Total number of printed pages–4

53 (EC 711) CRGY

2019

CRYPTOGRAPHY

Paper : EC 711 (Back)

Full Marks : 100

Time : Three hours

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

*Answer **any five** questions.*

1. *(a)* Describe the working of Cipher Block Chaining mode. Find out expression for the ciplertext and the plaintext for *j*th stage. 8

   (b) How is stream generation achieved through RC4 algorithm ? 8

   (c) Describe a Triple DES system. 4

2. *(a)* What is a Message authentication code (MAC)? How does it ansure both authentication and confidentiality? 8

(b) Describe a digital signature scheme using hash function. 8

(c) What is IPSec? 4

3. *(a)* Illustrate the SSL record format. Describe various SSL specific protocals. 8

(b) Describe a Public-key Cryphotography system to prosid autheatication. 5

(c) Describe the working of *any one* of the Traditional Ciphers. Write its disadvantages, if any. 5+2=7

4. *(a)* Describe RSA algorithm. 6

(b) What is PGP? Describe how PGP can be used to provide both autheatication and confidentiality. 2+5=7

(c) Describe various kinds of Active Attacks that can take place. 7

5. *(a)* Describe the various components of a Digital signature system. 6

(b) Perform encryption and decryption using RSA algorithm for: 5

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

(c) Encrypt the following plaintext using Vignener cipher with key

"Shake". "Meet me in the evening".

(d) What are the differenances between a block cipher and a streem cipher? 3

6. *(a)* Define a secure hash function. What is an SSL session and an SSL connection? 6

(b) What are the design criteria for the F-function and S-boxes of Fiestel Block Cipher? 6

(c) Encrypt the following plaintext using Playfair cipher. Use the key "deceptive". "Defend the south-east wall". 5

(d) What are the sevices provided by IPSec? 3

Contd.

7. Write short notes on : 5×4=20

(i) Differeatial Cryptanalysis

(ii) Steganography

(iii) Fiestel Block Cipher and

(iv) S/MIME.
