|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Enrollment No.** |  |  |  |  |  |  |  |  |  |  |  |  |  |

**KADI SARVA VISHWAVIDYALAYA**

**LDRP INSTITUTE OF TECHNOLOGY & RESEARCH, GANDHINAGAR**

**B.E. MID-SEMESTER EXAMINATION March 2019**

|  |  |
| --- | --- |
| **Date :- 5/3/2019** | **Branch: CE** |
| **Subject Name & Code: Cryptography and Network Security (CE-601)** | **Semester :6th** |
| **Time: 12:15 pm to 1:45 pm** | **Max. Marks :- 30** |

Instructions: 1) All questions are **compulsory**.

2) Figures to the **right** indicate full marks.

3) Indicate **clearly**, the options you attempt along with its respective question number.

4) Use the last page of main supplementary for **rough work**.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Marks** |
| **Q.1** | **(A)** | What are the key principles of security and Explain the role of session key in public key schemas. | **[5]** |
|  | **(B)** | Calculate multiplicative inverse of the following using extended Euclid theorem   1. 50mod71 2. 43mod64 | **[5]** |
|  |  |  |  |
| **Q.2** | **(A)** | Explain RSA algorithm with example. | **[5]** |
|  | **(B)** | Explain single round of DES. | **[5]** |
|  |  | **OR** |  |
| **Q.2** | **(A)** | Explain any two block cipher modes of operation. | **[5]** |
|  | **(B)** | Discuss evaluation criteria for AES**.** | **[5]** |
|  |  |  |  |
| **Q.3** | **(A)** | Differentiate passive and active attacks with example. | **[5]** |
|  | **(B)** | Explain Fermat theorem. | **[5]** |
|  |  | **OR** |  |
| **Q.3** | **(A)** | List out four categories of security threats and explain any two threat with example. | **[5]** |
|  | **(B)** | Explain Euler theorem. | **[5]** |

Best of Luck