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: 18th December 2023 **Time: 10:30-12:30 Hours**

Instructions:

This Examination consists of **FIVE** questions

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

Question One [30 Marks]

a) Distinguish between the following (5 marks):
   i. Stream cipher and block cipher
   ii. Known plaintext attack vs chosen plaintext attack
   iii. True random number generator vs pseudorandom number generator
   iv. Cryptanalysis vs cryptography
   v. Confusion and diffusion (as applied to cryptography)

b) State two disadvantages of one-time pads. (2 marks).

c) Discuss two vulnerabilities of DES (4 marks)

d) Explain the advantages of Output Feedback (OFB) mode over Cipher Feedback (CFB) mode when performing block ciphering. (2 marks)

e) Explain the two one-way functions that are applied to 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. Use a diagram for illustration. (6 marks).

g) Explain the advantages of hash functions over digital signatures. (3 marks)

h) Explain RC4 working mechanism. (4 marks)

Question Two [15 Marks]

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. Decryption in the Feistel network (3 marks)
   ii. Initial and final permutation (3 marks)

c) Briefly explain the what happens under the following blocks of AES:
   i. Inverse byte substitution layer (3 marks)
   ii. Mix column sub layer (3 marks)

Question Three [15 Marks]

a) Explain two functions that public cryptography provide but are not provided by symmetric key cryptography. (4marks)

b) 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. (7 marks)

c) Explain briefly two techniques that can be used 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 = 11, α=2, Bob's private key is 8 and message to be encrypted x as 10. Use a diagram for illustration. (8 marks)

b) Consider Elliptic Curve Diffie Hellman with the following domain parameters. The Elliptic Curve is $y^2 \equiv x^3 + 2x + 2$ which forms a cyclic group of order #E=19. The base point is P = (5,1). Assume Alice ($a = k_{pr,A}$ = 3) and Bob (($b = k_{pr,B} = 10$ = 3)) are communicating. Illustrate how joint secret will be computed and exchanged between Alice and Bob. (7 marks).

Question Five [15 Marks]

a) Explain two security requirements for Hash functions. (4 marks)

b) Explain the difference between message authentication codes and digital signatures. (2 marks)

c) Describe the working mechanism of :

   i. HMAC (3 marks)

   ii. CBC-MAC (3 marks)

d) Explain three properties of message authentication codes. (3 marks)