**18CS603**

**Hall Ticket Number:**

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

|  |  |  |  |
| --- | --- | --- | --- |
| **III/IV B.Tech (Regular/Supplementary) DEGREE EXAMINATION** | | | |
| **June, 2022** | **Computer Science & Engineering** | | |
| **Sixth Semester** | **Cryptography & Network Security** | | |
| **Time:** Three Hours | | **Maximum: 5**0 Marks | |
| *Answer Question No. 1 Compulsorily.* | | | (10X1 = 10 Marks) |
| *Answer* ***ANY ONE*** *question from each Unit.* | | | (4X10=40 Marks) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1. | a) | Find out Cipher text for the message “COLLEGE” by using additive Cipher with key = 15. | CO1 | |  |
|  | b) | Define ‘Confusion’ and ‘Diffusion’ terms. | CO1 | |  |
|  | c) | Distinguish between Asymmetric Encryption and symmetric Encryption? | CO2 | |  |
|  | d) | Find the primitive root of 11. | CO2 | |  |
|  | e) | What is the difference between private key and public key? | CO2 | |  |
|  | f) | What is an authentication service? | CO1 | |  |
|  | g) | What types of attacks are addressed by message authentication? | CO3 | |  |
|  | h) | Define hash fuction. | CO3 | |  |
|  | i) | What is email security? | CO4 | |  |
|  | j) | Define KDC. | CO4 | |  |
| **Unit - I** | | | | | |
| 2. | a) | Discuss in detail about Security Mechanisms. | CO1 | **5M** | |
|  | b) | Encrypt the message "**meet me at the usual place at ten rather than eight o clock**" using the Hill cipher with the key. Show your calculations and the result. | CO1 | **5M** | |
|  |  | **(OR)** |  |  | |
| 3. |  | Explain in detail DES encryption and decryption with neat sketches. | CO1 | **10M** | |
| **Unit - II** | | | | | |
| 4. | a) | Explain in detail about RSA Cryptosystem with an example. | CO2 | **5M** | |
|  | b) | Briefly discuss the security on hash functions and MAC’s. | CO2 | **5M** | |
|  |  | **(OR)** |  |  | |
| 5. | a) | Explain in detail about SHA-512 Algorithm. | CO2 | **5M** | |
|  | b) | What is Chinese Reminder Theorem? Explain with the following example.  x≡ 7 mod 13 and x ≡ 11 mod 12. | CO2 | **5M** | |
| **Unit - III** | | | | | |
| 6. | a) | What is meant by digital signature? Explain digital signature standard algorithm. | CO3 | **6M** | |
|  | b) | Discuss the Kerberos authenticated protocol in detail with neat sketch. | CO3 | **4M** | |
|  |  | **(OR)** |  |  | |
| 7. | a) | Discuss the Diffie - Hellman Key Exchange algorithm | CO3 | **5M** | |
|  | b) | Explain E-mail security package Pretty Good Privacy operation. | CO3 | **5M** | |
| **Unit - IV** | | | | | |
| 8. |  | Explain in detail SSL protocol operations with neat sketches? | CO4 | **10M** | |
|  |  | **(OR)** |  |  | |
| 9. |  | Write short notes on  i) IP security architecture  ii) Internet Key Exchange | CO4 | **10M** | |

****