Total No. of printed pages = 3

19/5th Sem/DCSE504

2021

CRYPTOGRAPHY AND NETWORK SECURITY

Full Marks – 100

Time – Three hours

The figures in the margin indicate full marks for the questions.

Answer any *five* questions.

1. (a) What do you understand by Cryptography and Network Security ? 5

   (b) Explain three key objectives of Network Security with examples ? 3×5=15

2. (a) What do you understand by a Threat, Vulnerability and Security Attacks ? 6

   (b) Explain different types of Security Attacks with example. 14

3. (a) What is a Cipher ? 2

   (b) Encrypt the message "ATTACKPOSTPONED" with the key "KINGDOM" using Playfair Cipher ? 6

[Turn over

(c) Explain Hill Cipher Algorithm. 6

(d) What is steganography and one time pad? Explain with example. 6

4 (a) Explain Electronic Code Book (ECB) Mode of Cipher. 5

(b) What is the difference between Symmetric Key Cipher and Asymmetric Key Cipher? 5

(c) Explain i^{th} round of encryption technique of DES algorithm. 5

(d) Explain RSA Algorithm. 5

5 (a) What is a digital signature and how does it work? 5

(b) How does the receiver verify the sender of the message in Digital Signature? Explain with diagram. 5

(c) What is a hash and message digest? 5

(d) Explain the application of hash and how does it help in storing password in database. 5

6 (a) In a public key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is plaintext M? 10

(b) Find the multiplicative inverse of 7 mod 29 using extended Euclid Algorithm? 10

7. Write short notes on any *four*: 4×5=20

(a) Spoofing

(b) Man in the Middle Attack

(c) SQL Injection

(e) Model for Network Security

(f) Phishing

(h) Secure Hash Algorithm

(i) AES.