C 62932 **(Pages : 2)** **Name..............................**

Reg. No.............................

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE [SUPPLEMENTARY] EXAMINATION, APRIL 2014

(2009 Scheme)

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

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

1. Define Cryptanalysis.
2. What is the difference between Sub-Bytes and Sub-Word ?
3. What is a one-way function ?
4. What do you mean by MAC ?
5. List the limitations of Firewall.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

1. Write short notes on symmetric encryption.
2. Briefly explain the idea behind Elliptic Curve Cryptosystem.
3. Explain Triple DES with neat diagram.
4. Briefly Explain HMAC algorithm.
5. Explain with elaborate about the Web Security Considerations.
6. Explain firewall configuration.

(4 × 5 = 20 marks)

Part C

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

1. (a) Distinguish between active and passive security attacks and name possible active and passive security attacks.

Or

(b) Briefly explain the categories of Security mechanisms.

2. (a) Briefly describe about the Strength of DES.

Or

(b) Explain in detail about the number theory concepts.

Turn over

3. (a) Explain in detail about the IP Security Architecture.

Or

(b) Discuss about the concept of Electronic Mail Security.

4. (a) Define Virtual private network and explain its protocols.

Or

(b) Explain security in 3G in detail.

(4 × 10 = 40 marks)