53 (EC 711) CRPG

2021

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 public-key cryptography ? How does it ensure both authentication and secrecy ? 3+7=10

   (b) What is SSL ? Describe the SSL specific protocols. 3+7=10

2. *(a)* Explain how does double DES get vulnerable to cryptanalytic attack. 6

   (b) Describe a single round of DES. 8

Contd.

(c) Explain a triple DES system based on two keys. 6

3. (a) Describe the Caesar Cipher. What are its advantages and disadvantages ? 4+4=8

(b) Describe public-key cryptography system. 12

4. (a) How stream generation is achieved through RC4 algorithm ? 8

(b) Describe the RSA algorithms. 8

(c) What is IPsec ? What are its services ? 4

5. (a) What is a message authentication code (MAC) ? Describe how does MAC ensure both authentication confidentiality. 3+7=10

(b) Describe a digital signature system using hash function. 10

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

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

(b) Describe the output feedback mode (OFB) of block ciphers. What are its advantages ? 8+3=11

(c) What are the advantages of counter mode (CTR) ? 4

7. (a) Decrypt the following plain text message using two stage columnar transposition technique using the key "4 5 1 2 3". "We are discovered. Save yourself". 6

(b) Define confidentiality and authentication. 4

(c) What is PGP ? Describe how can PGP functions be employed to achieve confidentiality and authentication. 10
