Total number of printed pages–4

53 (CS 603) INFS

2021

INFORMATION SECURITY

Paper : CS 603

Full Marks : 100

Time : Three hours

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

*Answer **all** questions.*

1. 4+6=10

(a) What do you understand by Information Security?

(b) Explain Threat, Vulnerabilities and Attacks.

2. 2+6+2=10

(a) What is a modular arithmetic?

(b) Find — 10 mod 26 and 600 mod 31.

Contd.

(c) Find whether inverse exists for 10 modulo 26 or not.

3. 4+6=10

(a) What do you understand by stream cipher and block cipher?

(b) Explain the i^{th} round DES encryption schedule.

4. 6+4=10

(a) Explain Confidentiality, Integrity and Availability with example.

(b) How can confidentiality and integrity be preserved for a particular information exchange? Explain.

5. 5+5=10

(a) Encrypt the message "CIPHER" with the key "MONARCHY" using playfair cipher.

(b) Encrypt the message "CIPHER" with the key "LONG" using vigenere cipher.

6. 5+5=10

(a) Explain extended euclid algorithm for finding inverse of a number.

(b) Using extended euclid algorithm, find 17 inverse in modulo of 31.

7. 4+6=10

(a) What do you understand by Secret Key Cryptography and Public-Key Cryptography?

(b) Explain RSA algorithm.

8. 5+5=10

Perform the encryption and decryption using the RSA algorithm.

(a) $p = 5; q = 11; e = 3; M = 9$

(b) $p = 11; q = 13; e = 11; M = 7$

9. 5+2+3=10

(a) In a public-key system using RSA, you intercept the ciphertext $C = 10$ sent to a user whose public-key is $e = 5$, $n = 35$. What is the plaintext M?

(*b*) What is Euler's totient function ?

(*c*) Find $\phi(8)$.

10. Write short notes on : ***(any two)*** 5×2=10

(*a*) Confusion and Diffusion

(*b*) Message Authentication Code (MAC)

(*c*) Digital Signature

(*d*) IPSec.