Roll No. ..... Total Pages : 03

(194)

D-C-190194

B. Tech. EXAMINATION, 2019

Semester VII (CBS)

INFORMATION SECURITY

CS-703

Time : 3 Hours *Maximum Marks : 60*

The candidates shall limit their answers precisely within the answer-book (40 pages) issued to them and no supplementary/continuation sheet will be issued.

Note : Attempt *Five* questions in all, selecting *one* question from each Section A, B, C and D. Q. No. **9** is compulsory.

Section A

1. (a) What do you mean by Information Security ? Explain various security goal implementation techniques. **5**

(b) What are extended Euclidean algorithm ? Discuss its advantage. **5**

2. What are various types of attacks on ciphers ? Explain the role of substitution ciphers and transposition ciphers in information security. **10**

Section B

3. What are perfect substitution ciphers ? Explain Vernam ciphers with example. **10**

4. Differentiate linear and differential cryptanalysis. Explain the vigenere ciphers analysis scheme. **10**

Section C

5. What is RSA encryption algorithm ? Explain its advantages and disadvantages with suitable example. **10**

6. What is Digital Signature Algorithm ? Explain RSA digital signature scheme algorithm in detail. **10**

Section D

7. Why low is required for information security in Indian scenario ? What are different pitfall in Indian IT-act and suggest some improvement point ? **10**

8. What do you mean by encryption standard ? Explain DES and AES standard in detail. 10

Section E

(Compulsory Question)

9. Answer the following questions :

(a) What is Information System and how it can be secured ?

(b) What is Block Ciphers ?

(c) What is Digital Signature Standard ?

(d) What are ethical issues in hacking ?

(e) What is Private Key ?

(f) Define Massage Authentication Code.

(g) What is role of cryptography in Information Security ?

(h) What are two basic functions used encryption algorithms ?

(i) What is limitation of firewalls ?

(j) What is Secure Socket Layer ?

10×2=20 (2 marks each)