CBCS SCHEME

USN □□□□□□□□□□

17CS743

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

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Define cryptosystem with diagram. **(10 Marks)**
b. Explain simple substitution cipher with example. **(10 Marks)**

OR

2 a. Explain double transposition cipher with example. **(10 Marks)**
b. Explain one-time pad with example. **(10 Marks)**

Module-2

3 a. Explain cryptographic hash function with its characteristics. **(10 Marks)**
b. Explain the H-MAC. **(10 Marks)**

OR

4 a. Explain tiger-hash outer round with neat diagram. **(10 Marks)**
b. Explain the uses for hash functions. **(10 Marks)**

Module-3

5 a. Compare non-deterministic and deterministic generator. **(10 Marks)**
b. Compare the three freshness mechanisms with relevant parameters. **(10 Marks)**

OR

6 a. Explain cryptographic password protection with neat diagram. **(10 Marks)**
b. Explain dynamic password scheme with neat diagram. **(10 Marks)**

Module-4

7 a. Explain the key life cycle with its different phases with neat diagram. **(10 Marks)**
b. Explain the philosophy behind key hierarchies and simple key hierarchy with the diagram of three-level key hierarchy. **(10 Marks)**

OR

8 a. Explain key translation and key dispatch with diagrams. **(10 Marks)**
b. List and explain techniques used to provide tamper resistance. **(10 Marks)**

Module-5

9 a. List and explain the SSL security issues and SSL design issues. **(10 Marks)**
b. List and explain WLAN design issues. **(10 Marks)**

OR

10 a. List and explain cryptographic improvements over GSM. **(10 Marks)**
b. List and explain main design issues concerning the EID card scheme. **(10 Marks)**

* * * * *

fImportant 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.