LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

SECOND SEMESTER – **APRIL 2015**

CS 2823 - CRYPTOGRAPHY & NETWORK SECURITY

Date : 16/04/2015 Dept. No. Max. : 100 Marks

Time : 01:00-04:00

PART – A

ANSWER ALL THE QUESTIONS: **10 X 2 = 20**

1. Write down the sizes of Plain text , Cipher text and Key of Simple DES.
2. What is Bruteforce attack?
3. Write down the differences between block cipher and stream cipher
4. Write any four characteristics of BLOW FISH algorithm.
5. Define mutual authentication protocol.
6. Convert "EFAC3468" in bytes of Little Endian format.
7. What is a payment gateway?
8. Define handshake protocol
9. What is trapdoor?
10. Who is masquerader?

PART – B

ANSWER ALLTHE QUESTIONS : **5 X 8 = 40**

11. a) Encrypt the following using two-stage transposition cipher with key 4312567 "ATTACKCHANNAICENTRALTRAINDECK"

(OR)

b) Explain Fiestel Cipher structure along with the parameters influences the design of Fiestel Network.

12. a) Write down the algorithm to test for prime numbers.

(OR)

b) Explain RSA algorithm with an example.

13. a) Explain Digital Signature algorithm

(OR)

b) Write down the message authentication requirements

14. a) What are IP security documents? Describe each of them through the hierarchical diagram.

(OR)

b) Explain the MIME content types

15. a) Write down the characteristics of Firewall.

(OR)

b) Explain data access control of trusted systems.

PART – C

ANSWER ANY TWO: **2 X 20 = 40**

16. i) Explain Simple DES in detail (10)

    ii) Explain RC5 algorithm in detail. (10)

17. i) Explain SHA-1 algorithm in detail. (10)

    ii) ExplainPretty good privacy functions. (10)

18. i) Explain the various intrusion detection methods. (10)

    ii) What are the limitations of RFC 822 of SMTP ? How they are resolved in RFC 2045-2049? (10)

****