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 – April / May – 2017**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **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. | Describe shiftrows and mixcolumns transformation of AES. | CO2 | 5 |
| b. | Explain the operation of S-Box operation in DES with suitable example. | CO2 | 15 |
| (OR) | | | | |
| 2. | a. | Compare and contrast AES and DES. | CO1 | 10 |
| b. | Illustrate the AES key expansion with a suitable diagram. | CO1 | 10 |
|  |  |  |  |  |
| 3. | a. | Perform encryption and decryption using the RSA algorithm for the following:  p = 5; q = 11, e = 3;M = 9 | CO3 | 15 |
|  | b. | Show that publick key crypto system enables authentication and confidentiality. | CO2 | 5 |
| (OR) | | | | |
| 4. | a. | Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 11 and a primitive root 2.   1. If user A has private key 9, what is A’s public key? 2. If user B has private key 3, 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 |
|  |  |  |  |  |
| 5. | a. | With necessary sketch, explain CMAC algorithm. | CO2 | 10 |
|  | b. | Explain the process of Message Digest Generation Using SHA-512. | CO1 | 10 |
| (OR) | | | | |
| 6. |  | Demonstrate the signing and verification process in DSS using the values given.  p=7; q=3; g=2; x=5; k=2; H(M)=3 | CO1 | 20 |
|  |  |  |  |  |
| 7. | a. | Explain Kerberos v5 authentication dialogue. | CO2 | 10 |
|  | b. | Describe the format of X.509 certificate. | CO3 | 10 |
| (OR) | | | | |
| 8. | a. | Explain with appropriate diagrams the transmission and reception of PGP messages. | CO2 | 10 |
|  | b. | Write short notes on the distributed intrusion detection. | CO3 | 10 |
|  | | **Compulsory:** |  |  |
| 9. | a. | Explain the various kinds of security attacks on systems and networks; also discuss the possible countermeasures. | CO3 | 10 |
|  | b. | Encrypt the message “Compuer viruses are harmful” using Caesar cipher. | CO1 | 5 |
|  | c. | Show that Caesar cipher is vulnerable to brute force attack. | CO2 | 5 |