C 1056 (Pages : 2) Name.....

Reg. No.....

EIGHTH SEMESTER B.TECH. (ENGINEERING) [09 SCHEME] DEGREE EXAMINATION, APRIL 2016

EC / PTEC 09 804 L11—CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three Hours Maximum : 70 Marks

Part A

Answer **all** *questions.*

I. (a) What are the requirements of DES encryption ?

(b) Mention any *two* techniques of attacking RSA.

(c) Give the advantages of public key cryptosystems.

(d) What do you mean by firewall ?

(e) Define IP security.

(5 × 2 = 10 marks)

Part B

Answer any **four** *questions.*

II. (a) What is the purpose of the S-boxes in DES ?

(b) Discuss the principles of public key crypto systems.

(c) Write short note on elliptic Curve cryptography.

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

(e) List the benefits of IP Security.

(f) Discuss in detail about Authentication Header.

(4 × 5 = 20 marks)

Part C

Answer **all** *questions.*

III. (a) (i) Explain the OSI Security Architecture.

(ii) Explain Classical Encryption Techniques.

Or

(b) Discuss in detail about Rotor machine and Steganography techniques.

IV. (a) Describe the RSA algorithm with an example and discuss its security.

Or

(b) Briefly explain the idea behind Elliptic Curve Cryptosystem.

Turn over

V. (a) Explain the following : (i) Message authentication codes ; and (ii) Hash functions.

Or

(b) Discuss in detail about authentication requirements and functions.

VI. (a) Explain the following : (i) PGP random number generator ; (ii) Security associations ; and (iii) Key management.

Or

(b) Give the format of the IP sec Authentication Header. Write short notes on authentication header and ESP.

(4 × 10 = 40 marks)