1. Alice and Bob both have a public and private key pair.
   a. Explain (i) how Alice signs a message and (ii) how she encrypts a message using her key-pair for confidentiality.
   b. Is there a security problem if Alice uses the same key-pair for signing and for encryption?

2. Explain why the Diffie-Hellman key generation protocol is vulnerable to a man-in-the-middle attack. Explain why this is no longer the case if Bob posts his value $g^b$ publicly and always uses the same value for $b$.

3. Explain how Alice can sign her message to Bob using secret key technology if she and Bob share a secret key.

4. Explain how you would instrument a dictionary attack on a UNIX password file. Explain the purpose of the salt. Explain how to modify the hash to slow down a dictionary attack.

5. Lists technologies available for biometric authentication and shortly discuss their operational shortcomings, in particularly false positives and false negatives.

6. How difficult is eavesdropping? How difficult is spoofing a TCP connection from a different domain?

7. Give an authentication protocol vulnerable to a reflection attack, explain how the attack functions, and give general principles that allow you to insure that a reflection attack is impossible.

8. Explain Needham-Schroeder. Explain the purpose of the various nonces.

9. Explain the scheme that Kerberos uses for mutual authentication of Alice and Bob.

10. Explain how SSL insures that Alice is truly talking to Bob.com.
11. Why does IPSec have problems with NAT-ing?

12. What is message flow confidentiality and how can it be achieved?

13. Why does S-MIME use base 64 encoding before applying cryptographic functions to the data it sends?