1. A trusted party publishes $p = 132\,347$ and $\alpha = 36$ to use with DHKE.

   You are playing the dastardly role of Oscar in this problem and are implementing a MITM attack where you can intercept and alter any messages that Alice and Bob send to each other. You choose to use a private key of $c = 1341$.

   Alice's value for DHKE is $A = 91\,371$ and Bob's value is $B = 126\,585$.
   You intercept these and apply a MITM attack.

   (a) What is the symmetric key that Alice will use for encrypting/decrypting messages to Bob?

   (b) What is the symmetric key that Bob will use for encrypting/decrypting messages to Alice?

   (c) If you had not implemented the MITM attack, what is the symmetric key that Alice and Bob would use?

2. The purpose of this problem is to explore the cryptographic suite and certificate of a website.

   (a) Visit a secure website (other than Wheaton's website). What's the url?

   (b) 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?

   (c) View the certificate for the website.
      i. When was the certificate first valid?
      When will it no longer be valid?
      What is the total length of time it is valid?
      ii. What type of public key credentials is the server providing?
      iii. What protocol does the server use for signatures?

   (d) What is the CA that signed the certificate?
      i. When was the certificate first valid?
      When will it no longer be valid?
      What is the total length of time it is valid?
      ii. What type of public key credentials is the CA providing?
      iii. What protocol does the CA use for signatures?

   (e) If the CA is not the root CA, repeat the previous question for the root CA.

   (f) What is the value in the "Fingerprint" section of the certificate of the root CA?

   (g) Do some searching and figure out how to find 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 Fingerprint listed there.
   How does it compare to the value from the previous question?

   (h) How are your answers to the previous two questions related to preventing MITM attacks?