

**R13**

Code No: 126AQ

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD****B. Tech III Year II Semester Examinations, April - 2018****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) Explain the Caesar cipher. [2]
- b) Define confidentiality and authentication [3]
- c) Differentiate conventional & public key encryption. [2]
- d) What is traffic Padding? What is its purpose? [3]
- e) What is the purpose of X.509 standard? [2]
- f) In the content of Kerberos, what is realm? [3]
- g) Explain the reasons for using PGP. [2]
- h) Compare Transport mode and Tunnel Mode. [3]
- i) What do you mean by malicious software? [2]
- j) What is application level gateway? [3]

**PART - B****(50 Marks)**

- 2.a) Explain how gateway works in internetwork security model.
  - b) Explain the various types of cryptanalytic attacks. [5+5]
- OR**
3. Explain symmetric and asymmetric key cryptography. [10]
  - 4.a) Explain how key exchange is done using Diffie-Hellman key exchange.
  - b) Discuss the "man-in-the-middle" attack. [5+5]
- OR**
5. Explain Blowfish algorithm. [10]
- 6.a) What is HMAC and what are its advantages over MAC?
  - b) Discuss different approaches to Message Authentication. [5+5]
- OR**
7. Discuss the requirements of Kerberos. Explain the Kerberos ver-4 message exchanges. [10]

AG AG AG AG AG AG AG A

- 8.a) Explain the different MIME content types.  
b) Explain S/MIME certificate processing method.

[5+5]

OR

- 9.a) What are the applications of IP security?  
b) Describe the general structure of IPSEC authentication header. Discuss how anti-reply service is supported.

[5+5]

10. Explain the different types of firewalls with neat diagrams.

[10]

OR

11. Discuss about Intrusion Detection and approaches of Intrusion Detection.

[10]

AG AG AG AG AG AG AG A

---ooOoo---

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A

AG AG AG AG AG AG AG A