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: 9th December, 2024 **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) Define the following terms (5 marks):
   i. Non-repudiation
   ii. Adaptive chosen plaintext attack
   iii. Cryptographically secure pseudorandom number generator
   iv. Cryptology
   v. Confusion (as applied to cryptography)

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

c) Discuss two advantages of AES over DES (4 marks)

d) State two advantages of counter mode of 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) State three properties of message authentication codes (3 marks)

h) Explain RC4 working mechanism. (4 marks)

Question Two [15 Marks]

a) Explain two types of attack against Caesar cipher (3 marks)

b) Briefly explain the what happens under the following blocks of DES:

   i. F-function (3 marks)

   ii. Initial and final permutation (3 marks)

c) Briefly explain the what happens under the following blocks of AES:

   i. Shift rows layer (3 marks)

   ii. Inverse mix column sub layer (3 marks)

Question Three [15 Marks]

a) Explain two weaknesses of symmetric cryptography that are addressed by public 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 7, respectively. Alice encrypts the message x = 10. 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 = 13, α=3, Bob's private key is 7 and message to be encrypted x as 9. 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 (($b = k_{pr,B} = 10$)) are communicating. Illustrate how joint secret will be computed and exchanged between Alice and Bob. Table below shows computation of powers of P = (5, 1). (7 marks).

$2P = (5,1) + (5,1) = (6,3)$
$3P = 2P + P = (10,6)$
$4P = (3,1)$
$5P = (9,16)$
$6P = (16,13)$
$7P = (0,6)$
$8P = (13,7)$
$9P = (7,6)$
$10P = (7,11)$
$11P = (13,10)$
$12P = (0,11)$
$13P = (16,4)$
$14P = (9,1)$
$15P = (3,16)$
$16P = (10,11)$
$17P = (6,14)$
$18P = (5,16)$
$19P = \mathcal{O}$

Question Five [15 Marks]

a) Define the terms hash function. (2 marks)

b) Explain the importance of hash functions. (3 marks)

c) State two input-output characteristics hash functions. (4 marks)

d) Describe the working mechanism of :

   i. HMAC (3 marks)

   ii. CBC-MAC (3 marks)