C 30102 (Pages : 2)

Name..

Reg. No...

SEVENTH SEMESTER B.TECH. (ENGINEERING) DEGREE [2014 SCHEME] EXAMINATION, NOVEMBER 2017

Computer Science Engineering

CS/IT 14 702—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours

Maximum : 100 Marks

Part A (Analytical/Problem solving short questions.

Answer **eight** *questions.*
Each question carries 5 *marks.*

1. State the need for network security.
2. State the similarities and differences between diffusion and confusion.
3. Highlight the strength and weaknesses of DES.
4. Give any four types of substitution techniques.
5. Perform encryption and decryption using RSA Algorithm for P = 7 ; q = 11 ; e = 17 ; M = 8.
6. List four general characteristics of schema for the distribution of the public key.
7. Mention the role of compression function in hash function.
8. Distinguish between message integrity and message authentication.
9. What are the steps involved in SSL required protocol?
10. Draw the general format for PGP message.

(8 × 5 = 40 marks)

Part B (Analytical/Problem solving Descriptive questions.

Answer **all** *questions.*
Each question carries 15 *marks.*

11. (a) Explain about the various types of security attacks with examples.

Or

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

12. (a) Draw the general structure of DES and explain the encryption decryption process.

Or

(b) Explain in detail about Elliptic Curve Cryptography with neat diagram.

Turn over

13. (a) Give the summary of cryptographic algorithms used by S/MIME.

Or

(b) Briefly explain Deffie Hellman key exchange with an example.

14. (a) Explain firewalls and how they prevent intrusions.

Or

(b) Describe in detail about Socket layer and transport layer security with neat diagram.

(4 × 15 = 60 marks)