Total number of printed pages–3

53 (IT 702) CRCS

2019

CRYPTOGRAPHY AND CYBER SECURITY

Paper : IT 702

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 Cryptography? What is Cryptanalysis?

   (b) What are CFB and OFB modes? Explain the significance of a Network Security model. 5+8+7=20

2. *(a)* Explain Stream Cipher and Block Cipher with examples. 10

   (b) Use additive cipher with key = 12 to encrypt the message "Happy" and show encrypted message. 10

Contd.

3. *(a)* Explain a single round of DES with block diagram. 10

(b) Explain the complete process of AES. 10

4. *(a)* Define Affine cipher. Show that the additive cipher and multiplicative cipher are special case of an affine cipher. 10

(b) Explain RSA algorithm in bbabc. Comment on the strength of this algorithm. 10

5. *(a)* Describe Diffie-Hellman Symmetric Key Exchange algorithm with an example. 10

(b) Explain how this process might become vulnerable. 10

6. *(a)* Given $p = 7$, $q = 17$, $N = p \times q$ and public key $e = 5$, compute the private key d corresponding to the RSA system. 10

(b) What is Firewall ? How does it resolve the security issues ? 10

7. Write short notes on ***any four*** of the following : 4×5=20

(a) S-DES

(b) RSA algorithm

(c) Comparison between Symmetric and Asymmetric Key Cryptography

(d) Brute-force attack

(e) Meet-in-the-middle attack.

———