CS458 Assignment 1

Sahil Riyaz Sheikh(A20518693)

Department of Computer ScienceIllinois
Institute of Technology

September 5, 2023

.

1. Problem Statement:

In this assignment I'll perform a brute force attack to decrypt the given Cipher Text to obtain the required Plain Text.

2. Proposed Solution:

I'll create a program to decrypt the given encrypted text (cipher text) to obtain the plain text. I'll do so by performing a brute force attack. In this attack I'll use decrypt the given cipher text by using all available keys, ranging from 0-25.

3. Implementation Detail:

Firstly, I decided to convert the letters of the cipher text into their corresponding ASCII values. After doing so all I had to do was subtract the key value form the ASCII value of the letter to obtain the required plain texts. After doing so I would convert these ASCII values back to their corresponding letters.

I converted the given string into a list to get the ASCII values. After doing so I created two for loops, the first loop which would be responsible for selecting different keys in the range of 0 to 25 and the inner loop who loop through the list containing the ASCII values. I used ord() function to cross verify the ASCII values of "A" and "Z", their ASCII values were found to be 65 and 90 respectively. I did so to I would be able to implement an if and else condition where when the key is subtracted from the ASCII value and results less than 65, then 26 would be added in the result. To put it simply, this is how I implemented the mod 26.

I was able to get the required results, then I decided to modify the code so it could take Cipher Text from the user to decrypt. The only drawback of this program was that it was only working for uppercase letter i.e A-Z and would not work for lowercase letters. I decided to overcome this drawback by implementing nested if-else conditions. The first if condition who check if the letter is a uppercase or not and the internal if-else were utilized to perform subtraction between the ASCII values and keys.

4. Results:

Here are the results which I obtained:

```
KEY =  0  Plaintext =  CSYEVIXIVQMREXIH
KEY =  1  Plaintext =  BRXDUHWHUPLQDWHG
KEY =  2  Plaintext =  AQWCTGVGTOKPCVGF
KEY =  3  Plaintext =  ZPVBSFUFSNJOBUFE
KEY =  4  Plaintext =  YOUARETERMINATED
KEY =  5  Plaintext =  XNTZQDSDQLHMZSDC
KEY =  6  Plaintext =  WMSYPCRCPKGLYRCB
KEY =  7  Plaintext =  VLRXOBQBOJFKXQBA
KEY =  8  Plaintext =  UKQWNAPANIEJWPAZ
KEY =  9  Plaintext =  TJPVMZOZMHDIVOZY
KEY =  10  Plaintext =  SIOULYNYLGCHUNYX
KEY =  11  Plaintext =  RHNTKXMXKFBGTMXW
KEY =  12  Plaintext =  QGMSJWLWJEAFSLWV
KEY =  13  Plaintext =  PFLRIVKVIDZERKVU
KEY =  14  Plaintext =  OEKQHUJUHCYDQJUT
KEY =  15  Plaintext =  NDJPGTITGBXCPITS
KEY =  16  Plaintext =  MCIOFSHSFAWBOHSR
KEY =  17  Plaintext =  LBHNERGREZVANGRQ
KEY =  18  Plaintext =  KAGMDQFQDYUZMFQP
KEY =  19  Plaintext =  JZFLCPEPCXTYLEPO
KEY =  20  Plaintext =  IYEKBODOBWSXKDON
KEY =  21  Plaintext =  HXDJANCNAVRWJCNM
KEY =  22  Plaintext =  GWCIZMBMZUQVIBML
KEY =  23  Plaintext =  FVBHYLALYTPUHALK
KEY =  24  Plaintext =  EUAGXKZKXSOTGZKJ
KEY =  25  Plaintext =  DTZFWJYJWRNSFYJI
```

For this example the cipher text will be: KHOORKRZDUHBRX

They key is 3 and the decrypyed output should be: HELLOHOWAREYOU

58]:

```
input_text = input("Enter Cipher Text: ")
ASCII_val = list(bytes(input_text,'ascii'))
for x in range(26):
    target=[]
    for i in ASCII_val:
        if i-x<65:
            i=i-x+26
        else:
            i=i-x
        target.append(i)
    final=[]
    for i in target:
        final.append(chr(i))
    str1 = ""
    #str1.join(final)
    print("KEY = ",x," Plaintext = ",str1.join(final))
    #print(final)
```

```
Enter Cipher Text: KHOORKRZDUHBRX
KEY =  0  Plaintext =  KHOORKRZDUHBRX
KEY =  1  Plaintext =  JGNNQJQYCTGAQW
KEY =  2  Plaintext =  IFMMPIPXBSFZPV
KEY =  3  Plaintext =  HELLOHOWAREYOU
KEY =  4  Plaintext =  GDKKNGNVZQDXNT
KEY =  5  Plaintext =  FCJJMFMUYPCWMS
KEY =  6  Plaintext =  EBIILELTXOBVLR
KEY =  7  Plaintext =  DAHHKDKSWNAUKQ
KEY =  8  Plaintext =  CZGGJCJRVMZTJP
KEY =  9  Plaintext =  BYFFIBIQULYSIO
KEY =  10  Plaintext =  AXEEHAHPTKXRHN
KEY =  11  Plaintext =  ZWDDGZGOSJWQGM
KEY =  12  Plaintext =  YVCCFYFNRIVPFL
KEY =  13  Plaintext =  XUBBEXEMQHUOEK
KEY =  14  Plaintext =  WTAADWDLPGTNDJ
KEY =  15  Plaintext =  VSZZCVCKOFSMCI
KEY =  16  Plaintext =  URYYBUBJNERLBH
KEY =  17  Plaintext =  TQXXATAIMDQKAG
KEY =  18  Plaintext =  SPWWZSZHLCPJZF
KEY =  19  Plaintext =  ROVVYRYGKBOIYE
KEY =  20  Plaintext =  QNUUXQXFJANHXD
KEY =  21  Plaintext =  PMTTWPWEIZMGWC
KEY =  22  Plaintext =  OLSSVOVDHYLFVB
KEY =  23  Plaintext =  NKRRUNUCGXKEUA
KEY =  24  Plaintext =  MJQQTMTBFWJDTZ
KEY =  25  Plaintext =  LIPPSLSAEVICSY
```

```
Enter Cipher Text: MjqqtMtbFwjDtz
KEY =  0  Plaintext =  MjqqtMtbFwjDtz
KEY =  1  Plaintext =  LippsLsaEviCsy
KEY =  2  Plaintext =  KhoorKrzDuhBrx
KEY =  3  Plaintext =  JgnnqJqyCtgAqw
KEY =  4  Plaintext =  IfmmpIpxBsfZpv
KEY =  5  Plaintext =  HelloHowAreYou
KEY =  6  Plaintext =  GdkknGnvZqdXnt
KEY =  7  Plaintext =  FcjjmFmuYpcWms
KEY =  8  Plaintext =  EbiilEltXobVlr
KEY =  9  Plaintext =  DahhkDksWnaUkq
KEY =  10  Plaintext =  CzggjCjrVmzTjp
KEY =  11  Plaintext =  ByffiBiqUlySio
KEY =  12  Plaintext =  AxeehAhpTkxRhn
KEY =  13  Plaintext =  ZwddgZgoSjwQgm
KEY =  14  Plaintext =  YvccfYfnRivPfl
KEY =  15  Plaintext =  XubbeXemQhuOek
KEY =  16  Plaintext =  WtaadWdlPgtNdj
KEY =  17  Plaintext =  VszzcVckOfsMci
KEY =  18  Plaintext =  UryybUbjNerLbh
KEY =  19  Plaintext =  TqxxaTaiMdqKag
KEY =  20  Plaintext =  SpwwzSzhLcpJzf
KEY =  21  Plaintext =  RovvyRygKboIye
KEY =  22  Plaintext =  QnuuxQxfJanHxd
KEY =  23  Plaintext =  PmttwPweIzmGwc
KEY =  24  Plaintext =  OlssvOvdHylFvb
KEY =  25  Plaintext =  NkrruNucGxkEua
```

5. References:

https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/

https://stackoverflow.com/questions/8452961/convert-string-to-ascii-value-python