Hall Ticket Number:

Code No. : 22905

VASAVI COLLEGE OF ENGINEERING *(Autonomous)*, HYDERABAD

M.Tech. (CSE: CBCS) II-Semester Main Examinations, July-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. Define security attack, security mechanism and security services.
2. Differentiate cryptography and cryptanalysis.
3. What is the purpose of S boxes in DES?
4. Differentiate RSA with ECC with respect to key sizes.
5. Why ECC is more suitable for resource constrained platform?
6. How authentication can be achieved by using RSA?
7. List the types of attacks that can be addressed by MAC.
8. What is public key certificate?
9. Differentiate tunnel mode with transport mode in IPSEC.
10. List the key exchange methods in SSL.

Part-B (5 × 10=50 Marks)

11. a) Define threat and attack. [3]
    b) Explain with neat sketch a model for network security and network access security. [7]

12. Explain DES Algorithm with neat diagram. [10]

13. a) Discuss SHA5 algorithm to generate message digest. [7]
    b) Explain DSS approach for digital signature. [3]

14. Discuss PKI infrastructure to generate digital certificates. [10]

15. a) Write the drawbacks of keberos earlier versions in comparison with version 4. [4]
    b) Explain in detail the Kerberos version 4 authentication protocol. [6]

16. a) Explain various phases in viruses. [5]
    b) Discuss RSA algorithm with an example. [5]

17. Write short note on any **two** of the following:
    a) CMAC [5]
    b) Fire Walls [5]
    c) Encapsulating Security payload and authentication header in IPSec. [5]

******