Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF COMPUTER NETWORKING AND SECURITY

CNS 3103: CRYPTOGRAPHY II

END OF SEMESTER EXAM

Date: 5th December 2022 **Time:** 2 Hours

Instructions:

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

Question 1 (20 Marks)

a) Explain how digital signatures work **(6 Marks)**

b) Determining who an entity is consists of two separate steps: identification and authentication. Differentiate between the two steps. Give examples of how you may achieve each. **(2 Marks)**

c) What are rainbow tables? How can they be used in password attacks? **(2 Marks)**

d) Scrambled passwords have another vulnerability. If 2 users have the same password, the password hashes will be the same. What control can mitigate an attack leveraging this vulnerability? **(2 Marks)**

e) Using a sketch, explain the SSL Architecture. **(8 Marks)**

Question 2 (20 Marks)

a) The security of signatures and encryption operations depend on TWO factors. Explain how **Public Key Infrastructure (PKI)** may help in this case. **(2 Marks)**

b) Explain the concept of **digital certificates** as used by PKI. **(3 Marks)**

c) There are many standards that describe the way certificates are formatted. One of those standards is the X.509 standard from ITU. Discuss the X.509 standard. **(10 Marks)**

d) x.509 defines delegated server roles of Registration Authority (RA) and Validation Authority (VA). Explain the roles of these delegated server roles and the significance of this delegation. **(5 Marks)**

Question 3 (20 Marks)

a) How 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) How may you foil the Man-in-the-middle attack using: i) the interlock protocol and ii) digital signatures. **(10 Marks)**

Question 4 (20 Marks)

a) Discuss the **secret splitting protocol** between any 2 entities. **(4 Marks)**
b) b) Briefly but clearly discuss the Needham-Schroeder Protocol **(10 Marks)**
c) c) Compare and Contrast PGP versus S/MIME. **(6 Marks)**

Question 5 (20 Marks)

a) Discuss Kerberos Authentication Protocol. **(10 Marks)**
b) Explain the role of Zero Knowledge Proofs. **(2 Marks)**
c) Explain ZKP using Jean-Jacques Quisquarter and Louis Guillou cave analogy. **(6 Marks)**
d) Explain any TWO example applications of ZKP systems. **(2 Marks)**