Name of the Program: B.Sc. in Computer Science Engineering **Date: 12 September, 2021**
Semester: Winter 2020-2021 **Time: 2:30 pm – 4:00 pm**

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)
ORGANISATION OF ISLAMIC COOPERATION (OIC)
DEPARTMENT OF MECHANICAL ENGINEERING (ME)

FINAL Semester Examination **Winter Semester: 2020 – 2021**
Course Number: CSE 4743 **Full Marks: 75**
Course Title: Cryptography and Network Security **Time: 1.5 Hours**

Programmable calculators are not allowed. Do not write anything on the question paper.
There are **3 (three)** sets of questions. Answer all **3 (three)** of them.
Marks of each question and corresponding CO and PO are written in brackets.

---

1. a) Explain the working process of a Digital Signature with necessary diagram. Analyze the security services that this mechanism provides. (10) (CO4) (PO1, PO2)

   b) Alice wants to use RSA to encrypt the message M=43 and send it to Bob. Bob has chosen two prime numbers (p=5 and q=11) to calculate the public number needed for the RSA keys. Furthermore, Bob has selected the number e=3 to use in his public key. (4+4) (CO4) (PO1, PO3)

      i) What is the resulting private key and public key published by Bob?
      ii) What is the resulting ciphertext block C that Alice with send to Bob using RSA to encrypt her message (M=43)?

   c) Why is the Diffie-Hellman key exchange strategy susceptible to Man-in-the-Middle attack (MITM)? Describe how can this issue be resolved. (7) (CO4) (PO1, PO2)

2. a) Kerberos is a protocol that is based around Needham-Schroeder protocol for many to many authentications. Now answer the following questions. (Use necessary diagrams to justify your answers) (3+4+5) (CO4) (PO1, PO2)

      i) Explain why the password of the user is not sent over the network and instead session keys are generated and shared in the Kerberos protocol.
      ii) The information in a TGT (Ticket Granting Ticket) is encrypted so the client cannot access the information in the TGT. However, all information in the ticket is already known to the client. Why is it still necessary to encrypt it?
      iii) Describe the working mechanism of how a ticket is generated between the client and server by the TGS (Ticket Granting Server) and how it is used for client-server communication.

   b) A secure hash function gives a condensed version of a message (it is a "lossy" compression function). (3x3) (CO5) (PO1, PO2, PO6)

      i) What are the most important properties of a secure hash function for message authentication?
      ii) Why do MD5 and SHA-1 require padding of messages that are already a multiple of 512 bits?
      iii) Why are "salts" normally used with hash function when storing passwords in databases?

2. c) "Using either IPsec or SSL/TLS will give users complete security over the internet." – Justify this statement. (4) (CO5) (PO1, PO2, PO6)

3 a) The IPsec specification defines two modes of applying IPsec protection to a packet. (2+5+2) (CO5) (PO1, PO2, PO6)

i) What are the two modes?

ii) Sketch what an IP packet looks like after IPsec protection in the two different modes. You only need to show payload and the different headers (not the individual header fields).

iii) Why can't AH all fields of an IP header be included in the AH's end-to-end integrity check?

b) IKE (Internet Key Exchange) is a protocol for doing mutual authentication and establishing a shared secret key to create an IPsec security association (SA). (3x2) (CO5) (PO1, PO2, PO6)

i) Why are there two phases in IKE?

ii) Why does IKE use cookies and nonces?

c) Describe the TLS handshake protocol with appropriate diagrams. Explain how Perfect Forward Secrecy is implemented in TLS and what happens in the event of an attack. (6+4) (CO5) (PO1, PO2, PO6)