Student ID:
Name:
Signature:

# COMP 417 INTRODUCTION TO CRYPTOGRAPHY

## QUIZ 1 (Total=100 points Duration:1 Hour)

## DATE: 02.11.2023 2:00 pm

**1.RSA (5*10=50 points)**

Alice and Bob want to communicate each other by using textbook RSA. They agree on p = 3 and q = 11.

a. Calculate n and totient n.

b. Create public key for Bob. Create private key for Bob.

d. Alice will send a message to Bob where m=2. Encrypt the message m=2 and send to Bob.

e. Show how Bob decrypts this message. Show the steps.

f. Which hardness assumption does RSA depend? i.e. In which cases RSA isnot breakable? Explain why. What is the minimum secure key length for RSA as of 2023?

**2. Diffie-Hellman Key Exchange (4*10=40 points)**

Alice and Bob want to communicate each other by using Diffie-Hellman Key exchange protocol. They agree on q = 17 and primitive root a= 5. If Alice's secret key is 2 and Bob's secret key is 4,

a. What is public key of Alice? What is public key of Bob?

b. Show both sides how Alice and Bob construct the shared key. What is the secret key they exchanged?

c. After they exchange the keys, how can they communicate each other? Offer one cryptographic method.

d. Which hardness assumption does Diffie-Hellman Key exchange protocol depend? Explain why.

**3. AS-S difference (10 points)**

Provide 3 main differences between symmetric cryptography and asymmetric cryptography. Explain. Give one algorithm as an example for each one.