Total No. of printed pages = 2

CS 131701 NR

Roll No. of candidate □□□□□□□□□□

8/2/22 2021

B.Tech. 7th Semester End-Term Examination

CSE

CRYPTOGRAPHY AND INFORMATION SECURITY

(New Regulation)

Full Marks – 70 Time – Three hours

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

Answer question No. 1 and any *four* from the rest.

1. Answer the following questions : (10 × 1 = 10)

   (a) What are the three goals of Network Security?

   (b) What do you mean my Spoofing?

   (c) What is Denial of Service attack?

   (d) What is non repudiation?

   (e) What is Substitution Cipher?

   (f) Define Fermat's theorem.

   (g) Find the value of ϕ (81), where ϕ (phi) is Euler's totient function?

   (h) What is parity drop in DES?

   (i) How do you know if two numbers are relatively prime?

   (j) What do you mean by internet worm?

2. Answer the following questions

   (a) Distinguish between Monoalphabetic and Polyalphabetic Substitution technique. Briefly discuss about Keyless and Keyed Transposition Techniques. (10)

   (b) Using Playfair Technique encrypt the word — BALLOON. Use MONARCHY as the keyword (5)

[Turn over

3. Answer the following questions

(a) Briefly discuss Key generation Technique in DES. (5)

(b) Briefly Discuss about key generation technique in RSA. Suppose, Alice uses Bob's RSA public key (e = 7, n = 143) to send a plaintext P encrypted as ciphertext c = 57. Show how eve can use the chosen ciphertext attack if she has access to Bob's computer to find the plaintext. (10)

4. Answer the following questions

(a) Distinguish between Public and Private keys in Asymmetric-key cryptosystem. How do you achieve confidentiality in public key Encryption mechanism? (7)

(b) Briefly discuss Man-in-the middle attack in Diffie Hellman Key exchange Protocol (8)

5. Answer the following questions

(a) Explain the various public key distribution Schemes. (10)

(b) Define Kerberos and name its Servers? Briefly mention the duties of each server (5)

6. Answer the following questions

(a) Briefly discuss about Transport and Tunnel mode in IPSec. (8)

(b) Briefly discuss about Pretty Good privacy (7)

7. Answer the following questions

(a) Explain any two approaches for intrusion detection? (7)

(b) What are the typical phases of operation of a virus? (8)

8. Write short notes on — (any *two*) (2 × 7 ½ = 15)

(a) Cryptographic Hash Function

(b) Digital Signature

(c) Transport Layer security