Total No. of printed pages = 3

CS 131701

Roll No. of candidate | | | | | | | | | | |

2018

B.Tech. (CSE) 7th Semester End-Term Examination

CRYPTOGRAPHY AND INFORMATION SECURITY

Full Marks – 100 Time – Three hours

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

Answer Question No. 1 and any *six* from the rest.

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

   (i) What do you mean by Authentication?

   (ii) What is Snooping?

   (iii) What do you mean by Active and Passive attacks?

   (iv) What do you mean by repudiation attack?

   (v) What is block cipher?

   (vi) What do you mean by parity drop in DES?

   (vii) What is Fermat's theorem?

   (viii) What is Co-prime?

   (ix) Name two protocols delined by IPSec?

   (x) What is a virus?

[Turn over

2. Answer the following questions :

(a) What is the need for Network Security? Explain its goals. (7)

(b) Briefly discuss Keyless and Keyed Transposition techniques? (8)

3. Answer the following questions :

(a) Mentioning the significance of Expansion D-Box and S-Box Substitution briefly discuss about the DES function with suitable diagrams. (10)

(b) What is Euler's totient function? Find the Value of ϕ (121). (5)

4. Answer the following questions :

(a) Describe the Key generation technique in RSA. Suppose. Alice uses bob's RSA public key (7, 77) and sends the plain text P = 5 to bob. Find Bob's private key and the cipher text. (8)

(b) Briefly discuss Dime Hellman Key exchange protocol. (7)

5. Answer the following questions :

(a) Write a short note on message authentication code. (10)

(b) Briefly discuss how Public key distribution is achieved using public key certificate scheme. (5)

6. Answer the following questions :

(a) What are the criteria of cryptographic hash function? (5)

(b) Explain MD5 algorithm with the help of a suitable diagram. (10)

7. Answer the following questions :

(a) Briefly discuss the working principle of Kerberos protocol. (10)

(b) Write short note on transport and tunnel modes in IPSec Protocol. (5)

8. 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)

9. Write short notes on — (any *two*) $(2 \times 7\frac{1}{2} = 15)$

(a) Firewall

(b) PGP

(c) Transport Layer security.
