ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION
DURATION: 3 HOURS

WINTER SEMESTER, 2022-2023
FULL MARKS: 150

CSE 4743: Cryptography and Network Security

Programmable calculators are not allowed. Do not write anything on the question paper.
Answer **all 7 (seven)** questions. Figures in the right margin indicate full marks of questions whereas corresponding CO and PO are written within parentheses.

---

1. a) Password-guessing attacks, such as dictionary attacks, can be more or less effective, depending on how users pick their passwords and how the attacks are launched. — 3 × 4 (CO1) (PO1)
   i. Adding salt to the UNIX password database is an attempt to make password-guessing attacks less effective in cases where the attacker has access to the database. Discuss what kind of attacks the salt can help against. Are there attacks where the salt does not help?
   ii. Consider that the salts are only 12 bits. If we would make the salt larger (say 64 bits), would that make the above attacks more difficult? Discuss what kind of attacks this could help against and what attacks it might not help against.
   iii. Organizations with strict security often enforce password policies to make password management more secure. What could such policies be? Give examples. Discuss the ways in which strict password policies may actually make password management less secure.

   b) In modern times, there are many techniques used to strengthen passwords. Discuss two modern techniques. — 2 × 2 (CO1) (PO1)

2. a) Describe the mechanism of Merkle-Damgard Scheme and analyze how it can be used for SHA-2. — 8 (CO5) (PO1)

   b) Based on the structure of SHA-512, identify why it has better collision resistance capabilities. — 7 (CO5) (PO1)

3. a) A trusted third party can be used for central key management in a shared-key authentication protocol. Such a protocol is usually successful in some ways but has many steps. Identify a protocol necessary for successful key sharing with step-by-step reasoning. Discuss an alternative approach with fewer steps. — 10+5 (CO4) (PO2)

   b) The network in Question 3.a) is insecure, so sensitive information cannot be sent. Analyze the scenario to suggest another approach where clients and services mutually authenticate themselves and secret keys are shared. — 8 (CO4) (PO2)

4. a) Explain the necessity of each of the four phases of the Secure Socket Layer (SSL) Handshaking Protocol. — 8 (CO5) (PO1)

   b) Compare the SSL Handshake Protocol with the Transport Layer Security (TLS) 1.3 Handshake. — 5 (CO5) (PO1)

c) SSL is used for security and authentication in websites, emails and many other services. However, there are some challenges SSL faces due to its inherent characteristics which is why TLS is necessary. Explain those challenges in short. (C (PO

5. a) Barbie and Ken want to communicate through an insecure channel, keeping the computational expense minimal. They do not have any prior shared secrets. In this channel, 13 is a *prime number* and 4 is a *shared integer number*. These two numbers are known to everyone. There is no third party for central key management.

i. They want to conduct secure communication in this channel. Suggest a key-sharing algorithm with proper justification. 5 (CO2) (PO2)

ii. Mathematically show how the key is established with an example. You may use suitable numbers, if necessary. 7 (CO4) (PO1)

b) The IPSec IKE Phase–I exchanges keys via the Diffie-Hellman technique. However, this technique is susceptible to the Man-In-The-Middle (MITM) attack as illustrated in Figure 1. Now, answer the following questions:

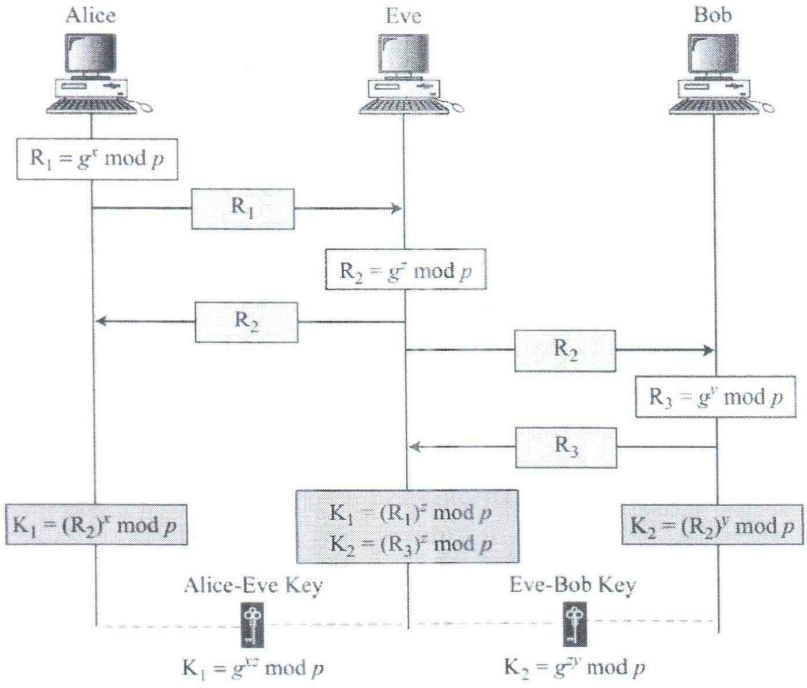

Figure 1: MITM Attack in IKE Phase – I for Question 5.b)

i. Explain how the MITM attack launched by Eve can be prevented. 4 (CO5) (PO1)

ii. Suppose Eve launches another attack by sending several half-keys to Bob (Server), masquerading herself as if these keys are from multiple sources. Determine with appropriate diagrams how this attack can be prevented. 9 (CO5) (PO2)

c) Perform a comparative analysis of the modes of operations which are used in the Authentication Header in IPSec. 6 (CO5) (PO1)

a) Military Bob wants to communicate with his base. The military has a secret language where large events can be described using a few letters. Their maximum length for any message is 200 Bytes. They want to use a public-key cryptosystem with two types of keys. Analyze the scenario to suggest a cryptography technique that could work for Bob. Also, explain the working mechanism of that technique in his case. 5 + 5 (CO4) (PO2)

b) Frank Underwood is trying to communicate with Doug Stamper using encryption techniques. Now, answer the following questions to help Frank encrypt the messages properly:

i. Frank is building a monoalphabetic cipher using Caesar Cipher, and then its output is an input for Multiplicative Cipher. He decides to use the same key of $K = 17$ for both the cyphers. Calculate the ciphertext if the plaintext is: `life is overrated`. 6 (CO2) (PO1)

ii. While Frank is very happy with his simple cipher, it is getting decrypted easily by his arch-nemesis, Claire. So, he tries to analyze the issues with his technique. Identify the drawbacks of the Cipher used by Frank in order to keep his messages private and secure. 4 (CO2) (PO1)

iii. Frank decides to add one more layer of Cipher. The ciphertext he gets in the previous case will be the key stream for his Vigenere Cipher. What should be the ciphertext with this new technique if his input plaintext is: `friends make the worst enemies.` 6 (CO2) (PO1)

iv. Frank needs to send a video to Doug. So, he needs a new technique to encrypt his message. Suggest an appropriate technique for Frank and discuss how he can implement it. 4 (CO3) (PO2)

7. It is important to know which entity is responsible for what activities in a secured system. Identify the entities and write short notes based on the following actions: 6 × 2 (CO1) (PO1)

i. A trusted third party that issues digital secure socket layer certificates binding public key to an identity.

ii. Tool(s) to sign and verify message signatures to provide proof of authenticity.

iii. A single key used for both encryption and decryption.

iv. A third party for maintaining a key with whom each node shares a single key.

v. A suite of protocols for securing Internet Protocol (IP) communications.

vi. An SSL protocol used for reporting errors and abnormal conditions.