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



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

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **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 a single round of Data Encryption Standard with an analysis of the number of rounds and discuss its strength and weakness. | CO2 | 10 |
| b. | Describe the security attacks, OSI security and the security mechanisms to counter the attacks. | CO1 | 10 |
| **(OR)** | | | | |
| 2. |  | Summarize the Advanced Encryption Standard with analysis of the key size, key expansion, s-box and decryption process. | CO2 | 20 |
|  |  |  |  |  |
| 3. | a. | Summarize the key management and key distribution issues with techniques for both symmetric and asymmetric keys. | CO1 | 10 |
| b. | Alice and Bob uses the Diffie-Hellman key exchange technique with a common prime *q = 7*, and a primitive root *α = 5*   1. Given *XA = 3*, and *XB =4*, find YA and YB. 2. Generate the shared secret key of both the parties and prove that the keys are the same.   Analyze each of the above steps with the maths behind Diffie-Hellman key exchange algorithm. | CO2 | 10 |
| **(OR)** | | | | |
| 4. | a. | Examine the ElGamal public Cryptosystem in detail. Perform the encryption and Decryption procedure using ElGamal technique for the given data:  **p/q = 23**, **g/α = 7**, **x/xA = 5** for the message **M=3** also the random integer, **k = 3**. | CO2 | 10 |
| b. | Explain the Elliptic Curve based algorithm with the analysis of the encryption and decryption process. | CO2 | 10 |
|  |  |  |  |  |
| 5. | 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.  1. Calculate the global public elements.  2. Find the public key of Alice with her chosen private key x=7.  3. 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. | CO3 | 10 |
| b. | Analyze the SHA-512 algorithm with clear understanding of a single round along with the process of deriving eighty 64-bit words from the 1024-bits for every block. | CO3 | 10 |
| **(OR)** | | | | |
| 6. | a. | Explain the authentication service provided by X.509 standard with inclusion of certificates, certificate authority hierarchy, certificate revocations and extensions. | CO1 | 10 |
| b. | Outline the various steps involved in hashed message authentication code (HMAC) using SHA-512. | CO1 | 10 |
|  |  |  |  |  |
| 7. | a. | Explain IP security architecture using a neat diagram. | CO1 | 10 |
| b. | Discuss in detail Encapsulating security payload. | CO1 | 10 |
| **(OR)** | | | | |
| 8. |  | Explain Kerberos version 5 protocol with illustrative diagrams of its advancement over Kerberos version 4. | CO3 | 20 |
|  | | **Compulsory**: |  |  |
| 9. | a. | Identify the classes of intruders with examples of intrusion attacks. | CO1 | 10 |
| b. | Discuss the handshake protocol of security socket layer (SSL) with relevant diagrams. | CO1 | 10 |