Reg. No. \_\_\_\_\_\_\_\_\_\_\_\_\_



**End Semester Examination – Nov / Dec – 2019**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA2024** | **Duration :** | **3hrs** |
| **Sub. Name :** | **NETWORK SECURITY** | **Max. Marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Describe about the various security services and mechanism. | CO1 | 10 |
| b. | Discuss about the various attacks with relation to security goals. | CO6 | 10 |
| **(OR)** | | | | |
| 2. |  | Explain about the mathematics for cryptography in detail. | CO3 | 20 |
|  |  |  |  |  |
| 3. | a. | Find the multiplicative inverse of 23 in Z100. | CO4 | 10 |
| b. | Explain in detail about the Keyless Transposition ciphers. | CO4 | 10 |
| **(OR)** | | | | |
| 4. |  | Elaborate on two classes of product ciphers. | CO3 | 20 |
|  |  |  |  |  |
| 5. |  | Illustrate on Data Encryption Standard. | CO3 | 20 |
| **(OR)** | | | | |
| 6. |  | Analyze about the transformation and key expansion of Advanced Encryption Standard. | CO3 | 20 |
|  |  |  |  |  |
| 7. |  | Examine about the various cryptosystems in detail. | CO4 | 20 |
| **(OR)** | | | | |
| 8. |  | Give an outline about the following concept:   1. Message Authentication 2. Random Oracle Model 3. Pigeonhole Principle 4. Birthday Problem. | CO2 | 20 |
|  | | **Compulsory**: |  |  |
| 9. |  | Elaborate on digital signatures. | CO5 | 20 |