53 (EC 711) CRYY

2014

CRYPTOGRAPHY

Paper : EC 711

Full Marks : 100

Pass Marks : 30

Time : Three hours

The figures in the margin indicate full marks for the questions.

Answer ***any five*** *questions.*

1. *(a)* Describe Feistel Encryption and Decryption with proper diagram. 8

   (b) Explain Triple DES with two keys and find out an expression for the output text. 6

   (c) Explain RC4 stream Cipher. 6

2. *(a)* Discuss various security attacks. 10

(b) Discuss the various security mechanisms mentioned in X.800 literature. 10

3. (a) Explain the working of Cipher Block Chaining Mode (CBC). 8

(b) What is PGP ? Discuss its services. 3+9=12

4. (a) Explain how is hash function used to create digital signature. 7

(b) What is MAC ? How is a MAC used to achieve confidentiality and authentication ? 3+7=10

(c) Differentiate between block ciphers and stream ciphers. 3

5. (a) Discuss the RSA algorithm. 6

(b) Explain the SSL Records Protocol. Describe its operation. 3+7=10

(c) What are the various web security measures ? 4

6. *(a)* Explain Data confidentiality and Authentication. 4+4=8

(b) Mention the IPSec services. 5

(c) Discuss the ingredients of Symmetric Encryption. 7

7. *(a)* Write short notes on : 5×4=20

(i) Caeser Cipher

(ii) Differential cryptanalysis

(iii) S/MIME

(iv) Requirement of Digital Signature.
