

Code No: 117DY

R13

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

B. Tech IV Year I Semester Examinations, November/December - 2016

INFORMATION SECURITY  
(Information Technology)

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) What is the need for security? [2]
- b) Explain symmetric key cryptography. [3]
- c) What is the difference between symmetric key cipher and asymmetric key cipher? [2]
- d) Write about stream ciphers. [3]
- e) What are the uses of digital signature? [2]
- f) What is public key certificate? [3]
- g) What are the principle services provided by PGP? [2]
- h) Discuss the basic approaches to building security associations. [3]
- i) What are the benefits provided by an intrusion detection system. [2]
- j) Briefly explain design issues for a fire wall. [3]

**PART-B**

**(50 Marks)**

- 2.a) Explain about different types of Attacks.
  - b) Explain in detail about a model for network security. [4+6]
- OR**
- 3.a) Write about security mechanisms.
  - b) Explain about transposition techniques in cryptography. [4+6]
4. What are the different types of cipher modes? Explain in detail with neat diagrams and also their significance. [10]
- OR**
5. Explain in detail about RSA Algorithm with suitable example. [10]
- 6.a) Explain client-server message exchange with Kerberos.
  - b) Explain about message authentication codes. [5+5]
- OR**
- 7.a) Explain knapsack algorithm in detail?
  - b) Explain about digital signatures. [5+5]
- 8.a) Discuss the operational description of PGP.
  - b) Discuss the transactions provided by S/MIME. [5+5]

**OR**

- 9.a) Explain transport and tunnel modes of ESP.  
b) Outline the applications and benefits of IP Security. [5+5]
- 10.a) Explain the various intrusion detection techniques.  
b) Explain the principles and limitations of firewall. [5+5]
- OR**
11. Explain secure electronic transaction. [10]

--ooOoo--