ST.XAVIER’S COLLEGE

(Affiliated to Tribhuvan University)

Maitighar, Kathmandu



**Cryptography Lab Assignment #1**

**SUBMITTED BY:**

Pradeep Dahal

017BSCIT029

3rd Year/5th Sem

|  |  |
| --- | --- |
| **SUBMITTED TO:** |  |

|  |  |  |
| --- | --- | --- |
|  | **Signature** | **Remarks** |
| **Er. Anil Kumar Shah**  **Lecturer, Dept. of Computer Science** |  |  |

**TITLE: WRITE A PROGRAM TO ENCRYPT AND DECRYPT A MESSAGE USING CEASER CIPHER**

**ALGORITHM**

**Theory**

The Caesar Cipher technique is one of the earliest and simplest method of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter some fixed number of positions down the alphabet. For example, with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials[1].

**Procedure**

1. Input the data to be encrypted or decrypted.
2. Iterate through all the characters in the string.
   1. Add/subtract the value 3 to the ASCII of the character and mod 26 for encryption/decryption.
3. Join and return the encrypted/decrypted string.

**SOURCE CODE**

import sys

def encrypt(x,key):

s=[]

for i in x:

if(ord(i)>64 and ord(i)<91):

temp=(((ord(i)-65)+key)%26)+65

s.append(chr(temp))

elif(ord(i)>96 and ord(i)<123):

temp=(((ord(i)-97)+key)%26)+97

s.append(chr(temp))

elif(ord(i)==32):

s.append(i)

else:

input("Invalid character program terminating. Enter any key to exit")

sys.exit()

encrypted\_text=(''.join(s))

return encrypted\_text

def decrypt(x,key):

s=[]

for i in x:

if(ord(i)>64 and ord(i)<91):

temp=(((ord(i)-65)-key)%26)+65

s.append(chr(temp))

elif(ord(i)>96 and ord(i)<123):

temp=(((ord(i)-97)-key)%26)+97

s.append(chr(temp))

elif(ord(i)==32):

s.append(i)

else:

print("Invalid character program terminating. Enter any key to exit")

sys.exit()

encrypted\_text=(''.join(s))

return encrypted\_text

key=3

data=input("Input the data:: Only A-Z and a-z::")

encData=encrypt(data,key)

print("The encrypted data is:")

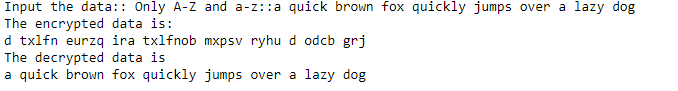
print(encData)

decData=decrypt(encData,key)

print("The decrypted data is")

print(decData)

**OBSERVATION**

****

**CONCLUSION**

Thus, Ceaser Cipher was implemented in the python programming language.

**REFERENCE**

[1] “Caesar Cipher in Cryptography - GeeksforGeeks.” [Online]. Available: https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/. [Accessed: 13-Nov-2019].