United International **University**

Department of Computer Science and Engineering

Final Exam, Summer2023

CSE 4531: COMPUTER SECURITY

Total Marks: 40 Duration: 2 Hours

Any examinee found adopting unfair means will be expelled from the trimester/program as per UIU disciplinary rules.

Answer all the questions.

1.	**(a)**	You have received the following email from the Help Desk: *Dear UIU Email User,* *Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.* **Name (first and last):* **Email Login:* **Password:* **Date of birth:* **Alternate email:* *Please contact the Webmail Team with any questions. Thank you for your immediate attention.* Identify what type of attack it is and justify your answer.	[2]
	(b)	A central authority is assigned the task of key generation for the RSA scheme. This authority decided to use the same n (i.e., the modulus) for generating keys for Alice and Bob. What are the potential problems with this approach?	[2]
	(c)	Suppose Alice wants to establish a shared secret session key with Bob over an insecure network. Both Alice and Bob are registered with a Key Distribution Center (KDC. Answer the following questions with explanation: i. Assuming that Alice is the initiator of a session key request to KDC, when Alice receives a response from KDC, how can Alice be sure that the **sending party for the response is indeed the KDC**? ii. Assuming that Alice is the initiator of a communication link with Bob, how does Bob know that **some other party is not masquerading as Alice**? iii. Why does Bob get assured that the session key Bob has received through Alice is **protected from eavesdropping/interception**?	[6]
2.	**(a)**	Let p = 13; q = 7; e = 9; m = 10 be the values for **RSA encryption/decryption algorithm**. Show the **Key generation** and **Encryption** steps, i.e., generate the keys and encrypt the message m = 10 with the keys to create a ***ciphertext***. **Also**, show the steps to demonstrate that you can successfully **decrypt** the ciphertext.	[3]
	(b)	Consider the **Diffie-Hellman key exchange protocol** where q is a prime number and α is primitive root mod q. Can 5 be an appropriate value for α if q = 23? Show calculation behind your opinion.	[2]

	(c)	Suppose Host A and Host B are using a platform to setup secure session between them, and they apply the **Diffie-Hellman key exchange protocol** with the following parameters: • Public parameters: modulus p = 19, base g = 10 (primitive root modulo p) • Private key of A: 3, Private key of B: 7 Generate the shared secret key between Host A and Host B	[3]
	(d)	Calculate the following big moduli: i. $13^{503}\ mod\ 15$ ii. $5^{425}\ mod\ 11$	[2]
	(e)	Which of the following would provide the strongest encryption? i. Random one-time pad ii. RSA with a 1024-bit key Explain your answer.	[2]
	(f)	How are one-way hash functions typically used in conjunction with public-key signature schemes, and why?	[2]
3.	**(a)**	What purpose does the authenticator in a Kerberos message serve? Explain briefly.	[1]
	(b)	Assume a public key distribution scheme where the user broadcasts s/her own public key to the other users. Are there any potential problems with this method? If yes, explain how this method ensures the distribution of the public key without being forged. Otherwise, devise a method where the public keys can be shared without forgery.	[3]
	(c)	A Kerberos realm consists of a KDC, a TGS, a number of clients sharing keys with the KDC, and a number of application servers sharing keys with the TGS. In cross-realm authentication, a client in one realm wishes to use a server in another realm. Explain briefly how Kerberos is used in cross-realm authentication (across two realms) and state what key(s) must be shared between the two realms.	[4]
	(d)	Suppose Alice wants to send a message to Bob containing her name *N*, her computer's IP address *IP*, and a request *R* for Bob. Different cryptographic approaches can be used by Alice and Bob. For describing the approaches, the following terminologies are used:	[8]

M	Plaintext Message
SHA	Hash Function
MAC	Message Authentication Code
PK_A	Public Key of Alice
SK_A	Corresponding Private Key of Alice
PK_B	Public Key of Bob
SK_B	Corresponding Private Key of Bob
K	Shared Symmetric Key in between Alice and Bob
E_{PK}	Encryption using RSA with the public key
D_{SK}	Decryption using RSA with the private key SK
$Sign_{SK}$	Signature using RSA with private key SK

i. Using the **symmetric key**, design a message that enables Bob to **verify** that the message's **integrity** has not been violated **and** that it is **from Alice**.

ii. Using **public key cryptography**, design a message that enables Bob to **verify** that the message's **integrity** has not been violated and that it is **from Alice**.

iii. Using **public key cryptography**, design a message that protects the **confidentiality** of the request only and ensures that Bob can **verify** the **message's integrity** and **source**.

iv. **Explain** the advantages of using public key cryptography over symmetric key cryptography.