53 (EC 711) CRYY

2013

(May)

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)* What protocols comprise SSL ? Describe a SSL protocal stack. 2+6=8

   (b) What is a replay attack ? 3

   (c) What services are provided by IPSec ? 9

2. *(a)* What is PGP ? What are the services provided by PGP ? 3+7=10

   (b) Differentiate between a Message Authentication Code (MAC) and Digital Signature. 8

   (c) What is a Secure Hash Function ? 2

Contd.

3. *(a)* Write the important features of public-key cryptography. 5

(b) Describe the RSA algorithm. 10

(c) Differentiate between a block cipher and a stream cipher. 5

4. *(a)* Compare DES and 3 DES. 6

(b) Describe Link and end-to-end encryption techniques. Find their application areas. 14

5. *(a)* What are the various cipher block modes of operation ? Describe *any one* of them. 10

(b) How Stream Generation is achieved through RC4 algorithm ? 10

6. *(a)* Describe Feistel Encryption Algorithm. 10

(b) List and define categories of passive and active attacks. 10

7. *(a)* Describe Security Services *(x.800)*. 10

(b) Elaborate design criteria for the *F*-functional and *S-box* of Feistel Block Cipher. 10
