Total number of printed pages–4

53 (EC 711) CRYY

2017

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 the working principle of Output Feedback (OFB) mode. Find expressions for C_j and P_j. 7

   (b) Perform encryption and decryption using RSA algorithm for the following : $p = 3; q = 13; e = 5; M = 10.$ 5

   (c) Describe *two* schemes to achieve digital signature using cryptographic hash function. 8

Contd.

2. *(a)* What is PGP ? Describe how can PGP functions be employed to achieve both confidentiality and authentication. 2·5+6·5=9

(b) Encrypt the following plain text message using a classical two-stage transposition technique. Take a key of your choice "meet me at the usual place at ten rather than eight O'Clock". 6

(c) What are the services provided by IP Sec ? 5

3. *(a)* Establish the fact that "at every round, the intermediate value of the decryption process is equal to the corresponding value of the encryption process with the two halves being swapped." — for Feistel Cipher. 10

(b) Describe the RSA algorithm. 10

4. *(a)* Explain why Double DES was found to be vulnerable to cryptanalytic attack. 6

(b) What is SSL ? Describe the SSL specific protocols. 2·5+6·5=9

(c) What are the essential ingredients of a public-key cryptosystem ? 5

5. (a) Describe the working principle of Differential Cryptanalysis. 6

(b) How stream generation is achieved through RC4 algorithm ? 6

(c) What is Messege Authentication Code (MAC) ? Describe how does MAC ensure both authentication and confidentiality. 2·5+5·5=8

6. (a) Differentiate between cryptography and steganography. Describe different means of steganography used in ancient times. 3+6=9

(b) How does public-key cryptography ensure authentication and secrecy ? 6

(c) Differentiate between block ciphers and stream ciphers. 5

7. *(a)* Describe SSL Record Protocol operation. 6

(b) What is S/MIME? Explain its functions. 2·5+5·5=8

(c) The following S-box is considered for DES :

2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

What is the output of the above S-box for input 011001 ? 6