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



**UNIVERSITY**

(Karunya Institute of Technology & Sciences)

(Declared as Deemed-to-be University under Sec.3 of the UGC Act, 1956)

**End Semester Examination – Nov/Dec – 2017**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **14CS3064** | **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 Hashed Message Authentication Code with explanation of its security features. | CO1 | 10 |
|  | b. | Summarize the Rivest Shamir Adlemen encryption and decryption technique with the mathematical assumptions behind it. | CO1 | 10 |
| (OR) | | | | |
| 2. | a. | Define Message authentication Code? | CO1 | 2 |
| b. | Explain Secure hash Algorithm (SHA) 512. | CO1 | 15 |
| c. | Illustrate the difference between Hashing and message authentication code. | CO1 | 3 |
|  |  |  |  |  |
| 3. |  | Explain the cryptographic algorithms in Secure / Multipurpose Internet Mail Extension (S/MIME) with examples of signed and enveloped data formats. | CO1 | 20 |
| (OR) | | | | |
| 4. | a. | Appraise the protocols of Authentication Header (AH) and Encapsulating Security Payload (ESP) used in Internet Protocol Security (IPSec) services. | CO3 | 15 |
|  | b. | Compare and contrast tunnel mode and transport mode of operation in Internet Protocol Security (IPSec) services. | CO3 | 5 |
|  |  |  |  |  |
| 5. |  | Analyze Secure Socket Layer in detail in comparison with Transport Layer Security. | CO3 | 20 |
| (OR) | | | | |
| 6. | a. | Deduce the difference between Simple Network Management Protocol version1 and version2. | CO3 | 5 |
|  | b. | Evaluate the Simple Network Management Protocol version 3 in terms of packet format, message flow and message format. | CO3 | 15 |
|  |  |  |  |  |
| 7. | a. | Outline the requirement for intrusion detection system in modern networks? | CO3 | 5 |
|  | b. | Infer the types of intrusion detection systems with appropriate examples. | CO3 | 15 |
| (OR) | | | | |
| 8. | a. | Appraise the need for firewall. | CO3 | 5 |
|  | b. | Examine the types of firewall with diagrammatic explanations. | CO3 | 15 |
|  | |  |  |  |
|  | | **Compulsory**: |  |  |
| 9. | a. | Compare and contrast virus and worms. | CO2 | 5 |
|  | b. | Describe the structure and special characteristics of the Chernobyl virus and design its counter measures. | CO2 | 15 |

ALL THE BEST