Experiment Number: 1

UID : 2019140050 **Name: Tanvi Sunil Pen**

Batch: C **Branch: TE IT**

Aim:

1)To implement Substitution, ROT 13, Transposition, Double Transposition, and Vernam Cipher in Scilab/C/Python/R.

For this experiment I have implemented the Cipher techniques in Python

Program:

```
#Implementation of various cryptography methods
print("Select the Cryptography Method you want to implement :")
print("1: Substitution method")
print("2: ROT 13 method")
print("3: Transposition method")
print("4: Double Transposition method")
print("5: Vernam Cipher method")
print("6: End Program")
loop=True
while loop:
  choice=int(input("\nEnter Your Choice : "))
  if choice==1:
    print("1. Substitution method")
    text1=input("Enter the text to be encrypted :")
    k=int(input("Enter the no. of Position shift :"))
    text2=""
    print("The Encrypted Message is: ")
    for i in range(0,len(text1)):
      if ord(text1[i])+k<=122:
        print(chr(ord(text1[i])+k),end="")
        text2+=chr(ord(text1[i])+k)
      else:
        print(chr(ord(text1[i])+k-26),end="")
        text2+=chr(ord(text1[i])+k-26)
    print()
    print("The Decrypted Message is: ")
    for i in range(0,len(text2)):
      if ord(text2[i])-k>=97:print(chr(ord(text2[i])-k),end="")
      elif ord(text2[i])-k==32:print(chr(ord(text2[i])-k),end="")
      else:print(chr(ord(text2[i])-k+26),end="")
    print()

  elif choice==2:
```

```
  print("2. ROT 13 method")
  text1=input("Enter the text to be encrypted :")
  print("The Encrypted Message is: ")
  text2=""
  for i in range(0,len(text1)):
    if ord(text1[i])+13<=122:
      print(chr(ord(text1[i])+13),end="")
      text2+=chr(ord(text1[i])+13)
    else:
      print(chr(ord(text1[i])-13),end="")
      text2+=chr(ord(text1[i])-13)
  print()
  print("The Decrypted Message is: ")
  for i in range(0,len(text2)):
    if ord(text2[i])-13>=97:print(chr(ord(text2[i])-13),end="")
    elif ord(text2[i])-13==32:print(chr(ord(text2[i])-13),end="")
    else:print(chr(ord(text2[i])+13),end="")
  print()

elif choice==3:
  print("3. Transposition method")
  text1=input("Enter the text to be encrypted :")
  text2=""
  print("The Encrypted Message is: ")
  if len(text1)<2:print(text1)
  else:
    for i in range(0,2):
      j=2
      print(text1[i],end="")
      text2+=text1[i]
      while i+j<len(text1):
        print(text1[i+j],end="")
        text2+=text1[i+j]
        j+=2
  print()
  print("The Decrypted Message is: ")
  if len(text2)<2:print(text2)
  else:
    if len(text2)%2==0:a=int(len(text2)/2)
    else: a=int(len(text2)//2+1)
    for i in range(0,a):
      j=a
      print(text2[i],end="")
      while i+j<len(text2):
        print(text2[i+j],end="")
        j+=a
  print()
```

```
elif choice==4:
  print("4. Double Transposition method")
  text1=input("Enter the text to be encrypted :")
  text2=""
  str1=""
  str2=""
  print("The Encrypted Message is: ")
  if len(text1)<2:print(text1)
  else:
    for i in range(0,2):
      j=2
      str1+=text1[i]
      while i+j<len(text1):
        str1+=text1[i+j]
        j+=2
    for i in range(0,2):
      j=2
      print(str1[i],end="")
      text2+=str1[i]
      while i+j<len(str1):
        print(str1[i+j],end="")
        text2+=str1[i+j]
        j+=2
  print()
  print("The Decrypted Message is: ")
  if len(text2)<2:print(text2)
  else:
    if len(text2)%2==0:a=int(len(text2)/2)
    else: a=int(len(text2)//2+1)
    for i in range(0,a):
      j=a
      str2+=text2[i]
      while i+j<len(text2):
        str2+=text2[i+j]
        j+=a
    for i in range(0,a):
      j=a
      print(str2[i],end="")
      while i+j<len(str2):
        print(str2[i+j],end="")
        j+=a
  print()

elif choice==5:
  print("5. Vernam Cipher method")
  text2=""
  text1=input("Enter the text to be encrypted :")
  key=input("Enter the key text :")
```

```
    print("The Encrypted Message is: ")
    for i in range(0,len(text1)):
      if ord(text1[i])+ord(key[i])-194>25:
        print(chr(ord(text1[i])+ord(key[i])-123),end="")
        text2+=chr(ord(text1[i])+ord(key[i])-123)
      else:
        print(chr(ord(text1[i])+ord(key[i])-97),end="")
        text2+=chr(ord(text1[i])+ord(key[i])-97)
    print()
    print("The Decrypted Message is: ")
    for i in range(0,len(text2)):
      if ord(text2[i])<ord(key[i]):print(chr(ord(text2[i])-
ord(key[i])+123),end="")
      else:print(chr(ord(text2[i])-ord(key[i])+97),end="")
    print()

  else:
    print('Thank You')
    loop=False
```

Output:

```
PROBLEMS  OUTPUT  TERMINAL  DEBUG CONSOLE

PS C:\Users\manal> & C:/Users/manal/AppData/Local/Programs/Python/Python39/python.exe c:/Users/manal/Desktop/Tanvi/Sem5/CCS/EXP1.py
Select the Cryptography Method you want to implement :
1: Substitution method
2: ROT 13 method
3: Transposition method
4: Double Transposition method
5: Vernam Cipher method
6: End Program

Enter Your Choice : 1
1. Substitution method
Enter the text to be encrypted :mission impossible
Enter the no. of Position shift :4
The Encrypted Message is:
qmwwmsr$mqtswwmfpi
The Decrypted Message is:
mission impossible

Enter Your Choice : 2
2. ROT 13 method
Enter the text to be encrypted :mission impossible
The Encrypted Message is:
zvffvba-vzcbffvoyr
The Decrypted Message is:
mission impossible

Enter Your Choice : 3
3. Transposition method
Enter the text to be encrypted :mission impossible
The Encrypted Message is:
msinipsiliso mosbe
The Decrypted Message is:
mission impossible

Enter Your Choice : 4
4. Double Transposition method
Enter the text to be encrypted :mission impossible
The Encrypted Message is:
miisls obsnpiiomse
The Decrypted Message is:
mission impossible

Enter Your Choice : 5
5. Vernam Cipher method
Enter the text to be encrypted :mission impossible
Enter the key text :agsyhdvkuytshbaths
The Encrypted Message is:
mokqpri*ckigztiusw
The Decrypted Message is:
mission:impossible

Enter Your Choice : 6
Thank You
PS C:\Users\manal>
```

Conclusion:

In the above screenshots we can see how the same plain text can be converted into different cipher text by using various techniques. These methods were used during the war to transfer messages securely. Some of my observations regarding each method are:

- Substitution could be easy to understand as the letters are substituted with another letter every time for the same key.
- ROT 13 could be the easiest of all as every time we enter a letter the substitute letter would be the same.
- Transposition is a good option as we can implement it in various ways and it can be difficult to decrypt for an eavesdropper. Some of the transposition techniques are rail fence cipher, scytale, route cipher, etc. I have implemented columnar transposition.
- Double transposition is better than transposition as in this the transposition step is repeated twice and hence the cipher text becomes more complex.
- Vernam Cipher method is a very nice option to encrypt plaintext as it encrypts the plaintext using a random stream of text as the key; the only drawback is that we require the key of the same length as of the plain text.

Github link: https://github.com/tanvipen/Cipher.git