LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

M.Sc. DEGREE EXAMINATION – **COMPUTER SCIENCE**

SECOND SEMESTER – **APRIL 2016**

CS 2823 – CRYPTOGRAPHY & NETWORK SECURITY

Date: 16-04-2016 Dept. No. Max. : 100 Marks
Time: 01:00-04:00

PART – A

ANSWER ALL THE QUESTIONS: **(10 x 2 = 20 marks)**

1. Define enciphering.
2. Define active attack.
3. State Euler's Theorem.
4. Define Hash function.
5. What are the schemes available in public key distribution?
6. What is digital signature?
7. Write down the steps to prepare signed data MIME entity.
8. Draw the IPV4 tunnel mode authentication header.
9. What is IP address spoofing?
10. What are trapdoors?

PART – B

ANSWER ALLTHE QUESTIONS : **(5 x 8 = 40 marks)**

11. a) What are the Security services of X.800?

(OR)

b) Explain transposition technique with example.

12. a) Write down the application of Euclidean Algorithm in Cryptography? Give an example.

(OR)

b) Explain RSA algorithm with example.

13. a) Explain Digital Signature algorithm.

(OR)

b) What is Birthday attack? Give an example.

14. a) Explain SSL architecture with block diagram.

(OR)

b) Write down the services of Pretty Good Privacy.

15. a) Write down the types of viruses. What are the phases of virus?

(OR)

b) Explain audit records in Intrusion Detection.

PART – C

ANSWER ANY TWO QUESTIONS: **(2 x 20 = 40 marks)**

16. i) How encryption and decryption is performed through Simplified DES algorithm? (10)
ii) Explain RC5 algorithm with block diagram. (10)

17. i) ExplainRIPEMD-160 algorithm in detail. (10)
ii) Describe the working principles of Kerberos Version 4 with block diagram. (10)

18. i) Explain the types of firewalls. (10)
ii) Compare the following algorithms
a) RSA and DSS (5)
b) MD5 and SHA-1 (5)

$$$$$$$