RANI RASHMONI GREEN UNIVERSITY

Post Graduate Department of Computer Science

M.Sc. Semester-III Examinations 2025

Subject: Computer Science

Paper: MSCCS302 (Introduction to Cryptography)

Time: 2 Hours. Mull Mark: 40

The figures in the margin indicate full marks. Candidate are required to give their answer in their own words as far as practicable.

*Question **No.1 is compulsory** and answer any **five** from the rest.*

1. Answer the questions (any **five**):
   (a) Explain the difference between symmetric and asymmetric cryptography. **(2)**
   (b) What is message digest? **(2)**
   (c) What do you mean by hash function? **(2)**
   (d) Mention the key principles of security. **(2)**
   (e) Define : Message Authentication Code (MAC). **(2)**
   (f) What is public key infrastructure (PKI)? **(2)**
   (g) Define: Encryption and Decryption. **(2)**

2. Explain the working principle of the Vigenère Cipher with an example. **(6)**

3. What is a cryptographic key? Why is it important? What is the difference between a private key and a public key? **(2+2+2)**

4. Using the Playfair cipher, encrypt the following message:
   Keyword: CRYPTOGRAPHY,
   Plaintext: BALLOON ATTACK AT DAWN. **(6)**

5. Explain the working principle of RSA with a suitable example **(6)**

6. Explain Caesar cipher with an example. Why is substitution cipher vulnerable to frequency analysis? Encrypt the message "**HELLO**" using Caesar cipher with shift 3. **(2+2+2)**

7. How does HTTPS use both symmetric and asymmetric encryption? What are the function of certificate authority (CA). What is two-factor authentication (2FA)? **(2++2+2)**

8. Write short notes (any two): **(3+3)**

   (a) Elliptic Curve Cryptography (ECC),

   (b) Man-in-the-middle attack,

   (c) Secure Hash Algorithm(SHA),

   (d) ElGamal algorithm,

   (e) Advanced Encryption Standard (AES).