D 50497 (Pages 2) Name.....

Reg. No.....

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, NOVEMBER 2013

CS 09 704—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 70 Marks

Part A

I. (a) Give any *four* names of substitution techniques.

(b) Define passive attack.

(c) Specify the IP security services.

(d) What are the key algorithms used in S/MIME ?

(e) Define Firewall.

(5 × 2 = 10 marks)

Part B

II. (a) What are the key principles of security ?

(b) Compare stream cipher and block cipher with example.

(c) Draw a simple public key encryption model that provides authentication alone.

(d) What are the services provided by PGP services ?

(e) Give the applications of IP security.

(f) What are the requirements involved in Kerberos ?

(4 × 5 = 20 marks)

Part C

III. (a) Explain the Key generation process in Data Encryption Standard (DES) algorithm.

Or

(b) Describe the DES encryption process and the strength of DES.

IV. (a) Discuss about Elliptic Curve Cryptography and List few requirements for public key cryptography.

Or

(b) Explain RSA algorithm. Throw some light on the security of RSA.

Turn over

V. (a) Give an overview on S/MIME functionality.

Or

(b) Write short notes on Pretty Good Privacy.

VI. (a) Sketch the IPSec Authentication header and explain the header fields? With neat diagrams, show the scope of encryption and authentication provided by ESP for Transport and Tunnel mode in ; (i) IPV4 ; and (ii) IPV6.

Or

(b) Discuss in detail about Secure Electronic Transaction.

(4 × 10 = 40 marks)