

CBCS SCHEME

USN

--	--	--	--	--	--	--	--	--	--

15CS743

Seventh Semester B.E. Degree Examination, Feb./Mar. 2022 Information and Network Security

Time: 3 hrs.

Max. Marks: 80

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

Module-1

- 1 a. Define : i) Cryptology ii) Cryptography iii) Cryptanalysis. Compute encryption of the plaintext VSRQJHERE VTX DUHSDQWU using CAESAR cipher. Assume shift positions $k=3$. (08 Marks)
- b. Apply one time Pad to encrypt and decrypt the data given : heilhitter ; refer data $e = 000, h = 001, i = 010, k = 011, \ell = 100, r = 101, s = 110, t = 111$ and key : 7565740560. (08 Marks)

OR

- 2 a. Explain the concept of Project Venona and codebook cipher. (08 Marks)
- b. Explain the taxonomy of CRYPTOGRAPHY and CRYPTANALYSIS. (08 Marks)

Module-2

- 3 a. Describe in detail the technique of Tiger Hash algorithm with neat diagram. (08 Marks)
- b. Define Hash function. Explain the properties of Hash function. (08 Marks)

OR

- 4 a. Discuss the applications/uses of Hash function. (08 Marks)
- b. Explain the concept of SECRET sharing and information hiding. (08 Marks)

Module-3

- 5 a. Explain the need of randomness in cryptographic primitives and deterministic generator and non-deterministic generator approaches in detail. (08 Marks)
- b. Explain Zero knowledge analogy with example. (08 Marks)

OR

- 6 a. List the properties of PASSWORD and analyze the dynamic password scheme with neat diagram. (08 Marks)
- b. Explain Diffie – Hellman protocol against the typical AKE protocol security goals. (08 Marks)

Module-4

- 7 a. Explain the scope of key management and its lifecycle. (08 Marks)
- b. Illustrate different key generation techniques. (08 Marks)

OR

- 8 a. With a neat diagram, explain the Unique Key Per Transaction (UKPT) scheme in key establishment process. (08 Marks)
- b. Explain public key certificate management models. (08 Marks)

Module-5

- 9 a. Explain SSL protocols in detail with analysis of handshake protocol. (10 Marks)
- b. Explain the GSM authentication and encryption. (06 Marks)

OR

- 10 a. Write short notes on 'Attacks on WEP'. (06 Marks)
- b. Explain eID key management in detail. (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.