Total number of printed pages–3

53 (EC 711) CRGR

2016

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)* Discuss various web security threats. What are the security approaches that can be opted for web traffic ? 6+4=10

   (b) Show that for a Feistel Cipher — "the output of the first round of the decryption process is equal to a 32-bit swap of the input to the sixteenth round of the encryption process". 10

Contd.

2. *(a)* Describe SSL Record protocol operation. What are the services provided by SSL Record protocol. 6+4=10

(b) Describe various PGP cryptographic functions. 10

3. *(a)* Differentiate between block ciphers and stream ciphers. Give examples of each. 5+3=8

(b) Describe *any three* classical ciphers in brief. 3×4=12

4. *(a)* What is brute-force attack ? Discuss the concept of Linear Cryptanalysis. 3+7=10

(b) What are the various block cipher modes of operations ? Discuss *any one* of them, citing its merits and demerits. 2+8=10

5. *(a)* What do you mean by Message Authentication Code (MAC) ? Describe how can MAC be used to provide confidentiality, authentication and digital signature. 3+7=10

(b) Describe various security services defined in X.800. 10

6. (a) Describe a public-key encryption scheme. What is a cryptographic hash function? What is the purpose of S-boxes used in DES? 6+2+2=10

(b) Describe RSA algorithm. Why is it not desirable to reuse a stream cipher key? 8+2=10

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

(b) Describe a digital signature scheme. 7

(c) Write short notes on : 4+4=8

(i) IPsec and

(ii) S/MIME