53 (EC 711) CRYY

2018

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 PGP ? Describe how does PGP provide both confidentiality and authentication. 3+7=10

   (b) What is the main purpose of Message Authentication Code (MAC) ? How can MAC be used to provide authentication and confidentiality ? 3+7=10

2. *(a)* Describe how does "meet-in-the-middle" attack take place in double DES. 6

(b) Describe a Public-key cryptography system. What is a Cryptographic hash function? 5+3=8

(c) Decrypt the following message using playfair cipher with key "keyword".

L C N K Z K V F Y O G Q C E B W

6

3. (a) Explain the RSA algorithm. 6

(b) Describe the stream generation process by RC4. 7

(c) Decrypt the following cipher text using Vigenere cipher with key "Shake".

E R E D Q W N T O P W C H K R L Y A U I

7

4. (a) Describe a digital signature system, citing its important components. 5

(b) Show how can you achieve a digital signature scheme using cryptographic hash function. 6

(c) What is an Electronic Code Book ? Why is this mode of block cipher application not appropriate for longer amount of data? 6+3=9

5. (a) What are the functional areas of IPSec ? Mention the services provided by IPSec. 5+3=8

(b) Perform encryption and decryption using the RSA algorithm for

$p = 5$; $q = 7$; $e = 7$; $M = 12$.

6

(c) Explain the various steps involved in SSL Record Protocol operation. 6

6. (a) Illustrate the SSL record format. Describe various SSL specific protocols. 2·5+6·5=9

(b) Explain Triple DES using three keys. 5

(c) Explain the working of Cipher Block Chaining mode. 6

7. (a) Describe the functions provided by S/MIME. 6

(b) Explain the functioning of Differential Cryptanalysis. 8

(c) Discuss the design criteria for the F-function of Feistel cipher and the S-boxes. 6
