|  |  |
| --- | --- |
|  | **Department of Information Technology** |

|  |  |
| --- | --- |
| **Semester** | T.E. Semester V – INFT |
| **Subject** | Computer Network Security |
| **Laboratory Teacher:** | Prof. Vinita Bhandiwad |
| **Theory**  **Teacher:** | Prof. Vinita Bhandiwad |
| **Laboratory** | Microsoft Teams |

|  |  |  |
| --- | --- | --- |
| **Student Name** | Pranali Sharad Darekar | |
| **Roll Number** | 19101B0032 | |
| **Grade and Subject Teacher’s Signature** |  |  |

|  |  |  |
| --- | --- | --- |
| **Experiment Number** | 1 | |
| **Experiment Title** | Implementation of Substitution Cipher - Additive Cipher | |
| **Objective** | To apply the knowledge of symmetric cryptography to implement classical ciphers. | |
| **Resources / Apparatus Required** | Hardware:  PC with the Configuration of Intel Dual core Processor or higher, Minimum 2 GB RAM, Minimum 40 GB Hard disk, Network interface card. | Software:  Python 3.9/Pycharm |
| **Theory** | Additive Cipher is a type of monoalphabetic substitution cipher. In this ciphering method for encryption or encoding we add the key into value of particular text and then take modulus of 26 for it. And similarly for decryption or decoding we subtract the key from value of letter . Additive Cipher is the most basic ciphering method. So, the disadvantage of additive cipher is that it can be easily hacked as the intruder will know the key after trying to decrypt some text immediately.  E = ( P + K ) % 26  D = ( P - K) % 26 | |
| **Code** | text = [**'a'**, **'b'**, **'c'**, **'d'**, **'e'**, **'f'**, **'g'**, **'h'**, **'i'**, **'j'**, **'k'**, **'l'**, **'m'**, **'n'**, **'o'**, **'p'**, **'q'**, **'r'**, **'s'**, **'t'**, **'u'**, **'v'**,  **'w'**, **'x'**, **'y'**, **'z'**]   def encrypt(plaintext, k):  result = **""** for i in plaintext:  if i != **" "**:  result += text[(text.index(i) + k) % 26]  else:  result += plaintext[i]  return result   def decrypt(ciphertext, k):  result = **" "** for i in ciphertext:  if i != **" "**:  result += text[(text.index(i) - k) % 26]  else:  result += ciphertext[i]  return result   choice = 0 while True:  print(**"-"** \* 25, **"ADDITIVE CIPHERING METHOD"**, 25 \* **"-"**)  print(**"1. Generate Cipher Text**\n**2. Generate Plain Text**\n**3. Quit"**)  choice = int(input())  if choice == 3:  break  if choice == 1:  plaintext = input(**"Enter Plain Text:**\n**"**)  k = int(input(**"Enter key:"**))  print(**"Cipher Text :"**, encrypt(plaintext, k))  elif choice == 2:  ciphertext = input(**"Enter Cipher Text:**\n**"**)  k = int(input(**"Enter key:"**))  print(**"Plain Text :"**, decrypt(ciphertext, k))  else:  print(**"Invalid choice!!!"**) | |
| **Output** |  | |