C 60561 (Pages : 2) Name.........................

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

EIGHTH SEMESTER B.TECH. (ENGINEERING) DEGREE EXAMINATION, APRIL 2014

(2009 Scheme)

EC/PTEC 09 804 L 11—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *the questions.*
Each question carries 2 *marks.*

1. What is the strength of DES ?
2. Draw a figure to show the establishment of session key for public key encryption system.
3. What is MAC ?
4. What is Birthday attack ?
5. What is MOST in S | MIME ?

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*
Each question carries 5 *marks.*

6. Explain the avalanche effect in DES.
7. Explain about Rotor machines.
8. Explain about the essential elements of public key crypto system.
9. Write down the steps involved in the secret key distribution.
10. Explain the message authentication is done using MAC.
11. Explain about trusted system.

(4 × 5 = 20 marks)

Part C

Answer section (a) **or** *Section (b) of each question.*
Each question carries 10 *marks.*

12. (a) With an example, show how encryption and decryption is carriedout in polyalphabetic cipher, rail fence cipher and one time pad.

Or

(b) Explain about cipher block chaining mode and stegnography.

Turn over

13. (a) With an example show, the operation of RSA algorithm and Diffie Hellman key exchange protocol.

Or

(b) Discuss in detail the encryption, decryption and security of Elliptic curve cryptography.

14. (a) Explain about Message authentication functions and Digital signature algorithm.

Or

(b) Explain about any *two* authentication protocols.

15. (a) Describe in detail about PGP.

Or

(b) Briefly explain about IP security.

(4 × 10 = 40 marks)