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

**KADI SARVA VISHWAVIDYALAYA**

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

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

DATE:13/11/2019 TIME: 12:00 noon to 3:00 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. Indicateclearly, 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)** | Differentiate passive attack and active attack with example. | **5** |
|  | **b)** | Explain CIA model for network security. | **5** |
|  | **c)** | Explain Differential cryptanalysis. | **5** |
|  |  | **OR** |  |
|  | **c)** | Explain Feistel cipher structure. | **5** |
|  |  |  |  |
| **Q-2.** | **a)** | Explain any two block cipher modes of operation. | **5** |
|  | **b)** | Explain Euler theorem. | **5** |
|  |  | **OR** |  |
| **Q-2.** | **a)** | Explain block cipher design principles. | **5** |
|  | **b)** | Explain Fermat theorem. | **5** |
|  |  |  |  |
| **Q-3.** | **a)** | Explain 3DES and discuss attacks possible on 3DES. | **5** |
|  | **b)** | Solve for encryption using hill cipher, key is ‘GYBNQKURP’ and plaintext is ‘ACT’. | **5** |
|  |  | **OR** |  |
| **Q-3.** | **a)** | Explain 2DES and discuss attacks possible on 2DES. | **5** |
|  | **b)** | Explain vigenere cipher with example. | **5** |
|  |  |  |  |
|  |  |  | **P.T.O** |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **SECTION – 2** |  |
| **Q-4.** | **a)** | Explain RSA algorithm. | **5** |
|  | **b)** | Explain principles of public key cryptography. | **5** |
|  | **c)** | Discuss applications of hash functions. | **5** |
|  |  | **OR** |  |
|  | **c)** | Discuss applications of Digital Signature. | **5** |
|  |  |  |  |
| **Q-5.** | **a)** | Explain structure of secure hash code. | **5** |
|  | **b)** | Explain honeypots. | **5** |
|  |  | **OR** |  |
| **Q-5.** | **a)** | What is Firewall? Explain types of Firewall. | **5** |
|  | **b)** | Explain Diffie Hellman Key Exchange. | **5** |
|  |  |  |  |
| **Q-6.** | **a)** | Explain MAC. | **5** |
|  | **b)** | Give overview of Kerberos version 4. | **5** |
|  |  | **OR** |  |
| **Q-6.** | **a)** | Explain S/MIME functionalities. | **5** |
|  | **b)** | Explain MD5 algorithm. | **5** |

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

|  |
| --- |
|  |