**20CB/CS/DS/IT603**

**Hall Ticket Number:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **III/IV B.Tech (Regular) DEGREE EXAMINATION** | | | |
| **July/August, 2023** | **Common to CB,CS,DS & IT Branches** | | |
| **Sixth Semester** | **Cryptography & Network Security** | | |
| **Time:** Three Hours | | **Maximum:**70 Marks | |
| ***Answer question 1 compulsory.*** | | | **(14X1 = 14Marks)** |
| ***Answer one question from each unit.*** | | | **(4X14=56 Marks)** |
|  | | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | a) | What is security? | | CO1 | L1 | 1 |
|  | b) | What are the security Goals to protect the message? | | CO1 | L1 | 1 |
|  | c) | Why S-Boxes are required in DES? | | CO1 | L1 | 1 |
|  | d) | Write the cipher text to the plain text “BEC CSE” using Rail Fence transposition cipher | | CO2 | L1 | 1 |
|  | e) | What is multiple DES? | | CO2 | L1 | 1 |
|  | f) | What is asymmetric cryptography? | | CO2 | L1 | 1 |
|  | g) | How can validate the data authentication? | | CO3 | L2 | 1 |
|  | h) | What is message authentication? | | CO3 | L1 | 1 |
|  | i) | What are digital Signature standards? | | CO4 | L1 | 1 |
|  | j) | What is PGP? | | CO4 | L1 | 1 |
|  | k) | List out the attacks on digital signatures. | | CO1 | L1 | 1 |
|  | l) | Draw SSL Message format for record protocol? | | CO1 | L2 | 1 |
|  | m) | Write a short note on security association. | | CO1 | L1 | 1 |
|  | n) | List out the two modes in security at the network layer. | | CO2 | L1 | 1 |
| **Unit-I** | | | | | | |
| 2 | (a) | | Encrypt the message ‘**this is exercise**’ using the following ciphers. Ignore the spaces between the words while encrypting.   1. Caesar cipher using the Key=5 2. Play fair using the key=’Monarchy’ | CO1 | L3 | 7M |
|  | (b) | | Discuss in detail about the security services and mechanisioms. | CO1 | L1 | 7M |
|  |  | | **(OR)** |  |  |  |
| 3 |  | | Describe the modes of modern Block Ciphers with design principles. | CO1 | L1 | 14M |
| **Unit-II** | | | | | | |
| 4 | a) | Perform the RSA algorithm on the given data and explain how encryption and decryption are performed on the message: p=17, q=31; e=7; M=2. | | CO2 | L3 | 7M |
|  | b) | Discuss the process of the message digest generation using SHA 512. | | CO2 | L2 | 7M |
| **(OR)** | | | | | | |
| 5 | a) | With a neat diagram illustrate the process of AES | | CO2 | L2 | 7M |
|  | b) | Write a short note on Robin Cryptosystem, and Elgamal Cryptosystem. | | CO2 | L2 | 7M |
| **Unit-III** | | | | | | |
| 6 | a)  b) | Explain five security services of PGP.  Explain e-mail system architecture? | | CO3  CO3 | L2  L2 | 7M  7M |
| **(OR)** | | | | | | |
| 7 | a) | Explain the concept of digital Signature with a neat diagram. | | CO3 | L2 | 7M |
|  | b) | Illustrate functioning process of Kerberos | | CO3 | L1 | 7M |
| **Unit-IV** | | | | | | |
| 8 | a) | Illustrate the SSL services with a neat architecture along with the four protocols. | | CO4 | L2 | 14M |
|  |  |  | |  |  |  |
| **(OR)** | | | | | | |
| 9 | a) | Write a short note on security protocols and security policy in network layer. | | CO4 | L2 | 7M |
|  | b) | Describe any four ISAKMP payload types listing the parameters of the payload. | | CO4 | L2 | 7M |

