## VASAVI COLLEGE OF ENGINEERING (Autonomous), HYDERABAD
### B.E. (I.T.) IV Year I-Semester Main Examinations, December-2017

## Network Security

Time: **3 hours**
Max. Marks: **70**

*Note: Answer **ALL** questions in **Part-A** and any **FIVE** from **Part-B***

### Part-A (10 × 2 = 20 Marks)

1. List out the definitions of different types of active attacks.
2. Describe Modular Arithmetic.
3. Define Block cipher.
4. Write the functionality of triple DES.
5. Mention the applications of Hash functions.
6. Define MAC.
7. List out the roles of Firewalls.
8. Define virus and threat.
9. Describe PGP.
10. List out the protocols used in order to provide Email security.

### Part-B (5 × 10 = 50 Marks)

| | | |
|---|---|---|
| 11. a) | Explain the model for Network security. | [5] |
| b) | Discuss about Extended Euclidean Algorithm. | [5] |
| 12. a) | Explain about RSA Algorithm. | [7] |
| b) | Mention and briefly discuss the steps involved in AES Algorithm. | [3] |
| 13. a) | Illustrate and discuss about SHA algorithm. | [7] |
| b) | Discuss briefly about DSS. | [3] |
| 14. a) | Explain the Firewall Design Principles. | [5] |
| b) | Explain about Kerberos. | [5] |
| 15. a) | Explain about IPSec Architecture. | [5] |
| b) | Explain about S/MIME. | [5] |
| 16. a) | State the definition of Chinese Remainder Theorem, explain the steps with a suitable example. | [4] |
| b) | Explain about Blowfish Algorithm. | [6] |
| 17. | Answer any *two* of the following: | |
| a) | List out the merits and de-merits of MD5. | [5] |
| b) | Define what a Trusted System is, and explain about it. | [5] |
| c) | Explain in detail about ESP Packet format. | [5] |

*****