1:Refer to the section in Week4 Part2 of the lecture notes that describe the Diffie-Hellman key exchange.

What values are sent in the clear between the two parties and what values are kept secret? Your answer needs to enumerate both values.

Use the description of the algorithm below to help identify the values in your answer.

Be thinking about the information that is available to an eavesdropper. 20 points.

*Description of Algorithm (by example)*

The algorithm works as follows:

 Person A and B want to exchange secure messages over any unsecure channel. They agree on using two prime numbers for values of p and the base g. For this example: p=17 and g=5.

 Person A selects a secret key known only to them (*a* = 9)

 Person B selects a secret key known only to them (*b* = 13)

 Person A sends to person B the result of the calculation for:

ga mod p =

59 mod 17 = 12

 Person B sends to person A the result of the calculation for:

gb mod p =

513 mod 17 = 3

 Person A computes:

(**gb** mod p)**a** mod p

(3)a mod p =

(3)9 mod 17 = 14 # Note: 3 represents (**gb** mod p)

 Person B computes:

(**ga** mod p)**b** mod p

(12)b mod p = # Note: 12 represents (**ga** mod p)

(12)13 mod 17 = 14

2. Calculate the Diffie-Hellman key values**. Calculate values for both keys (secret key a and secret key b).** You must show your work for full credit.This includes the calculations each person performs to calculate and verify the values.

You should show the calculation that proves the keys are correct. That requires you calculate the values for both private keys which are for person a and person b. Then to show they are correct you must use both of these keys in separate calculations to calculate the resultant value, which should be the same for both person a, and for person b.

 Using the following values: p=29, g=2 (base), secret key a = 23 secret key b=19 20 points

 Using the following values: p=11, g=5 (base), secret key a =7, secret key b=5 20 points

3. Explain what the following are: root certificates, self signed certificates. Provide some examples of each. You should be able to find examples of each on your system by looking through various options available on your browser. 20 points

4. Provide a listing of the fields associated with a certificate or your choosing. Use the X509 definition to match the general fields of a certificate with the certificate you choose to look at. Describe each field. 15 points

5. Your manager is considering implementing a PKI infrastructure. They are considering using RSA encryption technology for the central part of their infrastructure. You manager would like to know some products or services that utilize RSA encryption technology. Provide three examples and explain how they make use of the RSA encryption technology. 20 points

6. Compare the functionality offered by the RSA and Diffie-Hellman algorithms. 20 points

7. For this problem I would folks to gain some experience acquiring Digital Certificates and encryption packages. **Eventually** I would also like for you to gain experience using these packages. I want people to tread cautiously doing this problem. Whenever you install new software or copy files to your system you need to understand the implications. You need to have backups made for any important data, as well as a “rollback” strategy should the installation fail. Sometimes rollback strategies are as simple as remove the installation. Other times rollback strategies are more involved if data has been changed.

I would like you to attain a free personal email certificate. In this weeks lecture notes refer to the section **Public Key Infrastructure Exercise Week5 Part4.** In this section I provide a url to the Comodo website to obtaining a free personal email certificate:

<http://www.instantssl.com/ssl-certificate-products/free-email-certificate.html>

I would like for each of you to obtain a certificate and to document the process you used to obtain it. I would like the process documented in bulleted list format so that someone else trying to obtain a certificate can easily follow your instructions. Consider that these instructions will be in a user manual. Including screen shots to support your directions is encouraged and will enhance your presentation.

The accuracy and ease of use of your instructions are key components of your presentation. The overall usability of your presentation is important. This includes having instructions that are easy to follow. Using correct spelling and grammar is important.

For example:

 1) click on the following link.

 2) fill in the requested parameters, click NEXT

 3) locate the url at the bottom of the page and click

 4) copy the certificate to the following area.

 Etc.

You should download the certificate to your system and verify it is there. These steps should be part of you documentation. 25 Points

You should also start looking at what is involved in using these certificates in Microsoft Outlook Express or the email client of your choice. Also, start looking at the the GnuPG and PGP websites. This urls are in the lecture notes. You should consider what would be involved for you to make use of GnuPG and the Trial copy of PGP. Start keeping notes on how you might approach the use of these packages, what issues you envision and rollback strategies. Communicating with classmates about this assignment in the discussion board will be important.

In upcoming weeks we will have an assignment that “can” make use of this certificate in Outlook Express, Outlook or the email client of your choice. We will be sending email that makes use of Digital Signatures and Encryption. One way you can test this functionality by yourself is to set up multiple mail accounts and send mail to yourself. You can also exchange mail with classmates that are using the same mail clients.

Because of the operating systems or applications used by some students you are free to use the mail client of your choice. You may be comfortable using a different Microsoft or Linux mail client. Also if you make use of an internet mail service such as gmail or hotmail there are encryption and digital signature capabilities used by them for secure exchange of mail. This may mean not making use of this certificate to exchange signed and encrypted email.

Let’s start with obtaining the certificate, documenting that process and investigating the encryption packages. Irrespective of the email clients you will be using I want everyone to obtain this certificate according to the assignment.