**18CS603**

**Hall Ticket Number:**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **III/IV B.Tech (Regular) DEGREE EXAMINATION** | | | |
| **July, 2021** | **Computer Science & Engineering** | | |
| **Sixth Semester** | **Cryptography & Network Security** | | |
| **Time:** Three Hours | | **Maximum :** 50 Marks | |
| *Answer Question No.1 compulsorily.* | | | (10X1 = 10 Marks) |
| *Answer ONE question from each unit.* | | | (4X10=40 Marks) |

**1.** Answer all questions (10X10=10 Marks)

|  |  |
| --- | --- |
| a. | Define Diffusion. |
| b. | Distinguish between Stream Cipher and Block Cipher. |
| c. | Distinguish between Asymmetric Encryption and symmetric Encryption? |
| d. | Define primitive root? |
| e. | Who is an intruder? |
| f. | What types of attacks are addressed by message authentication? |
| g. | Define hash function? |
| h. | What are the four protocols of SSL? |
| i. | What is the abbreviation of ISAKMP? |
| j. | What is malicious software? |

**UNIT – I**

|  |  |  |
| --- | --- | --- |
| 2.a | Explain security services and mechanisms? | 5M |
| 2.b | Explain in detail about any two substitution ciphers with suitable examples. | 5M |

**(OR)**

|  |  |  |
| --- | --- | --- |
| 3. | Explain in detail AES encryption and decryption with neat sketch. | 10M |

**UNIT – II**

|  |  |  |
| --- | --- | --- |
| 4.a | State and prove the following: i)Fermat Theorem ii) Euler’s Theorem. | 5M |
| 4.b | Describe RSA algorithm? Perform encryption/decryption using RSA algorithm with instances: p=3; q=11,e=7;m=5 | 5M |

**(OR)**

|  |  |  |
| --- | --- | --- |
| 5.a | Explain in detail about SHA-512. | 5M |
| 5.b | Briefly discuss the security in HMAC. | 5M |

**UNIT – III**

|  |  |  |
| --- | --- | --- |
| 6.a | List and explain the services provided by PGP? | 5M |
| 6.b | Discuss the Kerberos authentication service with neat sketch. | 5M |

**(OR)**

|  |  |  |
| --- | --- | --- |
| 7.a | Discuss the x.509 directory authentication service. | 5M |
| 7.b | Explain in detail about digital signature algorithm. | 5M |

**UNIT – IV**

|  |  |  |
| --- | --- | --- |
| 8.a | Explain in detail IP security architecture with neat diagram. | 5M |
| 8.b | Explain in detail about SSL protocol. | 5M |

**(OR)**

|  |  |  |
| --- | --- | --- |
| 9.a | Explain about two security protocols of network layer. | 5M |
| 9.b | Write a short note on internet key exchange. | 5M |

