EECS 563
Homework 13

1. Explain the differences among the security goals of confidentiality, integrity and availability.
2. A KDC is designed to solve the problem of distributing i) symmetric, ii) public or iii) private keys. Select i) symmetric, ii) public, iii) private.
3. A CA is designed to solve the problem of distributing i) symmetric, ii) public or iii) private keys. Select i) symmetric, ii) public, iii) private.
4. Encryption protects a network from all types of security attacks. True or False.
5. A department of 20 people needs to communicate securely, if they use a symmetric key system how many keys are needed? As the number of people increases what are some problems with distribution of symmetric keys. How are symmetric keys distributed?
6. In public key systems all keys are publicly available. True or False.
7. For a digital signature the sender uses which of the following keys create the cipher text:
    a. The senders own symmetric key
    b. The senders own private key
    c. The senders own public key
    d. The receiver's private key.
8. What is the role of the hash function in digital signature?
9. What system component functions as the trusted third party in symmetric key systems.
10. What certifies the binding between a public key and its owner?
    a. CA
    b. KDC
    c. Hash
    d. Digital signature
11. In IPSec what is the difference between transport and tunnel modes?
12. What layer of the protocol stack is secured by SSL?
13. Suppose a directory that stores certificates is broken into and the certificates in the directory are replaced by bogus certificates (but the CA's private key is not disclosed)? Explain why users will still be able to identify these certificates as bogus.
14. View a certificate used by your browser. For example in Firefox, go to Options-->Privacy & Security (Scroll down) click on View Certificates, then under the Servers tab double click on any Certificate in the list.
    a. Certificate Name
    b. Who issued the certificate?
    c. Who was the certificate issued to?
    d. When does the certificate expire? Why do certificates expire?

15. Read “Spectre, Meltdown and More: What You Need to Know About Hardware Vulnerabilities”, March 12, 2019 By Charles DeBeck https://securityintelligence.com/spectre-meltdown-and-more-what-you-need-to-know-about-hardware-vulnerabilities/ What does Spectre and Meltdown leverage to create a security vulnerability, i.e., to gain access to sensitive data that would otherwise reside in a device’s protected memory?

16. Read “Trying to Keep Your E-Mails Secret When the C.I.A. Chief Couldn't” by Nicole Perlroth, November 16, 2012, New York Times.

a. What was the role of hotel WiFi networks in finding Ms. Broadwell’s computer?
b. What is Tor?
c. What is Wickr?
d. Would you do personal financial transaction over a hotel WiFi network, Yes or No?