Crypto – Caesar Cipher

Problem: If you can decrypt this file, you might find a flag

Hint: I like my salad with two ingredients

Given: file.enc

Steps:

1) When the file is opened, it will be obvious that the first step is to decode the base64.



A command to decode this is as follows (note: this is a python command but there are many other commands that can be used to decode base 64)

Command: python –m base64 –d <<< REpZRXtBeUNxeVBfR3FfQ3lRd30K==

Produces: DJYE{AyCqyP\_Gq\_CyQw}



2) Now there is a few different things you could do. These easiest would be to think about what this text looks like, four letters followed by {. That is a good indicator that it said flag{. One that has seen Caesar cipher would know that it looks like these characters have been shifted in some way.

Easiest solution: take the text ‘DJYE{AyCqyP\_Gq\_CyQw}’ and put this into an online Caesar cipher decoder. Such as this [link.](https://www.nayuki.io/page/automatic-caesar-cipher-breaker-javascript)

After you insert the text you will be given the flag and the key.

Key: 24

Flag: FLAG{CaEsaR\_Is\_EaSy}

3) Another solution could be to write a python script to crack caesar ciphers in the future.

#!/usr/bin/python

# -\*- coding: utf-8 -\*-

import sys

def main():

key = sys.argv[1]

text = "DJYE{AyCqyP\_Gq\_CyQw}"

print decryptMessage(key,text)

def decryptMessage(key,message):

translated = ""

for i in range(0,len(message)):

if message[i].isalpha():

if message[i].isupper():

char = chr((ord(message[i])-ord('A')+int(key))%26 + ord('A'))

translated+=char

else:

char = chr((ord(message[i])-ord('a')+int(key))%26 + ord('a'))

translated+=char

else:

translated+=message[i]

return translated

if \_\_name\_\_ == '\_\_main\_\_':

main()

This script takes each character and cycles it by the key. With this script the key is input in the system argument so you can test different keys in the future for a different Caesar cipher.

The equation in python has to use capital A and mod 26 to rap around with capital letters and a with lower case letters.

Below is the result of using brute force to test keys until you get an obvious result. Notice that when you enter a key argument of 2, you get a legible result, “FLAG{CaEsaR\_Is\_EaSy}”.

