**SVKM’s NMIMS**

**MPSTME**

**Electronics and Telecommunication Engineering Department**

**Subject: Data Encryption and Network Security Programme: B.Tech**

**Sem: VIII ACAY: 2019-20**

**EXPERIMENT NO. 3**

|  |  |
| --- | --- |
| **Aim:** | 1. To write a program to find multiplicative inverse a a given number in 2. To implement Affine Cipher |
| **Software** | Python |
| **Theory** | **Affine Cipher** is a combination of additive and multiplicative cipher. **Additive ciphers** are sometimes referred to as shift ciphers or substitution ciphers. In **multiplicative cipher**, the encryption algorithm specifies multiplication of the plain text by the key and decryption algorithm specifies division of the cipher text by the key. However, since the operations are in , the decryption here means multiplying by multiplicative inverse of the key. So the key needs to belong to the set to guarantee that the encryption and decryption are inverses of each other.  Note: Here is a subset of which only includes number from that have unique multiplicative inverse. |
| **Algorithm** | **Affine Cipher**   1. Enter the plain text. 2. Enter key from which has a unique multiplicative inverse. 3. Enter key from 4. For encryption: 5. For decryption: |
| **Program and Output** | To be attached. |
| **Conclusion** | To be written by the student |
| **References** | 1. William Stallings, Cryptography and Network Security, Pearson Education Asia Publication, 5th edition, 2013. 2. Behrouz A. Forouzan and Debdeep Mukhopadhyay, Cryptography and Network Security, Mc Graw Hill, 2nd edition, 2013. |

**Student Submission**

|  |  |
| --- | --- |
| Name |  |
| Roll No. |  |
| Program/Semester |  |
| Subject |  |
| Expt Title |  |