Hall Ticket Number:

Code No. : 22505

VASAVI COLLEGE OF ENGINEERING *(Autonomous)*, HYDERABAD

M.E. (ECE: CBCS) II-Semester Main Examinations, July-2017

(Communication Engineering & Signal Processing)

Network Security and Cryptography

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. Describe the need for security mechanism.
2. Specify the design criteria of block cipher.
3. Differentiate between link and end-to-end encryption.
4. List the characteristics of Blowfish and mention the key size.
5. Identify the possible threats for RSA algorithm.
6. Find gcd (1970, 1066) using Euclid's algorithm.
7. Compare the features of DSS with SHA.
8. Draw the frame format of IP Security.
9. Justify with appropriate example, why does Encapsulating Security Payload include a padding field?
10. What is the necessity of firewalls?

Part-B (5 × 10 = 50 Marks)

11. a) Draw the diagrams for various security attacks and define each one of them. [3]
    b) With the help of general structure of simple DES, explain how encryption and decryption are carried out. [7]

12. a) In detail explain the characteristics of advanced symmetric block ciphers. [5]
    b) What is key distribution? Explain. [5]

13. a) Write about Diffie-Hellman Algorithms with the help of all the steps of the algorithm. [5]
    b) Discuss the Chinese remainder theorem. [5]

14. a) With suitable diagrams explain the SHA algorithm. [5]
    b) Mention all the services provided by S/MIME. Explain in detail. [5]

15. a) Draw and explain authentication header structure in detail. [5]
    b) Discuss the virus related threats and the counter measures applied. [5]

16. a) Realize feistel network for implementing DES algorithm. [5]
    b) Explain about traffic confidentiality. [5]

17. Answer any ***two*** of the following:
    a) Describe in general terms an efficient procedure for picking a prime number. [5]
    b) Specify the processing steps involved in messaged digest algorithm. [5]
    c) Compare transport and tunnel mode of ESP with neat sketch. [5]