Total number of printed pages–3

53 (IT 811) CGNS

2018

CRYPTOGRAPH AND NETWORK SECURITY

Paper : IT 811

Full Marks : 100

Time : Three hours

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

Answer ***any five*** *questions.*

1. What is Cryptography? What is Cryptanalysis attack? Explain Ciphertext-only attack and Known-plaintext attack.

2+4+7+7=20

2. What is CFB and CBC mode? Explain the significance of a network security model.

12+8=20

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

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

10+10=20

Contd.

4. *(a)* Compare between Symmetric and Asymmetric Key Cryptography.

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

(c) Given $p=19$, $q=29$, $N=p \times q$ and public key $e=17$, compute the private key d corresponding to the RSA system.

5+7+8=20

5. Describe Diffie-Hellman Symmetric Key Exchange algorithm with an example. Explain how this process might become vulnerable. 20

6. *(a)* Outline the broad level steps in SET.

(b) Explain with figure how SSL is accommodated in TCP/IP protocol suite.

10+10=20

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

(a) Stream Cipher and Block Cipher

(b) Kerberos

(c) Digital Signature

(d) IPSec services

(e) Virtual private network.

———