53 (EC 711) CRYY

2013

(December)

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 a message authentication code ? 4

   (b) Describe how MAC is used to provide authentication and confidentiality. 6

   (c) What are the requirements of Digital Signature. 5

   (d) In what order should the signature function and the confidentiality function be applied to a message, and why ? 5

2. *(a)* What is a cryptographic hash function ? 3

(b) Describe how a hash code is used to provide a digital signature. 5

(c) Describe some examples of the use of a hash function for message authentication. 12

3. *(a)* Write how the Web presents new challenges of security threats. 6

(b) What are the various Web Traffic Security approaches ? 6

(c) Describe the SSL protocol stack. 8

4. *(a)* What requirements must a public key cryptosystems fulfil to be a secure algorithm ? 7

(b) Describe the RSA algorithm. 7

(c) Perform encryption and decryption using the RSA algorithm for the following :

(i) $p = 3 ; q = 13 ; e = 5 ; M = 10$

(ii) $p = 5 ; q = 7 ; e = 7 ; M = 12$. 3+3=6

5. *(a)* Write in detail the OSL Security Architecture *(X 800)*. 7

(b) Describe how does an apparent perform Replay Attack and Traffic Analysis. Which one is more dangerous and which one is more difficult to detect ? 3+3+3=9

(c) Differentiate between a Block Cipher and a Stream Cipher. 4

6. *(a)* Explain the basic principle of working of a stream cipher. 5

(b) Write down the IP Sec Services. 5

(c) What is PGP ? Describe its services. 10

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

(i) S/ MIME

(ii) Steganography

(iii) RC4

(iv) Wireless LAN Security.
