

**Department of Computer Engineering**

**Name : Shaikh Adnan Shaukat Ali**

**Roll No : 76**

**Class/Sem : TE/VI**

**Branch : Computer**

**Year : 2021-22**

**Subject : Cryptography and System Security(CSS)**



|  |  |  |
| --- | --- | --- |
| **Expt. No.** | **Date** | **Name of the Experiment** |
| 1 | 27/1/2022 | Find the multiplicative inverse of any number Zn using Extended  Euclidean algorithm. Also find the gcd and t values. Show the output of each step. |
| 2 | 27/1/2022 | Implementation of Euler’s Totient Function. |
| 3 | 8/2/2022 | To implement Caeser cipher (Encryption and Decryption). |
| 4 | 24/3/2022 | To implement a program in python for password cracking using Brute Force Method. Password contains only lower alphabet characters. Length of password is 4. |
| 5 | 24/3/2022 | Implementation of RSA Cryptosystem, which includes:  a. Implementation of RSA Key Generation Algorithm.  b. Encryption and decryption using RSA algorithm. |
| 6 | 24/3/2022 | For varying message sizes, generate message digest using MD5 algorithm and check the integrity of message. |
| 7 | 24/3/2022 | For varying message sizes, generate message digest using SHA-1 algorithm and check the integrity of message. |
| 8 | 4/4/2022 | Implementation of Diffie Hellman Algorithm in python. Also, perform Diffie Hellman Practical using Cryptography lab of Virtual labs of IIT Bombay. |
| 9 | 5/5/2022 | Study of packet sniffer tool “wireshark”:  a. Download and install wirshark and capture icmp,tcp,and http packets in promiscuous mode.  b. Explore how the packets can be traced based on different filters. |
| 10 | 13/4/2022 | Study the use of network reconnaissance tools like WHOIS, dig, tracert, nslookup. |
| 11 | 13/4/2022 | Perform Digital Signature Scheme Experiment using Cryptography lab of Virtual labs of IIT Bombay. |

**INDEX**

**Prof. Ritu Jain**

**Subject I/C**

**Prof. Sujata Bhairnallykar**

**H.O.D**

**Prof. Ritu Jain**

**Subject I/C**

**Subject I/C**



**INDEX**

|  |  |  |
| --- | --- | --- |
| **Assign. No.** | **Date** | **Name of the Experiment** |
| 1 | 17/3/2022 | Assignment 1 |
| 2 | 15/4/2022 | Assignment 2 |

**Prof. Sujata Bhairnallykar**

**H.O.D**

**Prof. Ritu Jain**

**Subject I/C**