CBCS SCHEME

USN □□□□□□□□□□

15CS743

Seventh Semester B.E. Degree Examination, Jan./Feb. 2023
Information & 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 the basic terminologies of crypto. Explain the working of crypto as a black box. **(08 Marks)**

b. Explain four Cipher methods with suitable examples. **(08 Marks)**

OR

2 a. Apply our Time Pad to encrypt and derypt the data given :
heilhitler ; refer data
e – 000, h – 001, i – 010, k – 011, l – 100, r – 101, s – 110, t – 111 and
key : 7 5 6 5 7 4 0 5 6 0 **(06 Marks)**

b. Explain the Taxonomy of cryptography and cryptanalysis. **(10 Marks)**

Module-2

3 a. Explain the characteristics of cryptographic hash function by taking Birthday Attack problem as an example. **(08 Marks)**

b. With a neat diagram, explain the Outer round and inner round operations of Tiger hash algorithm. **(08 Marks)**

OR

4 a. Define Hash MAC (HMAC). Explain the working of HMAC in securing online bids and spam reduction. **(08 Marks)**

b. Write a short notes on : (i) Secret sharing (ii) Information Hiding. **(08 Marks)**

Module-3

5 a. List any four properties of non-deterministic and deterministic generators. Explain Nonce-based freshness mechanism **(06 Marks)**

b. Explain one-way function for UNIX password protection system. **(06 Marks)**

c. Explain in brief zero-knowledge mechanism. **(04 Marks)**

OR

6 a. List the stages and goals of protocol design. Explain the reflection attack against protocol 3. **(06 Marks)**

b. Analyze the Diffie-Hellman protocol against the typical AKE protocol security goals. **(06 Marks)**

c. Describe an AKE protocol based on key distribution. **(04 Marks)**

Module-4

7 a. What is key management? Explain the process of key Life Cycle. **(06 Marks)**

b. Explain a three-level key hierarchy system. **(06 Marks)**

c. Briefly explain the key storage mechanism. **(04 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.

OR

8 a. With suitable figure, explain a generic Unique Key Per Transaction (UKPT) schemes. **(06 Marks)**

b. Explain various public-key certificate management models. **(10 Marks)**

Module-5

9 a. Mention SSL Security requirements and explain how cryptography used in SSL. **(06 Marks)**

b. Explain how Wired Equivalent Privacy (WEP) mechanism protect WLAN communication. **(06 Marks)**

c. List security issues in SSL and WLAN. **(04 Marks)**

OR

10 a. Explain the main cryptographic design used in GSM Authentication and Encryption system. **(08 Marks)**

b. Explain various ways of cryptography used to secure payment card transaction. **(08 Marks)**

* * * * *