Coving 2024					
Spring 2024 CS-352 Na	Tame:				
Network Security with Symmetric Key Cryptography, Key Distribution, and Plic Key Authenticity Please note: handouts will not be collected and graded. However, you are expected to compethem. The material on the handouts is a fair game for exams, quizzes, and assignments. It your best interest to use handouts during lectures. The instructor will be happy to assist y					
1. Interview Question: Analyze advantategies.	vantages and disadvantages of different encryption	n place-			
2. Interview Question: What sort of cryption?	of applications would most benefit most end-to-o	end en-			
3. Interview Question: What sort of	of applications would most benefit from link encry	yption?			
4. Interview Question: Explain the	basic approach for defeating traffic analysis.				

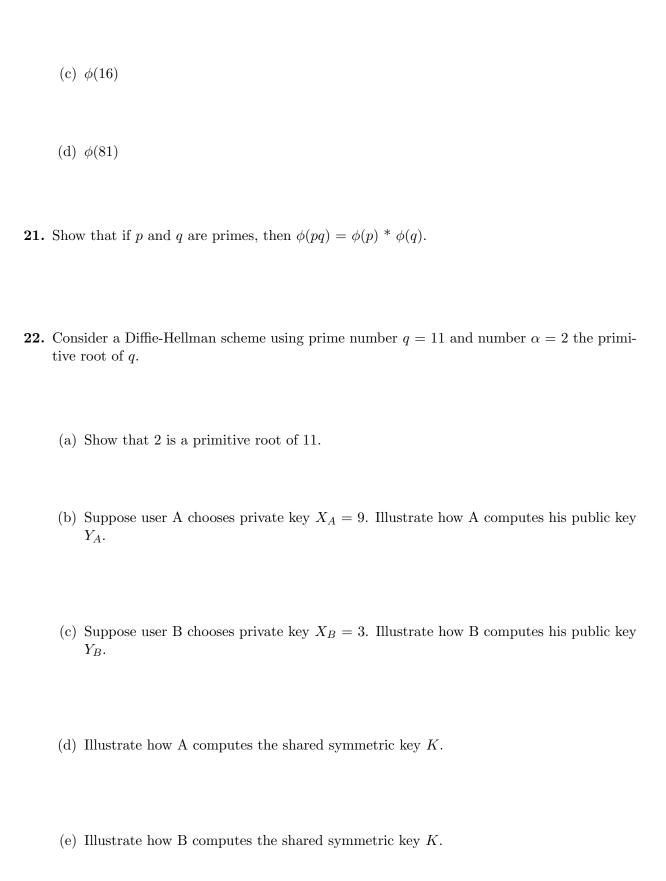
**6. Interview Question:** What are the three common ways of distributing an encryption key?

**5. Interview Question:** What is key distribution? Why is it important?

Analyze the advantages and disadvantages of each approach.

7.	<b>Interview Question:</b> 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.	<b>Interview Question:</b> 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 disadvangates?

14.	Explain the Public Key Authority approach to distributing public keys. What are its advantages and disadvangates?
15.	Explain the Public Key Certificates approach to distributing public keys. What are its advantages and disadvangates?
	What is the X.509 Certificate? Where is it used. Explain the fields of the certificate. 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.
20.	Diffie-Hellman related stuff Compute the following Euler Totients: (a) $\phi(31)$
	(b) $\phi(247)$



(f)	Illustrate how	${\rm attacker}$	$E \operatorname{can}$	execute a	man-in-the	middle	attack	${\it against}$	A	and	В.
-----	----------------	------------------	------------------------	-----------	------------	--------	--------	-----------------	---	-----	----

- 23. Now please repeat the previous problem when: Alice and Bob get public numbers a=9, q=29, Alice choses 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 choses 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.