1) Alice wants to send Bob a digitally-signed piece of email from her desktop computer to his. Assume the following:
   a) Alice uses certification authority X and has a public key certificate issued by X.
   b) Bob uses certification authority Y and has a public key certificate issued by Y.
   c) Y is a root CA and X is a non-root CA, certified by X.
   d) Alice has a true copy of X's public key certificate.
   e) Bob has a true copy of Y's public key certificate.
   f) X and Y each have a directory service by which users can retrieve public key certificates each CA has signed.
   g) Alice and Bob both use the same email program that uses public key-based digital signatures. Only the signature will be attached to the message.

The first and last steps of the process are given below. Fill in the rest of the steps needed for the protocol to be successful. Be complete, including steps that would most likely be automated. (Hint: there are more than ten steps.)

Begin: Alice writes a message M to send to Bob.
Alice uses her public key to sign the message.
Alice sends the message to Bob.
Bob opens the message and detects the digital signature.
Bob queries X for a copy of Alice's public key certificate, or Bob asks for and receives from Alice for a copy of her certificate.
Bob detects X's signature on Alice's public key certificate.
He queries X for a copy of its public key certificate.
Bob detects Y's signature on the public key certificate.
Bob retrieves Y's certificate from Y and discovers that it is a root certificate.
Bob checks that the certificate is valid, can be used for certificate issuance, and is associated with Y.
Bob verifies the signature on Y's self-signed certificate.
Bob retrieves a CRL from Y and makes sure that X's certificate is not revoked.
Bob checks that the certificate is valid, can be used for certificate issuance, and is associated with X.
Bob verifies the signature of Y on X's certificate.
Bob retrieves a CRL from X and makes sure that Alice's certificate is not revoked.
Bob verifies the signature of X on Alice's certificate.
Bob checks that the certificate is valid, can be used for signing, and is associated with Alice.
Bob verifies the signature of Alice on the email message.

End: Bob reads the message M, knowing that it is the message that Alice signed.
2) Eve is attempting to prevent Alice and Bob from communicating securely. She cannot physically disconnect Alice, Bob and the certification authorities X and Y, and she does not have the resources to break the cryptography and forge Alice's signature. What else might she do to disrupt the process described in Question #1?

Denial of service against Bob's email program and/or email service.  
Host attack against Alice's computer to steal her private key.  
Host attack against Bob's computer to alter the message after signature validation.  
Host attack against Bob's computer to alter the signature verification software.  
Host attack against Bob's computer to delete Alice's message.  
Masquerade attack against X to get Alice's certificate revoked.  
Denial of service attack against X and/or Y to prevent certificate validation.
3) You have passed ECT 582 with flying colors and are now in great demand as an e-commerce security consultant. Your client Alice owns and operates a defense contracting business of around 80 employees with close ties with the federal government. The Department of Defense is requiring that all contractors encrypt their email communications regarding the technical details of contracted work using public key encryption. They are also requiring that electronically-submitted proposals and bids for contracts be digitally signed. Alice is not familiar with public key encryption and has hired you to help her decide how to implement encryption policies for her company.

Alice's organization is very flexible and organized around its contracts of which there may be 10 or more going on at once. Most employees work on multiple contracts, but each contract has a single project manager responsible for interacting at an official level with contacts in the government and military. There is usually a great deal of interaction with government managers, scientists and other personnel during the course of a project. There is a separate Contracting department (10 employees) that works on bids and project proposals. There may be dozens of proposals being prepared at any one time.

Because the government's security requirements, all private keys must be generated and stored in secure hardware tokens, certificate issuance policies might provide high assurance, those possessing such keys must have background checks, and only government-approved certification authorities can be used. This makes certificate generation expensive, and Alice's first idea was that she, her chief operating officer, and the head of the Contracting division will each get one certificate.

Write a memo to Alice outlining an effective strategy for meeting the DoD requirements and integrating public-key cryptography into her business. Address the following points:

a. Certificate issuance: Explain why Alice's idea of obtaining three certificates is not a good one. Provide an alternate policy for certificate issuance. Who in the organization needs to have a public key certificate? Do some individuals need more than one certificate? Can you prioritize the need for certificates if Alice decides to get some immediately and others later?

b. Infrastructure: Outline the technical infrastructure that Alice will need. You can assume that her engineers and office staff use standard PC workstations. What additional components will be necessary to make effective use of encryption / digital signatures and meet the contracting requirements?

There is no single right answer to this question. I was looking for thoughtful and thorough consideration of various issues involved.

1. Three certificates is not enough. The primary reason is that encryption and signature keys have different purposes and different life cycles and one key cannot serve both purposes. If Alice's COO has an encryption certificate and the Contracting Officer has a signing certificate, what type does Alice have? If she has a signing key, then she can't interact securely with the government. If she has an encryption key, then she can't sign. To avoid a single point of failure, she (at the very least) would need to have both kinds of keys.

2. An encryption key is useful only for receiving encrypted mail, and because the key is issued to an individual and stored in a hardware token, it will need to be closely associated with an individual. It would be theoretically possible for a small number of individuals to do all the decryption for the whole company. (Necessarily more than one for single point of failure reasons.) However, a solution like this seems to introduce a bottleneck into the regular communication between Alice's company and its contacts. If we are going to introduce such a concentration point, the most logical place is probably the project manager. (Just for backup, a senior person under the manager might also having a key.)
3. As far as signing is concerned, there may only be a few individuals in the organization who are authorized to engage the company in contractual matters. Alice and the head of the contracting unit would be the absolute minimum for signing keys. It could be argued that more members of the contracting unit might ultimately need keys.

4. Alice will need to augment her technical infrastructure to meet the new requirements of encryption and digital signature. She will need software for encrypting email and for digitally signing documents. She will need hardware and software for interacting with the hardware tokens that are used to store private keys. She will need software to interact with the CA when keys are generated and certificates need to be issued. She will probably need to consider the problem of archiving encryption keys. She will have to develop key management policies including key lifetime, procedures for generating keys and requesting certificates (probably in conjunction with the CA's policies.)