Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF COMPUTER NETWORKING AND SECURITY

CNS 3103: CRYPTOGRAPHY II

END OF SEMESTER EXAM

Date: 4th August 2023 **Time:** 2 Hours

Instructions:

1. This Examination consists of **FIVE** questions.
2. Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question 1 (30 Marks)

a) Explain the concept of homomorphic encryption and provide an example of its application in a real-world scenario. Discuss the advantages and challenges of using homomorphic encryption in cloud computing environments. **(6 Marks)**

b) Describe the principles of quantum cryptography and explain how it ensures secure communication. Discuss the potential impact of quantum computers on traditional cryptographic algorithms and the need for quantum-resistant cryptography. **(4 Marks)**

c) Define the concepts of authentication, authorization, and accounting (AAA) in the context of access controls. Discuss the role of access control models (e.g., discretionary, mandatory, role-based) in ensuring information security. **(6 Marks)**

d) Compare and contrast PGP and S/MIME in terms of their encryption mechanisms and applications. Explain how PGP and S/MIME can be used to secure email communication and provide end-to-end encryption. **(6 Marks)**

e) Describe the purpose and functionality of SSL and TLS protocols in securing web communications. Discuss the differences between SSL and TLS and their respective versions, highlighting their evolution and security enhancements. **(4 Marks)**

f) Explain the components and roles of a PKI system in establishing a secure communication environment. Discuss the challenges and potential vulnerabilities associated with managing and maintaining a PKI infrastructure. **(4 Marks)**

Question 2 (15 Marks)

a) Explain how you can key exchange be achieved using symmetric key cryptography? **(5 Marks)**

b) Explain the Man-In-The-Middle Attack as it applies to public key exchanges. **(5 Marks)**

c) Describe how you may foil the Man-in-the-middle attack using digital signatures. **(5 Marks)**

Question 3 (15 Marks)

Consider a scenario where a company wants to establish secure communication between its employees and a centralized authentication server. Discuss the following cryptographic protocols: Kerberos, Needham-Schroeder, Yahalom, Neuman-Stubblebine, Wide-Mouth Frog, Otway-Rees, and Yahalom. Evaluate their suitability for the given scenario and explain how each protocol can be applied to achieve secure communication and authentication. Highlight the key steps, entities involved, and any potential vulnerabilities or limitations of each protocol.

Question 4 (15 Marks)

a) Discuss the **secret splitting protocol** between any 2 entities. **(4 Marks)**

b) Compare and contrast symmetric cryptography and public key cryptography in the context of cryptographic key exchange. Discuss the advantages and disadvantages of each approach, including considerations such as key distribution, computational overhead, and security. Provide scenarios where each approach is more suitable. **(6 Marks)**

c) Describe the concept of a man-in-the-middle attack in the context of cryptographic key exchange. Explain how this attack can compromise the security of symmetric key exchange and public key exchange protocols. **(5 Marks)**

Question 5 (15 Marks)

a) Explain the concept of a zero-knowledge proof and how it ensures confidentiality while proving the validity of a statement. Provide a real-world example where a zero-knowledge proof could be applied. **(6 Marks)**

b) The Fiat-Shamir identification protocol is a widely used zero-knowledge protocol. Describe a specific real-world example where it could be used to enhance privacy and security. Provide a detailed explanation of how the protocol would be applied in this scenario, including the roles of the entities involved and the steps of the protocol. Discuss the advantages and potential limitations of using the Fiat-Shamir identification protocol in this context. **(9 marks)**