53 (IT 702) ISCL

2021

INFORMATION SECURITY AND CYBER LAWS

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)* Explain the following types of Security Attacks : 3×4=12

   (i) Interruption

   (ii) Interception

   (iii) Modification

   (iv) Fabrication.

   (b) Describe a model for network security. 8

2. *(a)* Describe the following five security services : 3×5=15

   (i) Confidentiality

   (ii) Authentication

   (iii) Integrity

   (iv) Access control

   (v) Availability.

   (b) Show the relation between security services and mechanism. 5

3. 5+7+8=20

   (a) Explain Symmetric Encryption Principles.

   (b) What is Cryptanalysis ? Mention *five* cryptanalytic attacks.

   (c) Draw the Feistel Cipher Structure.

4. 7+6+7=10

   (a) Describe Data Encryption Standard (DES).

   (b) What are the strengths and weaknesses of DES ?

   (c) How does Triple DES work ? Explain.

5. *(a)* What is AES ? Show the overall structure of AES. 2+8=10

(b) What is the difference between block cipher and stream cipher ? 2

(c) Write RC4 Algorithm. 8

6. *(a)* Explain the following two cipher block modes of operation : 5+5=10

(i) Cipher Block Chaining Mode

(ii) Counter Mode.

(b) Explain message authentication using one-way hash function while using—

(i) conventional encryption

(ii) public-key encryption

5+5=10

7. *(a)* Explain the working of PGP and S/MIME. 5+5=10

(b) What is IPR ? Describe the following two types of IPRs : 6

(i) Patent

(ii) Copyrights.

(c) How does a digital signature work ? Describe. 4

8. Write short notes on : 5×4=20

(i) Transport Layer Security

(ii) SNMP

(iii) Firewall

(iv) Cyber Crime in India.