1. Describe how Optimal Asymmetric Encryption Padding (OAEP) improves the security of an RSA message.
   1. OAEP improves RSA encryption by adding a random element in the encryption process. This random element allows encryptions of the same plain text to become different each time. The differing results help prevent man-in-the-middle attacks or anyone else monitoring the transmissions since the original text is harder to extract because of the random element.
2. Encrypt the message “War is God’s way of teaching Americans geography" using a Vigenère cipher with the key "facilitate".
   1. bat qd ohd’l afy qn emtcamsg cupzbctrx ggwrztpac
3. Suppose Alice and Bob share two secret keys: an authentication key S1 and a symmetric encryption key S2. Augment Figure 8.9 so that both integrity and confidentiality are provided.
   1. Integrity: Alice should use both m and a newly created S1 inside the hash, H(m+S1). Bob should decrypt the message, since he will know S1. Bob can also check to make sure what he got from Alice matches what he gets when he encrypts the message. This allows him to know that the message has not been tampered with.
   2. Confidentiality: Alice can encrypt the message and the S1+message with another key, S2. Bob can decrypt the first layer with S2 and check if m+his S1 matches the received S1+m from Alice.
   3. Both of these can slightly overlap, especially if S1 and S2 are only known to Bob and Alice.
4. The OSPF routing protocol uses a MAC (Message Authentication Code) rather than digital signatures to provide message integrity. Why do you think a MAC was chosen over digital signatures?
   1. MAC addresses do not require encryption to create, but digital signatures do (645). This means that it is less work to use a MAC address than a digital signature.
5. In Section 8.6.1, it is shown that without sequence numbers, Trudy can wreak havoc in an SSL session by interchanging TCP segments. Can Trudy do something similar by deleting a TCP segment? What does she need to do to succeed at the deletion attack? What effect will it have?
   1. Trudy can delete TCP segments. To be able to succeed at the deletion, she needs to be able to be a woman-in-the-middle and intercept messages between the victims. The attack will result in a loss of communication between the two victims.