Noakhali Science and Technology University
Department of Information and Communication Engineering
Special Term Exam 2022 Session: 2017-2018
Course Code: ICE 4203 Course Title: Cryptography and Information Security
Credits: 3 Time: 4 Hours Total Marks: 70

Answer **any seven (07)** from the following **Marks**

1. a) Define the following terms: Computer Security, Network Security, Information Security, and Cryptography.**2**
b) Briefly explain the attacks threatening to integrity. **3**
c) What is Public Key Cryptography? Explain Public Key Cryptography with an example of how encryption and decryption occur. **5**

2. a) What are the differences between Stream Cipher and Block Cipher? **2**
b) Using Playfair cipher, find out the ciphertext of "COMMUNICATION" using the keyword "COMPUTER". **3**
c) Show the encryption and decryption process of the Hill Cipher technique for the message "ACT" using the keyword "GYBNQKURP". **5**

3. a) Implement the encryption process of Polyalphabetic Cipher for the plaintext "THISPROCESSCANALSOBEEXPRESSED" using the key "CIPHER". **6**
b) Briefly describe Confusion and Diffusion. **2**
c) Let be a Ciphertext is "GSGSEKFREKEOE" and the Key is 3. Find out the plaintext using Rail Fence cipher. **2**

4. a) Elaborate Euler's Totient theorem with an example. **3**
b) Let's p=3, q=11 and message=2, Find out the ciphertext using RSA algorithm and show the decryption process to retain the message. **3**
c) Draw the encryption diagram of IDEA algorithm and list down the 14 steps of IDEA algorithm for encryption process. **4**

5. a) What is Hash function in cryptography? Explain how hash function ensures the confidentiality of message. **5**
b) Define placement of encryption. How Link encryption and End-to-End encryption works? Explain with figures. **5**

6. a) What is the difference between passive and active security threats? **2**
b) Demonstrate the process of public key distribution. **4**
c) Suppose that two parties A and B wish to set up a common secret key (D-H key) between themselves using the Diffie Hellman key exchange technique. They agree on 7 as the modulus and 3 as the primitive root. Party A chooses 2 and party B chooses 5 as their respective secrets. What is their D-H key? **4**

7. a) Describe the RSA algorithm with suitable example. **5**
b) Define primitive root with suitable example.**2**
c) What is the difference between Symmetric and Asymmetric key encryption? **3**

8. a) What is a message authentication code? What types of attacks are addressed by message authentication? **3**
b) Explain what is meant by a digital signature and describe how it is generated. **5**
c) What are the properties a digital signature should have? **2**

9. a) Explain the security services for electronic mail. **5**
b) Explain what is meant by the term Firewall in network security and discuss how it is used in network architectures.**5**