[Total No. of Questions - 9] [Total No. of P ed Pages - 2]
(2126)

16202(D) 10 DEC 2016

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 any one question from Section A, B, C and D. Section E is compulsory.

SECTION - A

1. (a) In the conventional Military sense, it is occasionally suggested that "a strong offence is the best defense." Does this make sense in the context of cyber security and cyber defense? Explain your answer. (10)

   (b) What are mono alphabetic and poly alphabetic ciphers? Give the possible attacks on mono alphabetic ciphers. (10)

2. (a) Explain Hill cipher. Also give cryptanalysis of Hill cipher. (10)

   (b) What are different security goals and different security mechanisms? Explain. (10)

SECTION - B

3. (a) Give Euclid algorithm to find the multiplicative inverse of b in Z_n. Use this algorithm to find the multiplicative inverse of 11 in Z_{26}. (10)

   (b) Explain SHA 512 algorithm. (10)

4. (a) Explain three criteria that must be satisfied by a cryptographic hash function. (10)

   (b) What is digital signature? What are different types of attacks possible on digital signature? Explain. (10)

SECTION - C

5. (a) Discuss Meet-in-the middle attack on double DES? (10)

   (b) Write a note on Indian IT Act. (10)

6. Explain AES. Also give security analysis of AES. (20)

SECTION - D

7. (a) List out the different issue involved in providing database security. (10)

   (b) Discuss the security threats posed by electronic mails. (10)

8. What are the different protocols used in securing personal e-mail exchange? Explain them. (20)

SECTION - E

9. (a) Explain confusion and diffusion

   (b) Write a note on Implementation issue in Firewalls.

   (c) What do you understand by Ethical Hacking?

   (d) Security issues involved in Mobile databases.

   (e) Explain the concept of confusion and diffusion. (4×5=20)