1. 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?
   b. How might Alice and/or Bob detect Eve's subversion of the public keys?

2. Given a message M, an authentication function T_{k1} (MAC or digital signature), and an encryption function E_{k2} (symmetric or asymmetric), there are several choices of how to authenticate and encrypt messages. Three ways you can do this are:

$$T_{k1}(M), E_{k2}(M) \quad (1)$$
$$E_{k2}(M||T_{k1}(M)) \quad (2)$$
$$T_{k1}(E_{k2}(M)), E_{k2}(M) \quad (3)$$

   (1)says send the authentication of the message and the encryption of the message separately. (2) says first authenticate the message, then encrypt the concatenation of the message and its authentication. Finally, (3) says to encrypt the message, then send the authentication of the encryption along with the encryption. For each of these, discuss to what degree it is secure, and what trade-offs a given approach provides, such as regarding efficiency performance.

3. Below are two variations of the Needham-Schroeder algorithm. For each variation, state whether the protocol is secure; if it is, present an argument why it is so, if it is not, demonstrate an attack. (Note: exclude from consideration attacks that assume Eve is able to get the session key from past sessions.)

1) Alice → Cathy: Alice||Bob||r_1
   Cathy→Alice: {Alice||Bob||r_1||k_s||{Alice||k_s||r_1}k_{BC}}k_{AC}
   Alice→Bob: {Alice||k_s||r_1}k_{BC}||{r_1}k_s
   Bob→ Alice: {$r_1 + 1$}k_s

2) Alice → Cathy: Alice||Bob||r_1
   Cathy→Alice: {Bob||r_1||k_s}k_{AC}||{Alice||k_s}k_{BC}
   Alice→Bob: {Alice||k_s}k_{BC}
   Bob→ Alice: {r_2}k_s
   Alice→Bob: {$r_2 + 1$}k_s