****

**UNIVERSITY**

(Karunya Institute of Technology & Sciences)

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

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

**End Semester Examination – Nov/Dec - 2016**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Semester :** | **2016-17 ODD** |
| **Code :** | **09IT202/12IT208** | **Duration :** | **3 hrs** |
| **Sub. Name :** | **Cryptography and Network Security** | **Max. marks :** | **100** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Q. No.** | **Questions** | | **Marks** | | |
| **PART-A(10X1=10 MARKS)** | | | | | |
| 1. | Process of transforming plain text into cipher text is called\_\_\_\_\_\_\_\_\_\_ | | 1 | | |
| 2. | The principle of confidentiality ensures that only the sender and the intended recipients have access to contents of a message.(True/False) | | 1 | | |
| 3. | \_\_\_\_\_\_\_\_\_\_\_key is shared with everybody and \_\_\_\_\_\_\_key must be kept secret by the individual. | | 1 | | |
| 4. | In asymmetric key cryptography,\_\_\_\_\_\_\_ keys are required per communicating party. | | 1 | | |
| 5. | A \_\_\_\_\_\_\_\_\_\_\_\_can issue digital certificates. | | 1 | | |
| 6. | Define Kerberos. | | 1 | | |
| 7. | Email security can be achieved by the \_\_\_\_\_\_\_\_\_\_and \_\_\_\_\_\_\_\_\_\_\_\_\_ protocols | | 1 | | |
| 8. | \_\_\_\_\_\_is the world’s most widely used protocol for securing communications on the Internet. | | 1 | | |
| 9. | \_\_\_\_\_\_\_\_\_\_\_is a small program that causes harm to user’s computer and performs destructive activities. | | 1 | | |
| 10. | Define firewall. | | 1 | | |
| **PART B(5 X 3= 15 MARKS)** | | | | |
| 11. | List the principle security mechanisms. | | 3 | |
| 12. | Differentiate between Symmetric and Asymmetric Encryptions. | | 3 | |
| 13. | What are the desirable characteristics of hash function? | | 3 | |
| 14. | Give the functions provided by S/MIME. | | 3 | |
| 15. | Write down few guidelines for managing good passwords. | | 3 | |
| **PART C(5 X 15= 75 MARKS)** | | | |
| 16. |  | Explain in detail the attacks, mechanisms and services of OSI Security Architecture that is useful in organizing the task of providing security. |  |
| (OR) | | | |
| 17. |  | Draw the general structure of DES and explain a single round of the DES algorithm in detail. | 15 |
| 18. | a. | What are the limitations of symmetric key cryptography when compared to public key cryptography? | 3 |
| b. | Bring out the various steps involved in Diffie-Hellman key exchange with an example. | 12 |
| (OR) | | | |
| 19. |  | Explain RSA the popular asymmetric key cryptography with detailed procedure for encryption and decryption. |  |
| 20. |  | Illustrate HMAC with necessary sketch. |  |
| (OR) | | | |
| 21. |  | Explain the concept of Kerberos with necessary diagrams and exchange messages. |  |
| 22. |  | Summarize the services provided by PGP with clear diagrammatical explanation. |  |
| (OR) | | | |
| 23. |  | Discuss about IPSec Architecture, Benefits and Applications in detail. |  |
| 24. |  | Define Intruders and the classes of intruders. Discuss about the various intrusion. detection approaches that are effective against broad range of attacks. |  |
| (OR) | | | |
| 25. |  | Discuss about the firewall design with explicit explanation of its types. |  |

ALL THE BEST