[Total No. of Questions - 9] [Total No. of Printed Pages - 2]
(2125)

15328

B. Tech 7th Semester Examination

Information Security (NS)

IT-415

Time : 3 Hours **Max. Marks : 100**

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 each from section A, B, C & D. Section-E is compulsory.

SECTION - A

1. (a) Describe various cryptanalysis techniques. (10)

   (b) Describe the good characteristics of good cipher. (10)

2. Compare and contrast block cipher and stream cipher. (20)

SECTION - B

3. Describe Fermat's Theorem. Use the Theorem to do the following.

   (a) Find the least residue of 9^{794}= modulo 73.

   (b) Solve $x^{86} = 6$ (mod 29).

   (c) Solve $x^{39} = 3$ (mod 13). (20)

4 Describe the Euclidian Algorithm and find Multiplicative inverse of

   (a) 8 mod 11 (b) 50 mod 71 (c) 43 mod 6 (20)

SECTION - C

5. Determine the output of the first iteration of the DES algorithm when the plain text is all zero and the key is all zero. (20)

6. What is the legal status of information security in India, US and Europe? What are the implication of Snowden leaks on information security? Comment on the current concerns in the post Snowden era. (20)

SECTION - D

7. Describe the security concerns in an Operating system. Illustrate the role of OS hardening. (20)

8. Discuss the security issue in web services. (20)

SECTION - E

9. Write short notes on:

   (a) Threat, Vulnerability, Attack, Risk.

   (b) VPN.

   (c) DMZ.

   (d) RSA.

   (e) SHA2. (4×5=20)