United International **University**

Department of Computer Science and Engineering

Final Exam, Spring2024

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) Suppose you just got a call from the University System Administrator, who says that he has checked the network configurations and traffic and finds that you are flooding the varsity BSCSE results website with excessive requests to overload the system so that other students cannot access the portal and resources. (i) **Which attack are you supposed to conduct?** However, you know you are not doing this, rather, someone is using your network credentials, such as IP or MAC address. (ii) **In this case, which attack are you facing?** (iii) Among *interruption*, *interception*, *modification*, and *fabrication*, **in which categories do these two attacks lie**? In each part, justify your answer with short explanations. [1+1+2=4]

   (b) Analyze the following function according to the three main properties of a cryptographic hash function and determine whether the function is vulnerable or not. [3]

$$f(x) = \frac{|x|}{x}$$

   (c) Write one major similarity and one major difference between MAC and hash function. [2]

   (d) Can we use a digital signature scheme and public-key/asymmetric encryption-decryption technique together? What will be the benefit or loss of it? - Explain your answer using a block diagram. [3]

   (e) Assume an employee-management system that requires a strong password to log in to prevent the hacker from predicting the password. Inside the system, a user is allowed to access only what s/he is supposed to access. For example, regular employees can see their salary information, payslips, schedules, 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 **The 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. [3]

2. (a) Alice is implementing the RSA cryptosystem for secure communication. She selects a prime p=11 and q = 17. Alice then picks a public key e=5. However, during the computation of the private key (d), Alice encounters an unexpected issue. Identify the value that Alice has chosen incorrectly and explain why it does not meet the properties required for a secure RSA implementation in this scenario. [4]

(b) Find the smallest non-prime primitive root of 17. [3]

(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: [4]

- Public parameters: modulus p = 13, base g = 11 (primitive root modulo p)
- Private key of A: 10, Private key of B: 9

Generate the shared secret key between Host A and Host B. Then explain how the presence of an eavesdropper does not compromise the security of the key exchange.

(d) Does the number 8 have a multiplicative inverse in Z_{11}? If yes, then find the multiplicative inverse. [2]

(e) Which of the following would provide the strongest encryption? [2]

i. Random one-time pad

ii. RSA with a 1024-bit key

Explain your answer.

3. (a) 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: [3*2=6]

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**?

(b) For a Certification Authority, we need a Trusted Center. Alice wants to send an encrypted message to Bob using RSA. Suddenly, the Trusted Center gets down. *What will happen?* [2]

(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]