Hall Ticket Number:

Code No. : 22515

VASAVI COLLEGE OF ENGINEERING *(Autonomous)*, HYDERABAD

M.E. (ECE: CBCS) II-Semester Main Examinations, June-2018

(Communication Engineering & Signal Processing)

Network Security and Cryptography

Time: 3 hours Max. Marks: 60

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

Part-A (10 × 2 = 20 Marks)

1. Specify the four categories of security threats.
2. Compare Substitution and Transposition techniques.
3. What is Triple Encryption? How many keys are used in triple encryption?
4. Outline about traffic confidentiality.
5. Differentiate public key and conventional encryption.
6. Find gcd (1970, 1066) using Euclid's algorithm.
7. Recall the requirements for message authentication.
8. List out the requirements of kerberos.
9. State the services provided by IP Sec.
10. What is meant by intruder and write classes of intruders.

Part-B (5 × 8 = 40 Marks)
(All sub-questions carry equal marks)

11. a) Describe the model for Internet security.
    b) Discuss the strength of Data Encryption Standard.
12. a) Explain the steps involved in one round of IDEA in encrypt and decrypt the data.
    b) Discuss the characteristics of advanced Symmetric block ciphers.
13. a) State and explain the principles of public key cryptography.
    b) Define Euler's theorem and it's application.
14. a) Describe MD5 algorithm in detail. Compare its performance with SHA-1.
    b) Explain the operational description of Pretty good privacy.
15. a) Explain Transport layer security.
    b) Discuss the steps in virus removal process.
16. a) Specify the design criteria of block cipher.
    b) Discuss the features of Blowfish algorithm and explain the algorithm in steps.
17. Answer any ***two*** of the following:
    a) Write the Digital signature standard algorithm.
    b) Summarize the types of attacks addressed by message authentication.
    c) Describe Trusted system in detail.