

Code No: 126AQ**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD****B. Tech III Year II Semester Examinations, December - 2017****INFORMATION SECURITY****(Computer Science and Engineering)****Time: 3 hours****Max. Marks: 75****Note:** This question paper contains two parts A and B.

Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A**(25 Marks)**

- 1.a) Define Non Repudiation. [2]
- b) Write a short notes on steganography. [3]
- c) Define linear cryptanalysis. [2]
- d) Discuss about Electronic code book mode? [3]
- e) Define Message Authentication Code. [2]
- f) Illustrate about biometric authentication. [3]
- g) What is IP Security? [2]
- h) Discuss about the concept of combining security associations. [3]
- i) What is Firewall? [2]
- j) Write short notes on virtual elections. [3]

PART - B**(50 Marks)**

2. Compare and Contrast between Symmetric and Asymmetric key cryptography. [10]
- OR**
3. Give an example to explain the concept of transposition ciphers in detail. [10]
 4. With a neat diagram explain how encryption and decryption are done using Blowfish algorithm? [10]
- OR**
5. Given two prime numbers $p=5$ and $q=11$, and encryption key $e=7$ derive the decryption key d . Let the message be $x=24$. Perform the encryption and decryption using R.S.A algorithm. [10]
 6. Give a neat sketch to explain the concept of Secured Hash Algorithm (SHA). [10]
- OR**
7. Client machine C wants to communicate with server S. Explain how it can be achieved through Kerberos protocol? [10]

8. How the messages are generated and transmitted in pretty good privacy (PGP) protocol? Explain with clear diagrams. [10]

OR

9. Draw the IP security authentication header and explain the functions of each field. [10]

10. Explain the steps involved in performing Secure Inter-branch Payment Transactions. [10]

OR

11. List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway? [10]

---ooOoo---