D 90245 (Pages : 2) Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) [09 SCHEME] DEGREE EXAMINATION, NOVEMBER 2015

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

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

1. Specify the components of encryption algorithm.
2. What is trapdoor one way function ?
3. Perform encryption and decryption using RSA alg. for the following $p = 7$; $q = 11$; $e = 17$; $m = 8$.
4. Specify the four categories of security threats.
5. Define VPN.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

6. Tabulate and explain the relationship between security services and mechanisms.
7. List and describe security goals.
8. Explain RC5 in detail.
9. Explain Authentication functions.
10. Write and explain the digital signature Algorithm.
11. Explain case studies on DOS.

(4 × 5 = 20 marks)

Part C

Answer section (a) **or** *(b) of each question.*

12. (a) List the categories of active security attack and explain any one active security attack in detail.

Or

(b) Describe categories of Security Services in detail.

Turn over

13. (a) Explain DES algorithm in detail with an example.

Or

(b) Explain Block Cipher modes of Operation in detail.

14. (a) Explain authentication protocol in detail.

Or

(b) Assume a client C wants to communicate with a server S using Kerberos protocol. How can it be achieved ?

15. (a) Explain Wireless Application Protocol Security.

Or

(b) Explain security in GSM in detail.

(4 × 10 = 40 marks)