C 29695

(Pages : 2)

Name...

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

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION OCTOBER 2012

CS/IT 09 704—CRYPTOGRAPHY AND NETWORK SECURITY

(2009 Admissions)

Time : Three Hours

Maximum : 70 Marks

Part A

Short answer questions (one/two sentences)
Answer **all** *questions.*

1. Differentiate Confusion and Diffusion.

2. List out the measures to protect the Confidentiality of Information.

3. Define Brute-force attack.

4. Name the cryptographic keys used in PGP.

5. Mention the different types of Firewalls.

(5 × 2 = 10 marks)

Part B

Analytical/Problem solving questions.
Answer any **four** *questions.*

6. What common mathematical constants are used in RC5 ?

7. User A and B exchange the key using Diffie Hellman alg. Assume.

   á = 5 q = 11 XA = 2 XB =3. Find YA, YB, K.

8. Assume the client C wants to communicate server S using Kerberos procedure. How can it be achieved ?

9. Discuss operating system security.

10. What is meant by SET ? What are the features of SET ?

11. What is a Screened Subnet Firewall ?

(4 × 5 = 20 marks)

Part C

Descriptive/Analytical/Problem solving questions.

12. (a) Explain Transposition and Substitution ciphers with examples.

Or

(b) Explain DES Algorithm.

Turn over

13. (a) Explain Elliptic Curve Architecture.

Or

(b) Describe about Trusted Systems.

14. (a) What are the steps involved in SET Transaction ?

Or

(b) Discuss X.509 Authentication Service in detail.

15. (a) Describe the architecture of IP Security.

Or

(b) Discuss Web Security in detail.

(4 × 10 = 40 marks)