**Please give the assignment to someone that masters the topic.  
  
Complete both scenarios (2.5 pages per scenario)**

**SCENARIO ONE:**

**1.** Alice, a high net worth customer, she banks online at Super Secure Bank (SSB) and has agreed to use 3DES in communicating with SSB.

**2**. One day, Alice received a statement that shows a debit of $1,000,000 from her account. On inquiring, she was told that the bank manager,Bob, transferred the money out of Alice's account and into an account of his own in an offshore bank.

**3.** When reached via email in the Cayman Islands, Bob produced a message from Alice, properly encrypted with the agreed upon 3DES keys, saying: "Thanks for your many years of fine service, Bob. Please transfer $1,000,000 from my account to yours as a token of my esteem and appreciation. Signed, Alice."

**4.** Alice filed suit against Bob, SSB and the government of the Cayman Islands, claiming that the message was a forgery, sent by Bob himself and asking for triple damages for pain and suffering.

**5.** Bob has responded by claiming that all procedures were followed properly and that Alice is filing a nuisance suit.

**Your Role:** Informed that you have completed an Information Assurance Masters Degree at the University of Maryland University College, the SSB employed you as a cryptographic expert to lead the investigation of this matter, and produce a report for the SSB Board of Directors, which will assist them in determining how to proceed in this matter. Your professional fee for this service will be $25,000.

**Your Report:** This document to the Board of Directors should address the following issues:

**a.** What can be determined from the facts as presented about whether Alice intended to make Bob a gift of $1,000,000?

**b.** Assuming SSB wishes to continue using only 3DES as its cryptographic system, what could SSB and Alice have done to protect against this controversy arising?

**c.** Would this controversy have arisen if SSB had been using AES rather than 3DES?

Your report should clearly address these issues, with sufficient detail and background to allow the cryptographically challenged Board of Directors to understand the issues involved and formulate plans for how to approach the immediate issue with Alice, and to continue business in the future, assuming that they want to continue using 3DES.

**SCENARIO TWO:**

1. Alice changes banks following her troubles with SSB. At her new bank, Modern Security Trust (MST), she uses RSA as her cryptographic system.
2. She creates a key pair and supplies Frank, an officer of MST who will handle her account, with her public key {eA, nA}, securing her private key {dA, nA}on a floppy disk which she keeps locked in a wall safe at her home.
3. In turn, Frank gives Alice access to a key server maintained by MST so that she can readily obtain his current public key {eF, nF} whenever she needs to communicate securely with him.
4. Things are fine for several months, until Alice sends Frank a message m asking about current interest rates on Certificates of Deposit issued by MST. As shown below, she enciphers the message first, and then signs it:   
     
   http://polaris.umuc.edu/its/CSMN/csmn683/clip_image002.gif
5. A few days later, Alice received a statement that shows a debit of $1,000,000 from her account. On inquiring, she was told that Frank transferred the money out of Alice?s account and into an account of his own in a bank on the Caribbean island of Nevis. When reached via long distance in Nevis, Frank produced a message g from Alice saying: "Thanks for your excellent service, Frank. Please transfer $1,000,000 from my account to yours as a token of my esteem and appreciation. Signed, Alice."
6. Alice filed suit against Frank, MST and the government of the Nevis, claiming that the message was a forgery sent by Frank himself, and asking for triple damages for pain and suffering. Frank has responded by claiming that all procedures were followed properly and that Alice is filing a nuisance suit. You have been employed by MST as a cryptographic expert to assist in the investigation of this matter. You obtain Frank?s private key from the MST server, and the cipher text c, and calculate:  
     
   http://polaris.umuc.edu/its/CSMN/csmn683/clip_image004.gif

**Your report to the MST Board of Directors should address the following issues:**

* **What can be determined from the facts as presented about whether Alice intended to make Frank a gift of $1,000,000?**
* **Assuming MST wishes to continue using RSA as its cryptographic system, what MST and Alice could have done to protect against this controversy arising?**

Your report should clearly address these issues, with sufficient detail and background to allow the Board of Directors to understand the issues involved and formulate plans for how to approach the immediate issue with Alice, and to continue business in the future, assuming that they want to continue using only RSA.