**POORNIMA UNIVERSITY, JAIPUR**

**END SEMESTER EXAMINATION, November 2022**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **2BT3179** | Roll No. | Total Printed Pages: 1 |
| **2BT3179** |  |
| B. Tech. II Year III-Semester (Back) End Semester Examination, November 2022  **(CC/ CE)** | |
| **BCC03108 / BCE03108 : Information Security Fundamentals** | | | |

# Time: **3** Hours. Total Marks: **60**

Min. Passing Marks: **21**

Attempt **five** questions selecting one question from each Unit. There is internal choice from Unit I to Unit V. Marks of each question or its parts are indicated against each question / parts. Draw neat sketches wherever necessary to illustrate the answer. Assume missing data suitably (if any) and clearly indicate the same in the answer.

Use of following supporting material is permitted during examination for this subject.

# **1.--------------------------Nil--------------------** **2.------------------Nil-----------------------**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **UNIT-I (CO1)** | **Marks** |
| **Q.1** | **(a)** | Describe DES symmetric key cryptography algorithm. | **(6)** |
|  |  |  |  |
|  | **(b)** | Explain various transposition techniques | **(6)** |
|  |  | **OR** |  |
| **Q.2** | **(a)** | Explain various substitution techniques. | **(6)** |
|  |  |  |  |
|  | **(b)** | Write about biometric authentication. | **(6)** |
|  |  | **UNIT-II (CO2)** |  |
| **Q.3** | **(a)** | What is digital certification? How it can be achieved? | **(6)** |
|  |  |  |  |
|  | **(b)** | How key management is done in case of symmetric and asymmetric cryptography? | **(6)** |
|  |  | **OR** |  |
| **Q.4** | **(a)** | Generate public key and private key in case of RSA algorithm if two primes numbers giver is 7 and 13. p=7 and q=13. | **(6)** |
|  |  |  |  |
|  | **(b)** | How user authentication can be done with authentication token? | **(6)** |
|  |  | **UNIT-III (CO3)** |  |
| **Q.5** | **(a)** | Write the issues in GSM security? | **(6)** |
|  |  |  |  |
|  | **(b)** | Describe two types of cryptographic algorithms. | **(6)** |
|  |  | **OR** |  |
| **Q.6** | **(a)** | Explain Stream Cipher and Block Cypher with Example? | **(6)** |
|  |  |  |  |
|  | **(b)** | Define modern security standards? Differentiate between Black Hat and Grey Hat Hackers. | **(6)** |
|  |  | **UNIT-IV (CO4)** |  |
| **Q.7** | **(a)** | Enumerate different types of attacks on computer-based systems | **(6)** |
|  |  |  |  |
|  | **(b)** | Describe Steganography and Public-Key Infrastructure method? | **(6)** |
|  |  | **OR** |  |
| **Q.8** | **(a)** | What is cryptography? Discuss the different cipher methods with suitable Examples. | **(6)** |
|  |  |  |  |
|  | **(b)** | Explain Few Applications of Steganography? | **(6)** |
|  |  | **UNIT V (CO5)** |  |
| **Q.9** | **(a)** | Define Information Assets Ownership? | **(6)** |
|  |  |  |  |
|  | **(b)** | What Is Mobile Device Information Leakage? Explain Information Flow Tracking (IFT)? | **(6)** |
|  |  | **OR** |  |
| **Q.10** | **(a)** | Explain output feedback mode? | **(6)** |
|  |  |  |  |
|  | **(b)** | Explain the different methods to generate random numbers. | **(6)** |