Seat No: _____ **Enrollment No: _____**

PARUL UNIVERSITY

FACULTY OF ENGINEERING & TECHNOLOGY

B.Tech. Summer 2018 - 19 Examination

Semester:6 **Date:07/05/2019**
Subject Code: 03105354 **Time: 10:30pm to 01:00pm**
Subject Name: Information Security **Total Marks: 60**

Instructions:
1. All questions are compulsory.
2. Figures to the right indicate full marks.
3. Make suitable assumptions wherever necessary.
4. Start new question on new page.

Q.1 Objective Type Questions - (Fill in the blanks, one word answer, MCQ-not more than Five in case of MCQ) (All are compulsory) (Each of one mark) **(15)**

1. In cryptography, the order of the letters in a message is rearranged by
   a) transpositional ciphers b) substitution ciphers
   c) both transpositional ciphers and substitution ciphers d) none of the mentioned
2. Cryptographic hash function takes an arbitrary block of data and returns
   a) fixed size bit string b) variable size bit string
   c) both fixed size bit string and variable size bit string d) none of the mentioned
3. GCD(a,b) is the same as GCD(|a|,|b|). True/False
4. Shift cipher is sometimes referred to as the
   a) Playfair Cipher b) Polyalphabetic Cipher c) Caesar cipher d) Monoalphabetic Cipher
5. A digital signature need a :
   (a) Shared key system (b) Private key system
   (c) Public key system (d) None of the above
6. In an authentication using symmetric keys, if 10 people need to communicate, we need .....Keys.
   (a) 90 (b) 20 (c) 40 (d) 45
7. Kerberos is an authentication scheme that can used to implement:
   (a) Public key cryptography (b) Digital signature
   (c) Hash function (d) Single sign on
8. Which of the following is not a block cipher operating mode?
   (a) ECB (b) CBF (c) OFB (d) CBC
9. The process to discover the key with some knowledge is known ad _____
10. In DES the initial permutation table is of size
    a) 16X8 b) 12X8 c) 8X8 d)4X8
11. The method of hiding secret is _____
12. _____ is an example of product cipher.
13. Which scheme produces random output that bears no statistical relationship to the plaintext?
14. Use the playfair cipher to encipher the message “enjoy the balloon ride” and the key is “ticket”.
15. What is the difference between diffusion and confusion?

Q.2 Answer the following questions. (Attempt any three) **(15)**

A) What is the difference between an unconditionally secure cipher and a computationally secure cipher?

B) State Fermat's Theorem and solve s 3^{201} mod 11

C) What are the essential ingredients of a symmetric cipher?

D) List ways in which secret keys can be distributed to two communicating parties.

Q.3 A) State RSA algorithm and Perform encryption and decryption using RSA algorithm For the following. P=7; q=11; e=17; M=8. **(07)**

B) Differentiate MAC and Hash function? Explain both with example **(08)**

OR

B) With the help of diagram explain MD5 algorithm **(08)**

Q.4 A) Give the benefits of IP security? What are the protocols used to provide IP security? Specify the IP security services? **(07)**

OR

A) Draw and explain X.509 Authentication Services **(07)**

B) Explain AES Key expansion algorithm **(08)**