|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Seat No.** |  |  |  |  |  |  |  |  |

**KADI SARVA VISHWAVIDYALAYA**

**B.E. Semester-VI Examination (April -2019)**

SUBJECT CODE: CE-601 SUBJECT NAME: Cryptography and Network Security

DATE: 12/4/2019 TIME: 10:30 A.M to 1:30 P.M TOTAL MARKS: 70

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Instructions:

1. Answer each section in separate Answer Sheet.

2. Use of scientific Calculator is permitted.

3. All questions are compulsory.

4. Indicate clearly, the options you attempted along with its respective question number.

5. Use the last page of main supplementary for rough work.

**SECTION – 1**

|  |  |  |  |
| --- | --- | --- | --- |
| **Q-1.** | **a)** | Perform encryption and decryption using RSA for p=11, q=13, e=11, M=7. | **5** |
|  | **b)** | Encrypt the message “The Royal Army” using Playfair cipher where key is “cipher”. | **5** |
|  | **c)** | Explain AES with figure. (detailed explanation on individual functional block may not be required) | **5** |
|  |  | **OR** |  |
|  | **c)** | Explain single round of DES with figure. | **5** |
|  |  |  |  |
| **Q-2.** | **a)** | Explain block cipher design principles. | **5** |
|  | **b)** | Explain Extended Euclidean theorem with one example. | **5** |
|  |  | **OR** |  |
| **Q-2.** | **a)** | Differentiate between block cipher and stream cipher. Explain any two, block cipher modes of operation. | **5** |
|  | **b)** | State and prove Fermat theorem. | **5** |
|  |  |  |  |
| **Q-3.** | **a)** | Explain CIA model for network security. | **5** |
|  | **b)** | Explain any two schemes for distribution of public keys. | **5** |
|  |  | **OR** |  |
| **Q-3.** | **a)** | Explain specific security mechanisms. | **5** |
|  | **b)** | Explain how we can use public key cryptography for distribution of secret keys. | **5**  **P.T.O** |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **SECTION – 2** |  |
| **Q-4.** | **a)** | Explain Content Integrity and Strong authentication in relation with Network security. | **5** |
|  | **b)** | Explain any two intrusion detection systems. | **5** |
|  | **c)** | Explain PGP services. | **5** |
|  |  | **OR** |  |
|  | **c)** | Explain the format of PGP message. | **5** |
|  |  |  |  |
| **Q-5.** | **a)** | Explain Diffie Hellman Key Exchange algorithm. | **5** |
|  | **b)** | What is the need of firewall? Explain types of firewall. | **5** |
|  |  |  |  |
| **Q-5.** | **a)** | Explain Elgamal algorithm. | **5** |
|  | **b)** | Explain S/MIME functionalities. | **5** |
|  |  |  |  |
| **Q-6.** | **a)** | Explain Digital signatures. | **5** |
|  | **b)** | Explain MD5. | **5** |
|  |  | **OR** |  |
| **Q-6.** | **a)** | Explain basic uses of MAC. | **5** |
|  | **b)** | Explain SHA-512 with figure. | **5** |

**\*\*\*\*\*\*BEST OF LUCK\*\*\*\*\*\***

|  |
| --- |
|  |