LOYOLA COLLEGE (AUTONOMOUS), CHENNAI – 600 034

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

SECOND SEMESTER – APRIL 2017

CS 2823- CRYPTOGRAPHY & NETWORK SECURITY

Date: 06-05-2017 Dept. No. Max. : 100 Marks
Time: 09:00-12:00

PART – A

ANSWER ALL THE QUESTIONS: 10 X 2 = 20

1. Define "Denial of Service".
2. What is Cryptanalysis?
3. What is "man-in-the-middle" attack?
4. Define Public Key.
5. Define mutual authentication protocol.
6. Convert "11AC3468" in bytes of Little Endian format.
7. Write any four IPSec services.
8. What is handshake protocol?
9. What is trapdoor?
10. Who is misfeasor?

PART – B

ANSWER ALL THE QUESTIONS : 5 X 8 = 40

11. a) Explain Playfair Cipher with example.

(OR)

b) Explain encryption and decryption using Hill Cipher.

12. a) Explain the security levels of RSA.

(OR)

b) Write down the modes of RC5 algorithm.

13. a) Explain Diffie-Hellman key exchange algorithm with example.

(OR)

b) Explain Message Authentication code and its basic uses.

14. a) What are public key rings and private key rings? Describe their features.

(OR)

b) Write down the limitations of SMTP. How those problems are resolved by MIME?

15. a) Write down the basic techniques used in password selection.

(OR)

b) Explain data access control of trusted systems.

PART – C

ANSWER ANY TWO: 2 X 20 = 40

16. i) Explain Security services and security mechanisms of OSI (10)
    ii) Explain BLOWFISH algorithm in detail.(10)

17. i) Explain SHA-1 algorithm in detail.(10)
    ii) Write down the transaction types supported by SET.(10)

18. i) Explain Virus Counter Measures in detail.(10)
    ii) Explain hashing functions and their usage in cryptographic algorithms (10)

$$$$$$$$