the CA's public key.
 - Browser generates a symmetric session key and encrypts it with the server's public key and sends it to the server.
 - Server decrypts the message using its private key to get the symmetric session key.
 - Browser sends a separate encrypted message to server to indicate that the browser portion of the handshake is completed.
 - Server sends a separate encrypted message to browser to indicate that the server portion of the handshake is completed.
12. (a)
 - Encrypted digest of the e-mail message: Authenticates Alice to Bob.
 - Encrypted e-mail message: Confidentiality of the email message transferred.
 - Encrypted key: symmetric session key (one time session key) encrypted using Bob's public key. Bob decrypts using his private key to get the symmetric session key to decrypt the e-mail message.(b) Three keys ((Alice's private key, Bob's public key and the symmetric session key))
13. (a) $0.5 + (500000*8)/128000 + (0.4*10) = 35.75$ Secs
(b) $(500000*8)/128000 + 9 * (20000*8)/128000 + (0.4*10) = 46.5$ Secs
14. POST. File too big to embed in query string if using GET.
15. The Web server cannot know what type of content will be generated by a CGI script. For instance, a CGI script may generate an RSS feed, a JPEG map, a ZIP file.
16. SoC admin configures their local DNS server with the hostname cs2105-z.comp.nus.edu.sg but restricts the propagation of the entry to other DNS servers outside SoC. When connecting from ISP, the ISP's DNS server has no knowledge of the hostname, thus is unable to find its IP address.