Problem 1:
The OSPF routing protocol uses a MAC rather than digital signatures to provide message integrity. Why is use of a message authentication code, MAC, a better choice than use of a digital signature?

Problem 2:
Think about whether it is possible to use a nonce and public key cryptography to solve the end-point authentication problem. Consider the following natural protocol:
(1) Alice sends the message **"I am Alice"** to Bob.
(2) Bob chooses a nonce, **R**, and sends it to Alice.
(3) Alice uses her **private** key to encrypt the nonce and sends the resulting value to Bob.
(4) Bob applies Alice's public key to the received message. Thus, Bob computes **R** and believes the Alice he is communicating with is the authenticate Alice.

a) Diagram this protocol, using the notation for public and private keys employed in the textbook.
b) Suppose that certificates, as issued by certificate authorities are not used. Describe and diagram how Trudy can become a "woman-in-the-middle" by intercepting Alice's messages and then pretending to be Alice to Bob.

Problem 3:
Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (K_B^+, K_B^-), and Alice has Bob's certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function $H(\bullet)$.

a) In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message? If so, show how with a block diagram for Alice and Bob.
b) Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? If so, show how with a block diagram for Alice and Bob.

WIRESHARK LAB: SSL Lab