United International University

Department of Computer Science and Engineering

Final Exam, Fall2023

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.

<table>
<tr><td>1.</td><td>(a)</td><td>A multinational financial services corporation recently faced an incident that impacted both its online services and compromised sensitive customer information. The incident involved a simultaneous disruption of online operations and unauthorized access to confidential client data. Investigate the incident and identify the types of attacks the company encountered. Also, suggest how these incidents can be prevented.</td><td>[3]</td></tr>
<tr><td></td><td>(b)</td><td>Consider the following hash function and prove that it violates every property of a secure hash function.
$$f(x) = x^4 - 2x^2 - 8$$</td><td>[3]</td></tr>
<tr><td></td><td>(c)</td><td>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:
<table>
<tr><td>M</td><td>Plaintext Message</td></tr>
<tr><td>SHA</td><td>Hash Function</td></tr>
<tr><td>MAC</td><td>Message Authentication Code</td></tr>
<tr><td>PK_A</td><td>Public Key of Alice</td></tr>
<tr><td>SK_A</td><td>Corresponding Private Key of Alice</td></tr>
<tr><td>PK_B</td><td>Public Key of Bob</td></tr>
<tr><td>SK_B</td><td>Corresponding Private Key of Bob</td></tr>
<tr><td>K</td><td>Shared Symmetric Key in between Alice and Bob</td></tr>
<tr><td>E_{PK}</td><td>Encryption using RSA with the public key</td></tr>
<tr><td>D_{SK}</td><td>Decryption using RSA with the private key SK</td></tr>
<tr><td>$Sign_{SK}$</td><td>Signature using RSA with private key SK</td></tr>
</table>
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: M, $MAC(M)$
ii. Alice sends to Bob: $E_{PKB}(M)$, $Sign_{SKA}(SHA(M))$
iii. Alice sends to Bob: M, $E_{PKB}(M)$
iv. Alice sends to Bob: $K(M)$, $Sign_{SKA}(SHA(MAC(M)))$
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.</td><td>[8]</td></tr>
</table>

2.	(a)	Let P and Q be two prime numbers. Given P = 5 and Q = 7, and the public key e = 3. If the original message is 0001011, what will be the ciphertext value and private key value according to the RSA algorithm? Also, calculate the plaintext value from the ciphertext.	[4]
	(b)	Hosts Alice and Bob are setting up a secure communication channel using the Diffie-Hellman key exchange protocol. They choose the following parameters: Public parameters: modulus p=29, base g=3 (primitive root modulo p) Private key of Alice: a=5 Private key of Bob: b=11 Now, imagine an eavesdropper, Eve, who intercepts the public communication but cannot directly compute discrete logarithms. Determine the shared secret key between Alice and Bob, and explain how the presence of Eve does not compromise the security of the key exchange.	[3]
	(c)	Alice is implementing the ElGamal cryptosystem for secure communication. She selects a prime p=13 and chooses a g=3 to serve as a primitive element modulo p. Alice then picks a private key x=4 within the range of 1 to p−1. However, during the computation of the public key (y), 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 ElGamal implementation in this scenario.	[3]
	(d)	Suppose p is a prime number, and a is an integer not divisible by p. According to Fermat's Little Theorem, if p=31 and a=4, Calculate $a^{p-1} \, mod \, p$ and verify the theorem's statement.	[2]
	(e)	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]
3.	(a)	Assume a public key distribution scheme where the user broadcasts his/her own public key to the other users. Explain any potential issues this method might create and devise a method where the public keys can be shared without forgery.	[3]
	(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)	Explain the Kerberos authentication process for Alice accessing a network service, covering the steps from her initial request for a TGT to gaining access. Highlight the roles of long-term and short-term keys, the Ticket Granting Service (TGS), and the network service in this authentication flow.	[4]
	(d)	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.	[3]