

**Network Security with Symmetric Key Cryptography, Key Distribution, and Public Key Authenticity**

Please note: handouts *will not* be collected and graded. However, *you are expected to complete them*. The material on the handouts is a fair game for exams, quizzes, and assignments. It is in your best interest to use handouts during lectures. The instructor will be happy to assist you.

1. **Interview Question:** Analyze advantages and disadvantages of different encryption placement strategies.
  
  
  
  
  
  
  
  
  
  
2. **Interview Question:** What sort of applications would most benefit most end-to-end encryption?
  
  
  
  
  
  
  
  
  
  
3. **Interview Question:** What sort of applications would most benefit from link encryption?
  
  
  
  
  
  
  
  
  
  
4. **Interview Question:** Explain the basic approach for defeating traffic analysis.
  
  
  
  
  
  
  
  
  
  
5. **Interview Question:** What is key distribution? Why is it important?
  
  
  
  
  
  
  
  
  
  
6. **Interview Question:** What are the three common ways of distributing an encryption key? Analyze the advantages and disadvantages of each approach.

- 7. Interview Question:** Consider a network with  $n$  users. Each user wants to be able to securely communicate with all other users using symmetric encryption. How many symmetric keys are needed? How many symmetric keys are needed if a key distribution authority (KDC) scheme is used where each user shares a unique master key with the KDC?
- 8. Interview Question:** Explain each step of the key Needham-Schroeder Symmetric Key distribution scenario discussed in class. Be sure to address the importance of each step.
- 9.** Explain the attack against the Needham-Schroeder Symmetric Key protocol. According to ITU-T X.800 is this an active or passive attack? What is the name of the attack?
- 10.** What is Kerberos? Explain ways in which Kerberos is similar to Needham-Schroeder.
- 11.** Explain the basic flow of Kerberos authentication.
- 12.** Describe the basic problem that must be addressed when distributing public keys?
- 13.** Explain the Public Announcement approach to distributing public keys. What are its advantages and disadvantages?

14. Explain the Public Key Authority approach to distributing public keys. What are its advantages and disadvantages?
15. Explain the Public Key Certificates approach to distributing public keys. What are its advantages and disadvantages?
16. What is the X.509 Certificate? Where is it used. Explain the fields of the certificate.
17. What is the difference between V1, V2, and V3 versions of the X.509 certificate?
18. Describe the fields of the X.509 certificate.
19. Generate an X.509 certificate in Linux and Windows.

Diffie-Hellman related stuff

20. Compute the following Euler Totients:
  - (a)  $\phi(31)$
  - (b)  $\phi(247)$

(c)  $\phi(16)$

(d)  $\phi(81)$

**21.** Show that if  $p$  and  $q$  are primes, then  $\phi(pq) = \phi(p) * \phi(q)$ .

**22.** Consider a Diffie-Hellman scheme using prime number  $q = 11$  and number  $\alpha = 2$  the primitive root of  $q$ .

(a) Show that 2 is a primitive root of 11.

(b) Suppose user A chooses private key  $X_A = 9$ . Illustrate how A computes his public key  $Y_A$ .

(c) Suppose user B chooses private key  $X_B = 3$ . Illustrate how B computes his public key  $Y_B$ .

(d) Illustrate how A computes the shared symmetric key  $K$ .

(e) Illustrate how B computes the shared symmetric key  $K$ .

- (f) Illustrate how attacker  $E$  can execute a man-in-the middle attack against A and B.
- 23.** Now please repeat the previous problem when: Alice and Bob get public numbers  $a = 9$ ,  $q = 29$ , Alice chooses private key  $X_A = 4$  and Bob chooses private key  $X_B = 5$ .
- 24.** Consider a Diffie-Hellman scheme using prime number  $a = 2$  and number  $q = 11$  the primitive root of  $q$ . Choose proper private keys, compute the public keys, and compute the shared key.
- 25.** Now please repeat the previous problem when: Alice and Bob get public numbers  $a = 9$ ,  $q = 29$ , Alice chooses private key  $X_A = 4$  and Bob chooses private key  $X_B = 41$ .
- 26.** Compare and contrast the different key distribution schemes discussed in class.
- 27.** Explain how to execute a man-in-the middle attack against the simple key distribution scheme discussed in class.