Roll No: □□□□□□□□□

The Assam Royal Global University, Guwahati

Royal School of Information Technology

MCA, 3rd Semester

Semester End Examination, January 2023

Course Title: Cryptography and Network Security

Course Code: CAP054D306

Time: 3 Hours **Maximum Marks: 70**

Note: Attempt all questions as per instructions given.

The figures in the right-hand margin indicate marks.

Section – A

Q.1. Attempt **all questions.** **2 x 8**

a. What is symmetric cryptography?
b. What is asymmetric cryptography?
c. Differentiate between private and public key.
d. The multiplicative inverse of 5 in Z26 is ______________.
e. In asymmetric key cryptography, how many keys are required for each communicating party?
f. A _________ replicates itself by creating its own copies in order to bring the network to a halt
g. What is the value of $\Phi(10)$?
h. What are the advantages of a firewall?

Section – B

Q.2. Attempt **any one** of thc following **12 x 1**

a. If Alice wants to communicate securely with Bob, explain with example how both of them can be the victim of person in middle attack.
b. Explain different types of attack in details.

Q.3. Attempt **any two** of the following **7 x 2**

a. Explain transposition technique of encrypting a message.
b. Discuss the concept of double DES and triple DES.
c. Explain playfair cipher with example.

Q.4. Attempt **any two** of the following **7 x 2**

a. Explain the RSA algorithm in details.
b. State the capabilities and limitation of firewall.
c. Users A and B use the Diffie-Hellman key exchange technique with common prime $q = 11$, a primitive root $\alpha - 2$ and user B has private key $X_B = 8$. Show the calculation for questions below:
If user A has private key $X_A = 6$, what is A's public key Y_A?
What is B's public key Y_B?
What is the shared secret session key?

Q.5. Attempt **any two** of the following **7 x 2**

a. What are the requirements of a digital signature?
b. Explain different fields in AH Protocol.
c. Write a short note on malicious software.