United International **University**

Department of Computer Science and Engineering

Final Exam, Spring2023

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) During the 2008 U.S. Presidential campaign, hackers were able to gain access to an email account of Vice-Presidential candidate, Sarah Palin. Their attack is said to have involved tricking the mail system into resetting Governor Palin's password, claiming they were really Palin and had forgotten this password. The system asked the hackers a number of personal questions regarding Palin's identity, including her birthday, zip code, and a personal security question— "Where did you meet your spouse?"—all of which the hackers were able to answer using data available on the Internet. What kind of attack is this an example of? How to prevent such occurrences from happening? [3]

(b) Assume an employee-management system that requires a strong password to login to prevent the hacker from predicting the password. Inside the system, a user is allowed to only access what s/he is supposed to access. For example, regular employees can see their own salary information, payslip, schedule, missed offices, etc. The HR department can see the attendance of all the employees while the Accounts department can access the salary and payslips of other employees. There is also an AI that monitors user behavior and blocks any malicious user that tries to exploit the system. Is this system foolproof? Analyze the system with respect to Breach Quadrilateral to find the scopes where more security measures can be employed. If you think the system is secure, explain how it would handle all four stages of an attack. [4]

(c) Analyze the following function and determine whether it is a vulnerable hash function or not. [3]

$$f(x) = (9x+3) \bmod 7$$

2. (a) Design a process to show that public key cryptography can be used to achieve both message confidentiality and message authentication at the same time. Explain your process clearly. [3]

(b) To verify a certificate, we need a Certification Authority. Alice wants to send an encrypted message to Bob. Suddenly, the CA gets down. Do you think Alice can establish a secure connection without the supervision of CA if Bob has a certificate? How should Alice verify the certificate? [2]

(c) Suppose Alice wants to send a message M to Bob. Different cryptographic approaches can be used by Alice and Bob. For describing the approaches, the following terminologies are used: [4]

M	Plaintext Message
SHA	Hash Function
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
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

		Let us consider that Alice and Bob want their communication to achieve the following security properties: **Integrity, Confidentiality, and Non-Repudiation**. For each of the following approaches, identify which property/properties will hold in the presence of Malice, a Man-In-The-Middle attacker. i. Alice sends to Bob: $E_{PKA}(M), Sign_{SKA}(SHA(M))$ ii. Alice sends to Bob: $E_{PKB}(M), Sign_{SKA}(SHA(M))$ Write *NONE* if none of the properties are achieved. Write the name of the property/properties if any/all are achieved. Justify your answer. If your answer is *NONE*, suggest how the properties can be achieved.	
	(d)	In the Internet web security architecture, a session key is established between a client and the server after the client successfully verifies the server's certificate. A *nonce* is used during the session key establishment phase. Why?	[1]
3.	(a)	Let p = 17; q = 13; e = 25; m = 11 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 = 11** with the keys to generate a ***ciphertext***. Also, show the steps to demonstrate that you can successfully decrypt the ciphertext.	[4]
	(b)	Calculate the following big moduli: i. $11^{356} \ mod \ 35$ ii. $7^{521} \ mod \ 17$	[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 = 29, base g = 5 (primitive root modulo p) • Private key of A: 12, Private key of B: 22 Generate the shared secret key between Host A and Host B	[2]
	(d)	You are part of a team designing a new voting system for an upcoming election. The system needs to be secure against various types of attacks, including hacking and tampering. One option is to use a cryptographic system with unconditional security, while the other option is to use a system that provides computational security. Which approach would you recommend for this system? Justify your answer.	[2]
4.	(a)	"MAC, if used properly, provides both confidentiality and integrity." Is the statement True or False? Justify your answer.	[2]
	(b)	Suppose you have deployed Kerberos in your system. Answer the following questions: i. Why does a client need to send an authenticator to TGS to obtain a service ticket? ii. Suppose a user under your Kerberos wants a secure connection with a fileserver under another Kerberos. 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]
	(c)	If Alice needs to get Bob's Public Key, she may find that a CA issued a certificate for Bob. But Alice does not know that CA. How can Alice be sure that the certified Public Key belongs to Bob, not to Eve (an eavesdropper)?	[2]
	(d)	How does a gateway router decide if an outgoing packet should be encrypted using IPsec? How does it decide which Security Association to use if it does require encryption?	[2]