

**#CNS (20CP320P)**

Name: Jatin Prajapati

Roll No: 21BCP452D

Branch: Computer

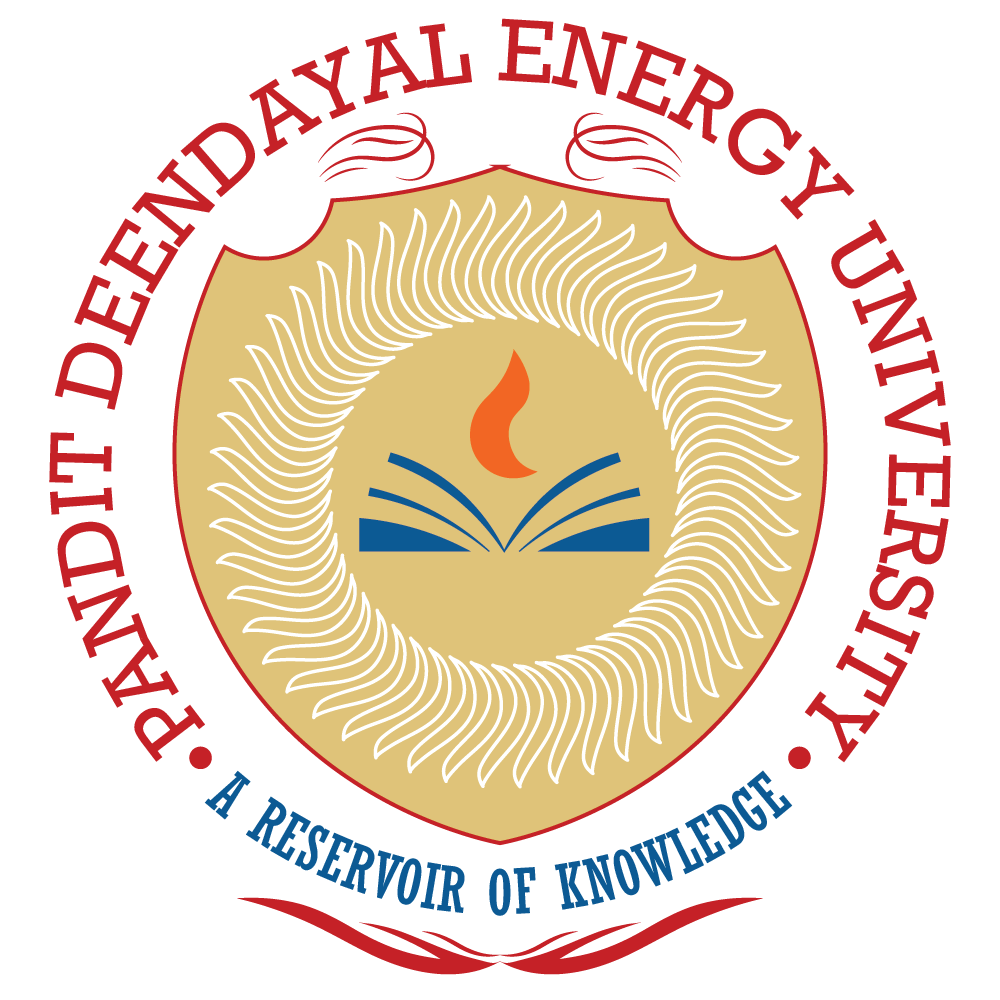
Semester: 6th

Division: 5th (G-10)

**PANDIT DEENDAYAL ENERGY UNIVERSITY**

**COMPUTER SCIENCE AND ENGINEERING DEPARTMENT**





This is to certify that **Mr. JATIN RAKESHBHAI PRAJAPATI** Enrolment number **21BCP452D** of 6th Semester Degree course in **Computer Science and Engineering** has satisfactorily prepared and presented his Term Work in **Cryptography and network security lab (20CP320P)** within four walls of the laboratory of this Institute during **JANUARY 2024** to **APRIL 2024.**

**CERTIFICATE**

Date of Submission: . Submitted To: .

|  |  |  |  |
| --- | --- | --- | --- |
| SR.NO | TITLE | PAGE | MARKS |
| 1 | Implementation of SDES encryption and decryption algorithm |  |  |
| 2 | Application of Brute force attack on SDES |  |  |
| 3 | Implementation of Extended Euclidean Algorithm |  |  |
| 4 | Implementation of RSA with all required algorithms |  |  |
| 5 | Demonstration of CCA2 attack on RSA |  |  |
| 6 | Implementation of Elgamal Algorithm for Encryption |  |  |
| 7 | Implementation of Elgamal Algorithm for Digital Signature |  |  |
| 8 | Implementation of your own designed pseudorandom number generation |  |  |
| 9 | Implement Shamir secret sharing scheme |  |  |
| 10 | Implementation of SHA 256 |  |  |
| 11 | Implementation of PBC library and performing bilinear pairing operation |  |  |
| 12 | Use Wireshark tool to view the network traffic passing across your lab computers |  |  |

**#INDEX**