The purpose of these activities is to explore the cryptographic suite and certificate of a website.

1. Visit a secure website (other than amazon.com). What's the url?
2. What is the cryptographic suite that is being used for the secure connection?
   Note: I don't think Safari allows you to find this information easily, so use another browser.
   Which acronyms do you understand? Which ones do you *not* understand?
3. View the certificate for the website.
   (a) When was the certificate first valid?
   When will it no longer be valid?
   What is the total length of time it is valid?
   (b) What type of public key credentials is the server providing?
   (c) What protocol does the server use for signatures?
   (d) What are the values of its public keys?

4. What is the CA that signed the certificate?
   (a) When was the certificate first valid?
   When will it no longer be valid?
   What is the total length of time it is valid?
   (b) What type of public key credentials is the CA providing?
   (c) What protocol does the CA use for signatures?
   (d) What are the values of its public keys?

5. If the CA is not the root CA, repeat the previous question for the root CA.

6. Do some searching to figure out where the root CAs are stored in your particular operating system. Locate the entry for the root CA for your website on your own computer, and find the public keys for the CA.
   How does it compare to the value from the previous question?

7. How are your answers to the previous two questions related to preventing MITM attacks?