

D 11937

(Pages : 2)

Name

Reg. No.

**SEVENTH SEMESTER B.TECH. (ENGINEERING) [09 SCHEME] DEGREE
EXAMINATION, NOVEMBER 2016**

CS/IT/PTCS 09 704—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours

Maximum : 70 Marks

Part A (Short Answers)

*Answer all questions in one or two sentences each.
Each question carries 2 marks.*

1. What are threats and attacks to security ?
2. What are block cipher modes ?
3. Define public key cryptography.
4. Define Authentication header.
5. What are firewalls ?

(5 × 2 = 10 marks)

Part B

*Answer any four questions.
Each question carries 5 marks.*

6. Differentiate between Transposition and Substitution ciphers.
7. Explain the strength of DES algorithm.
8. What is S/MIME ?
9. Explain X.509 authentication service.
10. What are the services provided by SSL ?
11. What are the different modes of IP security ?

(4 × 5 = 20 marks)

Part C

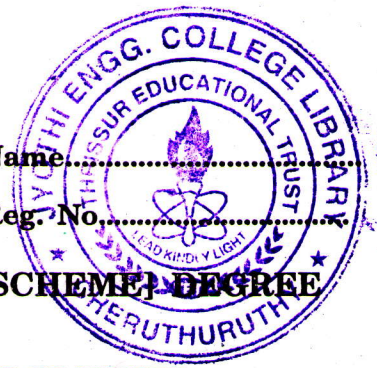
*Answer all questions.
Each question carries 10 marks.*

12. (a) Write short notes on polyalphabetic substitutions.

Or

- (b) Explain the structure of simplified DES with a neat diagram.

Turn over



13. (a) Explain how encryption and decryption is carried out in RSA algorithm.

Or

(b) Explain Diffie Hellman key exchange.

14. (a) Explain the architecture of AH and ESP protocol.

Or

(b) How handshaking is done in SSL protocol ?

15. (a) Write short notes on secure electronic transactions.

Or

(b) What are the different types of firewall ? Explain.

(4 × 10 = 40 marks)