53 (EC 711) CRGR

2019

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)* Describe a digital signature scheme using hash function. 8

   (b) What are the services provided by IPsec ? 4

   (c) Describe the RSA algorithm. 8

2. *(a)* Describe Caesar Cipher. What are its weaknesses ? 5+2=7

   (b) What is SSL ? Describe the SSL specific protocols. 2+6=8

Contd.

(c) Cite the differences between block ciphers and stream ciphers. 5

3. (a) Using the key "deceptive" with playfair matrix, encrypt the message — "The enemy must be stopped at all costs." 6

(b) What is PGP? Describe how PGP functions can be employed to achieve both confidentiality and authentication. 2+6=8

(c) Describe Triple DES system. What is Brute-force attack? 4+2=6

4. (a) Explain Encryption and Decryption processes of output feedback (OFB) mode of block ciphers. What are its advantages over CBC *or* CFB mode? 6+2=8

(b) Describe SSL Record Protocol operation. 6

(c) Perform encryption and decryption using RSA algorithm for the following: 6

$p = 3$; $q = 13$; $e = 5$; $M = 10$

5. (a) What is Message Authentication Code (MAC)? Describe how MAC is used to achieve confidentiality and authentication. 2+6=8

(b) Decrypt the following Ciphertext using Vigenère Cipher: 6

key → "gold"

Ciphertext → C S O R T H R R Z C L I X W N D Z C D W K O W Q U Q Z F U B F W Y

(c) Describe the working principle of differential cryptanalysis. 6

6. (a) What is public-key cryptography? How does it ensure authentication and secrecy? 3+6=9

(b) Describe the design criteria of S-boxes in DES. 6

(c) Explain the functions of S/MIME. 5

7. Write short notes on : 5×4=20

(i) RC4 algorithm

(ii) Ancient means of Steganography

(iii) Ingredients of a digital signature system

(iv) Diffusion and Confusion.