Strathmore UNIVERSITY

SCHOOL OF COMPUTING AND ENGINEERING SCIENCES

BACHELOR OF SCIENCE IN COMPUTER NETWORKS AND SECURITY

CNS 2201: Cryptography 1

END OF SEMESTER EXAM

Date: 14th December 2022 **Time:** 2 Hours

Instructions:

This Examination consists of **FOUR** questions

Answer **Question ONE (COMPULSORY)** and any other **TWO** questions.

Question One [30 Marks]

a) Distinguish between the following (5 marks):
   i. Substitution cipher and transposition cipher
   ii. Chosen plaintext attack vs adaptive chosen plaintext attack
   iii. Symmetric cryptography vs asymmetric cryptography
   iv. Cryptology vs cryptography
   v. Confusion and diffusion (as applied to cryptography)

b) Describe two attacks against the Caesar cipher (4 marks).

c) Discuss two vulnerabilities of DES (4 marks)

d) State three differences between the CBC mode and CTR mode (3 marks)

e) Explain two shortcomings of symmetric cryptography that are addressed in public key cryptography. (4 marks)

f) Explain steps involved in Diffie-Hellman key exchange where two parties Alice and Bob are communicating. Illustrate the steps with $p = 29$, $\alpha=2$. Assume that Bob's private key is 12 and Alice's private key is 4. (5 marks). Use a diagram for illustration. (6 marks).

g) Differentiate between digital signatures, message authentication codes and hash functions. (4 marks)

Question Two [15 Marks] Distinguish between the following:

a) Distinguish between the following: (3 marks)
   i. One time pad and Vigenère Cipher
   ii. Caesar cipher and polyalphabetic cipher

b) Briefly explain the what happens under the following blocks of DES:
   i. The f-function (during encryption) (3 marks)
   ii. Reverse key schedule (3 marks)

c) Briefly explain the what happens under the following blocks of AES during encryption:
   i. Shift rows sub layer (3 marks)
   ii. Mix column sub layer (3 marks)

Question Three [15 Marks]

a) State four applications of public key cryptography (4 marks)

b) HTTPs uses a hybrid of symmetric key cryptography and asymmetric key cryptography. Explain the motivation behind this. (3 marks)

c) Alice wants to send an encrypted message to Bob. Bob first computes his RSA parameters. He chooses p and q as 3 and 5, respectively. Alice encrypts the message x = 8. Show, with calculations, the entire process of computation of public and private keys, encryption and decryption. Use a diagram for illustration. (4 marks)

d) Describe how Chinese remainder theorem can help speed up RSA cryptosystem. (4 marks)

Question Four [15 Marks]

a) Show steps involved in El Gamal encryption protocol where two parties Alice and Bob are communicating. Illustrate the steps with $p = 29$, $\alpha=2$, Bob's private key is 12 and message to be encrypted x as 26. Use a diagram for illustration. (8 marks)

b) Explain the steps involved in Diffie-Hellman key exchange with Elliptic curves. (7 marks).

Question Five [15 Marks]

a) List four requirements for a Hash function. (4 marks)

b) Write short notes on the following:

i. MD4 (2 marks)

ii. MD5 (2 marks)

c) Explain two applications of: (7 marks)

i. Digital signatures

ii. Message authentication codes.