 *DEPARTMENT OF INFORMATION TECHNOLOGY*

|  |  |
| --- | --- |
| Semester | S.E. Semester V – Information Technology Engineering |
| Subject | Security Lab |
| Subject Professor In-charge | Prof. Vinita Bhandiwad |
| Assisting Teachers | - |
| Laboratory | MS Teams |

|  |  |  |
| --- | --- | --- |
| Student Name | Satyam Mishra | |
| Roll Number | 20101A0021 | |
| Grade and Subject Teacher’s Signature |  |  |

|  |  |  |
| --- | --- | --- |
| Experiment Number | 3 | |
| Experiment Title | Implement Affine Cipher | |
| Resources / Apparatus Required | Hardware:  Basic Desktop with Windows or Linux. | Software: Python |
| Objectives  (Skill Set / Knowledge Tested / Imparted) | To understand Encryption Decryption using Affine ciphering method. | |
| Theory: | **Affine Method:**  **Definition:** It is a substitution cipher in which the alphabet in the plain text is multiplied by a variable key 1,i.e, multiplicative key and then added with another key 2 , i.e, additive key down the alphabet.  **Formula:** To encrypt – [(p\*k1)+k2] mod 26, where p=plain text  k1 =multiplicative key k2=additive key  To decrypt - (p-k2)\*k1^-1) mod 26, where p=plain text  K1^-1 = multiplicative inverse of key1  **Advantages:** 1. It can work with very large keys  2. Encrypted key is complex which gives more security  **Disadvantages**: 1.Possiblity of decryption by following the algorithm  **Code:**  x = 26  k1= int(input("Enter the key1:"))  k2 = int(input("Enter the key2:"))  text=input("Enter the plain text:")  msg=""  #encryption  for i in range(len(text)):  t=text[i]  if t.isupper():  j= ((((ord(t)-65)\*k1)+k2)%26)+65  elif t.isspace():  j=32  else:  j= ((((ord(t)-97)\*k1)+k2)%26)+97    msg=msg+chr(j)  print("Cipher text:",msg)  n = min(x,k1)  hcf = 0  for i in range(1,n+1):  if x%i == 0 and k1%i == 0:  hcf = i    if (hcf==1):  r1=26  r2=k1  t1=0  t2=1  while r2>0:  q=r1//r2  r=r1%r2  t=t1-(q\*t2)  r1=r2  r2=r  t1=t2  t2=t  if(r1==1):  if(t1<0):  inv=t1+26  else:  inv=t1+0  print("Multiplicative inverse:",inv)  else:  print("invalid key")    #decryption  msgo =""  for i in range(len(msg)):  m=msg[i]  if m.isupper():  p=(((ord(m)-65)-k2)\*inv)%26+65  elif m.isspace():  p=32  else:  p=(((ord(m)-97)-k2)\*inv)%26+97  msgo=msgo+chr(p)  print("Decrypted msg:",msgo) | |
| Output |  | |
| Conclusion | In this experiment, we learned how to encrypt plain text and decrypt the cypher text using Affine method | |