Lab Report 1 Date:2081/02/32

Experiment 1: Caesar Cipher

Title: Programming to learn about Caesar Cipher.

1. Objective:The objective of this Lab-Work is to use Caesar Cipher to encrypt text by shifting the letters of the alphabet by a fixed number of positions.
2. Theory: Caesar Cipher is a type of substitution cipher, where each letter in the plain text is shifted a certain number of positions down or up the alphabet. For example, with a shift of 3, the letter “A” becomes “D”, “B” becomes “E”, and so on.

2.1.Encryption:

In the Caesar Cipher, encryption is a straightforward process where each letter of the plain text (the original message) is replaced by a letter a fixed number of positions down or up the alphabet. This fixed number is called the **shift** or **key**.

The formula for the encryption is : **c=E(k,p)=(p+k)mod 26**. Where p=plain text, c=cipher text and k=key.

2.1.Decryption:

In the Caesar Cipher, Decryption is the reverse process of encryption. To decrypt the message, you need to  **shift the letters in the cipher text back**  by the same number of positions used during encryption. (**shift key**).The formula for the encryption is : **p=D(k,p)=(c-k)mod 26**. Where p=plain text, c=cipher text and k=key.

1. Implementation of Caesar Cipher Encryption.

*##ENCRYPTION CAESER CIPHER*

*text=input("Enter the PLAIN TEXT")*

*key=int(input("Enter the key value"))*

*print("The plain text is :",text)*

*encrypted=' '*

*for char in text:*

*if char.isalpha():*

*start = 65 if char.isupper() else 97*

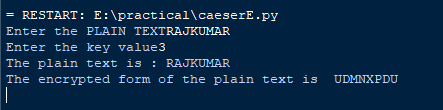
*encrypted=encrypted+chr((ord(char)-start+key)%26+start)*

*else:*

*encrypted+=char*

*print("The encrypted form of the plain text is ",encrypted)*

Output:



1. Implementation of Caesar Cipher Decryption.

*##DECRYPTION CAESER CIPHER*

*encrypt=input("Enter the ENCRYPTED TEXT")*

*key=int(input("Enter the key value"))*

*print("The plain text is :",encrypt)*

*decrypted=' '*

*for char in encrypt:*

*if char.isalpha():*

*start = 65 if char.isupper() else 97*

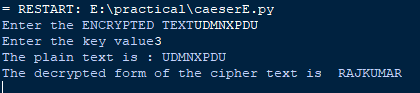
*decrypted=decrypted+chr((ord(char)-start-key)%26+start)*

*else:*

*decrypted+=char*

*print("The decrypted form of the cipher text is ",decrypted)*

Output:



1. Conclusion: In the above page we have learned about Caesar Cipher’s encryption and decryption and implemented them by using python.