53 (IT 702) ISCL

2018

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. What is Cryptography? What is Cryptanalysis? Explain Ciphertext — only attack and known-plaintext attack. 2+4+7+7=20

2. *(a)* Explain the significance of a network security model (with diagram).

   (b) Explain stream cipher and block cipher with examples. 20

3. *(a)* Use additive cipher with key = 15 to encrypt the message "hello" and show the encrypted message.

(b) Eve has intercepted the ciphertext "UVACLYF ZL JBYL". Show how she can use a brute-force attack to break the cipher. 20

4. *(a)* What is a Double DES? Explain the meet-in-the-middle attack.

(b) Explain a single round of DES with block diagram. 20

5. *(a)* Define affine cipher. Show that the additive cipher and multiplicative cipher are special case of affine cipher.

(b) What is the drawback of 3-DES? Describe various steps of encryption and decryption in AES algorithm. 20

6. *(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. 20

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

(b) Explain how this process might become vulnerable. 20
