Total number of printed pages–3

53 (EC 711) CRYY

2015

CRYPTOGRAPHY

Paper : EC 711

Full Marks : 100

Time : Three hours

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

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

1. *(a)* What is PGP ? Discuss the services provided by PGP in detail. 2+8=10

   (b) Describe Feistel Encryption and Decryption techniques. 10

2. *(a)* Explain SSL protocol stack architecture and SSL record protocol operation. 10

   (b) Describe RSA algorithm. 10

Contd.

3. *(a)* What is IP Sec ? Discuss its services. 10

(b) Explain the terms — *(i)* Authentication and *(ii)* Data Confidentiality. 5+5=10

4. *(a)* How is Stream Generation achieved in RC4 ? Write down the steps. 10

(b) Describe the various Passive and Active attacks citing proper example. 10

5. *(a)* Give examples of the use of hash function for Message Authentication. 8

(b) What are the various block cipher modes of operations ? Discuss the output Feedback Mode of operation with proper diagram. 12

6. *(a)* What is Digital Signature ? Describe a scheme to produce Digital Signature. 3+7=10

(b) What do you mean by MAC ? Cite some examples to achieve messege authentication using MAC. 3+7=10

7. Write short notes on : 5×4=20

(i) Diffie-Hellman Key Exchange Algorithm

(ii) SMIME

(iii) Symmetric Encryption

(iv) Linear Cryptanalysis.