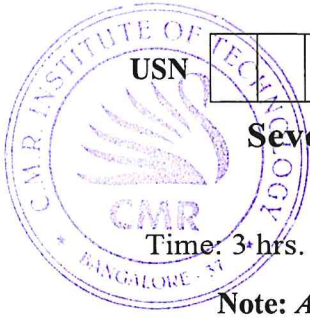


CBCS SCHEME



18CS744

Seventh Semester B.E. Degree Examination, July/August 2022 Cryptography

Time: 3 hrs.

Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

- 1 a. Using Hill Cipher technique, encrypt the plain text "Paymoremoney" using the key.
- $$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$
- [Hint : $a = 0$, $b = 1$, $z = 25$]. (08 Marks)
- b. Explain the playfair cipher and its rules for the following example.
Keyword : MONARCHY ; Plain text : Cryptography. (08 Marks)
- c. Define Substitution and Transposition techniques. (04 Marks)

OR

- 2 a. Explain DES Encryption algorithm, with neat diagram. (10 Marks)
- b. Explain Feistel encryption and Decryption algorithm, with neat diagram. (10 Marks)

Module-2

- 3 a. Explain Public – Key Cryptosystems. (10 Marks)
- b. Explain the description of the RSA algorithm. (10 Marks)

OR

- 4 a. Explain the Diffie – Hellman key exchange algorithm. (10 Marks)
- b. Describe Elgamal Cryptographic systems. (10 Marks)

Module-3

- 5 a. Explain Elliptic curve over real numbers. (10 Marks)
- b. Describe Micali – Schnorr pseudorandom Bit generator with neat diagram. (10 Marks)

OR

- 6 a. Explain Key – distribution Scenario, with neat diagram. (10 Marks)
- b. Explain Public – key authority technique proposed for the distribution of Public keys. (10 Marks)

Module-4

- 7 a. Describe Public key infrastructure, with neat diagram. (10 Marks)
- b. Explain Remote User – Authentication Principles. (10 Marks)

OR

- 8 a. Describe in detail PGP (Pretty Good Privacy) Cryptographic functions. (10 Marks)
- b. Explain DKIM (Domain Keys Identified Mail) functional flow with diagram. (10 Marks)

Module-5

- 9 a. Describe the application and benefits of IPsec. (10 Marks)
- b. Describe IP Security Architecture, with neat diagram. (10 Marks)

OR

- 10 a. Explain Internet Key Exchange (IKE) Key determination features. (10 Marks)
- b. Explain Basic Combinations of Security Associations. (10 Marks)

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

CMRIT LIBRARY
BANGALORE - 560 037

