Roll No. ..... Total Pages : 04

D-180318

B. Tech. EXAMINATION, 2018

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 Sections A, B, C and D. Section E is compulsory.

Section A

1. (a) What is an Information Security ? Describe the critical characteristics of information security. 5

   (b) Explain the components of Information Security. How will you balance the security and access ? 5

2. What is Cryptography ? Discuss the role of cryptography in Information security. Also explain the Fermat's Theorem. 10

Section B

3. (a) What do you mean by perfect substitution in cryptanalysis ? Explain in detail. 5

   (b) Differentiate between stream cipher and block cipher in detail. 5

4. What is Cryptanalysis ? Describe it and also explain Monoalphabetic ciphers and Polyalphabetic ciphers. 10

Section C

5. What is the purpose and major issues of Encryption ? Explain the concept of Public Key encryption system in detail. 10

6. Explain the following :

   (a) RSA Digital signature Scheme algorithm 5

   (b) Digital Signature Standards (DSA). 5

Section D

7. Define the DES encryption algorithm. Explain the various components of DES Encryption algorithm with neat diagram. **10**

8. Explain the following :

   (a) Ethical domain for Information Security **5**

   (b) Ethical Hacking. **5**

Section E

9. Explain the following :

   (a) Define the concept of Unicity Distance.

   (b) What are the Information Securities Goals ?

   (c) Explain Euler Totient Function

   (d) Describe the types of Attacks on Ciphers.

   (e) Draw neat diagrams of symmetric and asymmetric cryptography.

   (f) What is Vignere Cipher ?

   (g) What are the different types of cryptanalytic attacks ?

   (h) Which are two important issues are addressed with public key cryptography ?

   (i) Define RSA encryption.

   (j) On which premises relies the strength of RSA ? Explain. **2×10=20**