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 – 2016**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Semester :** | **2016-17 ODD** |
| **Code :** | **14CS2008** | **Duration :** | **3hrs** |
| **Sub. Name :** | **CRYPTOGRAPHY AND NETWORK SECURITY** | **Max. marks :** | **100** |

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Explain the various kinds of security attacks on systems and networks; also discuss the possible countermeasures. | CO3 | 10 |
|  | b. | Encrypt the message “meet me at central library” using playfair cipher. (Hint: use the key “victory”) | CO1 | 10 |
| (OR) | | | | |
| 2. |  | List and explain the security services as given by X.800. | CO2 | 20 |
| 3. | a. | Discuss the strengths of DES. | CO2 | 5 |
| b. | Explain with details the AES transformation functions. | CO2 | 15 |
| (OR) | | | | |
| 4. | a. | Draw and explain single round of DES operation. | CO1 | 10 |
| b. | Illustrate the AES key expansion process with a suitable diagram. | CO1 | 10 |
| 5. | a. | Perform encryption and decryption using the RSA algorithm for the following:  p = 3; q = 11, e = 7;M = 5 | CO3 | 15 |
|  | b. | Describe the techniques used for the distribution of public keys. | CO2 | 5 |
| (OR) | | | | |
| 6. | a. | Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root 7.   1. If user A has private key 5, what is A’s public key? 2. If user B has private key 12, what is B’s public key? 3. What is the shared secret key? | CO1 | 10 |
|  | b. | Summarize the steps involved in ElGamal cryptosystem to encrypt and decrypt the given message. | CO3 | 10 |
| 7. | a. | With necessary sketch, explain HMAC algorithm. | CO2 | 10 |
|  | b. | Draw and explain the single round of SHA-512 operation. | CO1 | 10 |
| (OR) | | | | |
| 8. |  | Demonstrate the signing and verification process in DSS using the values given.  p=23; q=11; h=16; x=7; k=5; H(M)=10 | CO1 | 20 |
|  | | **Compulsory:** |  |  |
| 9. | a. | Explain with adequate diagram the transmission and reception of PGP messages. | CO2 | 10 |
|  | b. | Describe the various types of firewalls. | CO3 | 10 |

ALL THE BEST