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



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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **18CS3102** | **Duration :** | **3hrs** |
| **Sub. Name :** | **PRINCIPLES OF CYBER SECURITY** | **Max. Marks :** | **100** |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course Outcome** | **Marks** |
| **ANSWER ANY FIVE QUESTIONS (5 x 16 = 80 Marks)** | | | | |
| 1. |  | List and explain the possible web-user side attacks and suggest suitable mitigating techniques for those attacks. | CO1 | 16 |
|  |  |  |  |  |
| 2. | a. | Explain in detail the various DDOS attacks and different layers of DDOS attacks. | CO1 | 10 |
| b. | Discuss the security enforcement procedures in the design of an operating system. | CO2 | 6 |
|  |  |  |  |  |
| 3. |  | Design a simple firewall configuration table and list the various types of firewalls. | CO4 | 16 |
|  |  |  |  |  |
| 4. |  | Illustrate the general structure of the data encryption standard and elaborate on the single round function of DES. | CO3 | 16 |
|  |  |  |  |  |
| 5. | a. | Elaborate on the international and national privacy principles and policies. | CO6 | 8 |
| b. | Discuss the privacy implications of any two emerging technologies. | CO2 | 8 |
|  |  |  |  |  |
| 6. | a. | Discuss the importance of the CIA triad and stress more closely on each of its elements. | CO3 | 8 |
| b. | List the possible ways of attacking a user through email. | CO4 | 8 |
|  |  |  |  |  |
| 7. | a. | Alice chooses q=11, p=23, h=16. Now Alice wants to transmit his message and signature to Bob with his secret number k = 5.  i) Calculate the global public elements.  ii) Find the public key of Alice with her chosen private key x=7.  iii) Verify the signature that is received by Bob along with the  hash code H(M) = 10.  Prove that the above process provides integrity for the data transferred against modification attacks. | CO5 | 8 |
| b. | Analyze a SHA-512 algorithm with a clear understanding of a single along with the process of deriving eighty 64-bit words from the 1024-bits for every block. | CO5 | 8 |
| **COMPULSORY QUESTION (1 x 20 = 20 Marks)** | | | | |
| 8. | a. | When is an attack on the cyber infrastructure considered to be an act of Warfare? List few attacks in the recent times that could be listed as Cyber Warfare. | CO1 | 10 |
| b. | Explain in detail the concept of electronic voting and what are the critical aspects to ensure a fair election process. | CO3 | 10 |