1. Bob is tired of typing a long and complex password every time he logs into his remote server using the SSH protocol. Alice suggests using asymmetric cryptography for “password-less” authentication. What are the steps that Bob should perform to implement Alice’s suggestion? Apart from listing the steps, please provide us with a suitable public key that you have generated.

Solution:
(a) create a public-private ssh key pair.
(b) store the public key on the server.
Since Bob doesn't want to type a passphrase, he should create private key without a passphrase.

2. You were asked to enter a “passphrase” when you created the authentication key. While Bob may not want to type a passphrase, how is the passphrase used by SSH, and what benefits does it provide?

Solution:
passphrase encrypts the private key when it is stored on Bob's machine. If the machine is compromised, his private key is still safe as long as no one figures out the passphrase.

7. Assume you are using web.cert.pem as a certificate for your Web site. When you try to make a secure connection to your Web site what message will be displayed on your browser? Why? [Note, you don’t have to set up an actual Web site, nor do you have to actually use this certificate to answer this question].

Solution:
the browser should say that the certificate is not signed by a trusted authority, or maybe just that the certificate is not trusted (unless the user has installed the certificate locally as a trusted root, but that is not one of the steps we carried out)

8. In this problem you have to demonstrate the receipt of a certificate by your browser using a packet trace. Is it possible to receive multiple certificates? Why?

Solution:
Yes, the server may send the browser not only the certificate for the domain of interest (e.g., for www.example.com), but also any intermediate certificates needed to verifying the entire certificate chain.
From RFC 2246:
If the server is authenticated, its certificate message must provide a valid certificate chain leading to an acceptable certificate authority.

9. What certificate authorities are recognized by your browser? List any 5 of them.

Solution:
Answers various depend on your OS and browser.
For question 3-6, the steps are provided in the question or during the lectures. If you have any question, please post on Piazza or send me an email.