1. Consider an RSA system with p = 11  q = 17.  
   (a) Find Φ(pq).

N = 11 x 17 = 187

Φ(n) = (11 – 1)(17 – 1)

= (10)(16)

= (160)

(b) Let e = 3, find d such that e·d=1 (mod Φ (pq)).

E \* D mod p(n) = 1

3 \* D mod 160 = 1

106x + 3y = 1

160 = 53(3) + 1

160 – 53(3)

160 – 53 = 107

D = 107

(c) Encrypt M = 47.

C(m) = m3(mod 187)

C(m) = 38

2. Suppose Alice and Bob have RSA public keys in a file on a server. They communicate regularly using authenticated, confidential messages. Eve wants to read the messages but is unable to crack the RSA private keys of Alice and Bob. However, she is able to break into the server and alter the file containing Alice’s and Bob’s public keys.

a. How should Eve alter that file so that she can read confidential messages sent between Alice and Bob, and forge messages from either?

By replacing their public keys with your own, which will result in both Bob and Alice encrypting their messages with your public keys and thus you are able to decrypt their messages.

b. How might Alice and/or Bob detect Eve’s subversion of the public keys?

After the public keys are replaced, Bob and Alice won’t be able to decrypt the messages correctly and soon enough they will realize that there is a problem with the keys.

3. Digital Certificate practice.   
1). Go to verisign.com to submit a certificate request. In the link below, click “buy online”, and select the 25 days trial version. Fill in the enrollment form and finish the request. <http://www.symantec.com/digital-id>

I went to the website and clicked on the free trial version. I filled out the necessary information and finished the request

2). An email will be sent to your mail box with a PIN number.

An email was sent with a PIN number needed to access my account.

3). Pick up the signed certificate at VeriSign site using the PIN number.

I picked up the signed certificate at the VeriSign site using the PIN number.

4). Install the certificate on browser.

I am prompted to click generate key & install to generate a new public and private key pair. The public key is sent to Symantec and there it is used to create the certificate and it is stored. The certificate and private keys are then stored in our local key store.

5). Export the digital ID following the instructions in the following link. Submit your .PFX file as part of the deliverables.

<https://knowledge.verisign.com/support/digital-id-support/index?page=content&id=AR226>