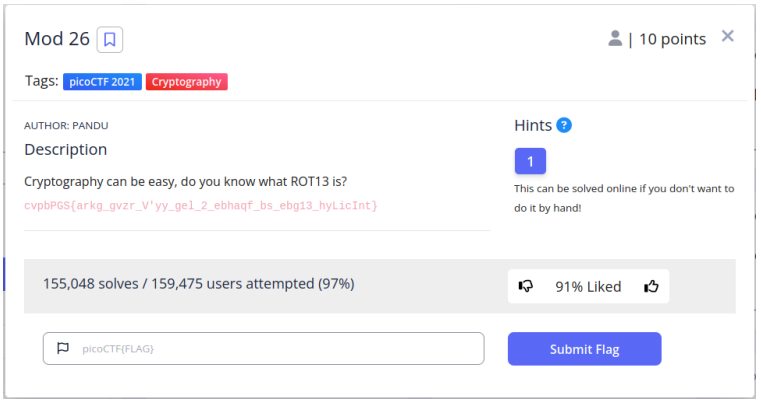
CRYPTOGRAPHY

Mod 26

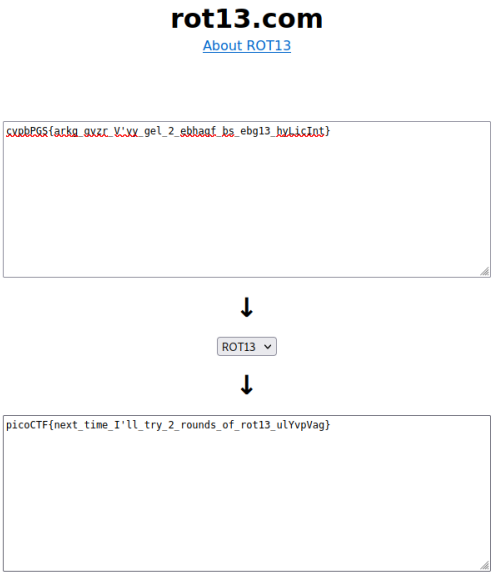


Diberikan sebuah flag yang di enkripsi menggunakan ROT13:

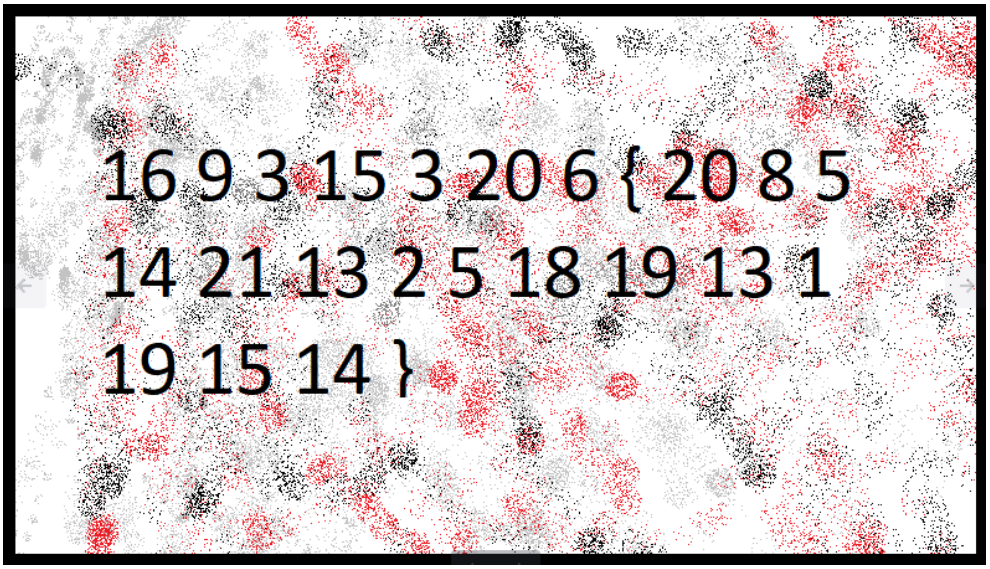
cvpbPGS{arkg_gvzr_V'yy_gel_2_ebhaqf_bs_ebg13_hyLicInt}

Lalu saya coba decrypt menggunakan tools online, setelah saya coba maka terdapat flag sebenarnya:

picoCTF{next_time_I'll_try_2_rounds_of_rot13_ulYvpVag}



The Numbers



Diberikan sebuah serangkaian nomor yang berformat seperti flag picoCTF. Saat dicek ternyata nomor tersebut merupakan index dari huruf alphabet, 16 = “P”, 9 = “I”, dst. Maka saya buat script:

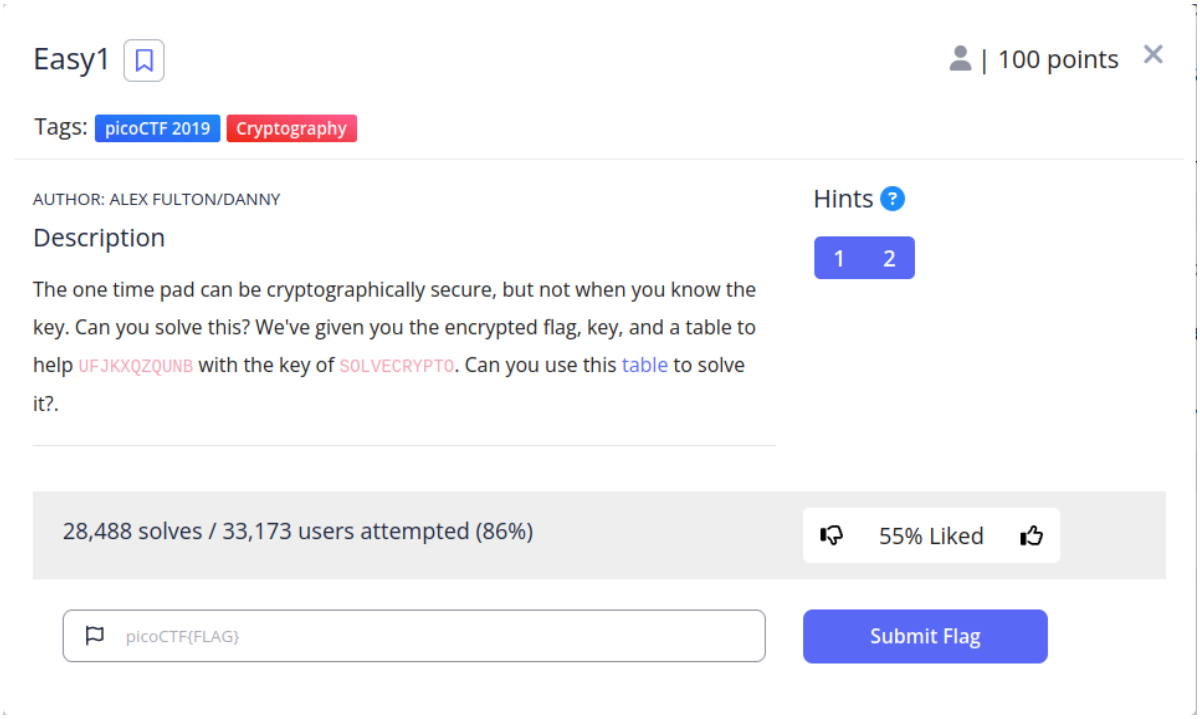
```
from string import ascii_uppercase as uppercase

num = [16, 9, 3, 15, 3, 20, 6, "{", 20, 8, 5, 14, 21, 13, 2, 5,
    18, 19, 13, 1, 19, 15, 14, "}"]

flag = []

for i in num:
    if(not isinstance(i, int)):
        flag.append(i)
    else:
        i = i - 1
        flag.append(uppercase[i])

print (''.join(flag))
```

Karena library ascii_uppercase menggunakan zero base alphabet maka setiap nomor harus dikurang 1 agar mendapatkan hasil yang diinginkan.

```
└─[$]> python3 numbers.py
PICOCTF{THENUMBERSMASON}
```

Maka flagnya adalah: **PICOCTF{THENUMBERSMASON}**

Easy1



Diberkan encrypted flag, key, dan sebuah table.

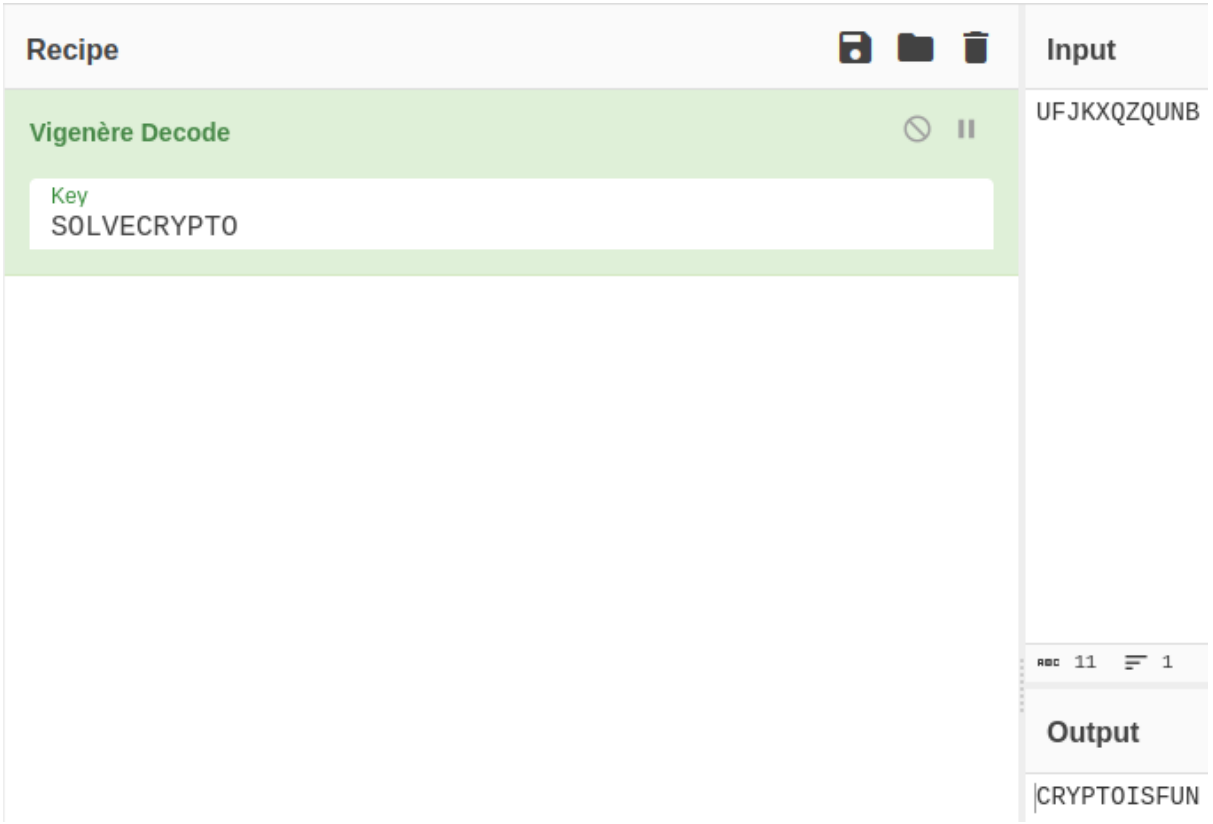
Encrypted flag = UFJKXQZQUNB

Key = SOLVECRYPTO

Table =

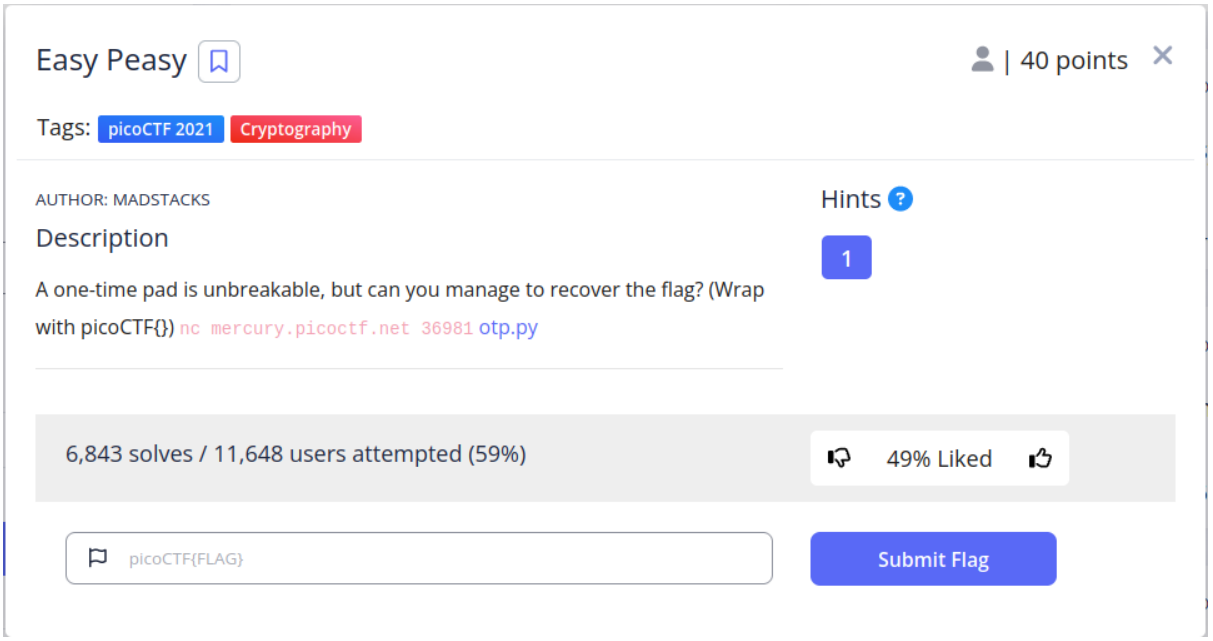
```
└─[$]> cat table.txt
   A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
  +---------------------------------------------------
A | A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
B | B C D E F G H I J K L M N O P Q R S T U V W X Y Z A
C | C D E F G H I J K L M N O P Q R S T U V W X Y Z A B
D | D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
E | E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
F | F G H I J K L M N O P Q R S T U V W X Y Z A B C D E
G | G H I J K L M N O P Q R S T U V W X Y Z A B C D E F
H | H I J K L M N O P Q R S T U V W X Y Z A B C D E F G
I | I J K L M N O P Q R S T U V W X Y Z A B C D E F G H
J | J K L M N O P Q R S T U V W X Y Z A B C D E F G H I
K | K L M N O P Q R S T U V W X Y Z A B C D E F G H I J
L | L M N O P Q R S T U V W X Y Z A B C D E F G H I J K
M | M N O P Q R S T U V W X Y Z A B C D E F G H I J K L
N | N O P Q R S T U V W X Y Z A B C D E F G H I J K L M
O | O P Q R S T U V W X Y Z A B C D E F G H I J K L M N
P | P Q R S T U V W X Y Z A B C D E F G H I J K L M N O
Q | Q R S T U V W X Y Z A B C D E F G H I J K L M N O P
R | R S T U V W X Y Z A B C D E F G H I J K L M N O P Q
S | S T U V W X Y Z A B C D E F G H I J K L M N O P Q R
T | T U V W X Y Z A B C D E F G H I J K L M N O P Q R S
U | U V W X Y Z A B C D E F G H I J K L M N O P Q R S T
V | V W X Y Z A B C D E F G H I J K L M N O P Q R S T U
W | W X Y Z A B C D E F G H I J K L M N O P Q R S T U V
X | X Y Z A B C D E F G H I J K L M N O P Q R S T U V W
Y | Y Z A B C D E F G H I J K L M N O P Q R S T U V W X
Z | Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
```

Setelah di cek ini merupakan sebuah Vigenère cipher. Lalu saya coba decrypt menggunakan CyberChef



Maka flagnya adalah: **PICOCTF{CRYPTOISFUN}**

Easy Peasy



Diberikan sebuah alamat host dan port nya, serta sebuah file python yang merupakan source code dari program yang ada di host. Lalu, saya coba jalankan alamat yang diberikan tadi maka tampil seperti berikut:

```
**********Welcome to our OTP implementation!**********
This is the encrypted flag!
5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c

What data would you like to encrypt? abc
Here ya go!
50035d
```

Disini terlihat program bisa mengenkripsi inputan dari user. Lalu saya periksa flagnya menggunakan pyhon.

```
Python 3.9.2 (default, Feb 28 2021, 17:03:44)
[GCC 10.2.1 20210110] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> len("5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c")
64
```

Berdasarkan screenshot diatas, bisa diketahui bahwa flag tersebut merupakan bilangan desimal 32 bit.

```
KEY_FILE = "key"
KEY_LEN = 50000
FLAG_FILE = "flag"


def startup(key_location):
    flag = open(FLAG_FILE).read()
    kf = open(KEY_FILE, "rb").read()

    start = key_location
    stop = key_location + len(flag)
```

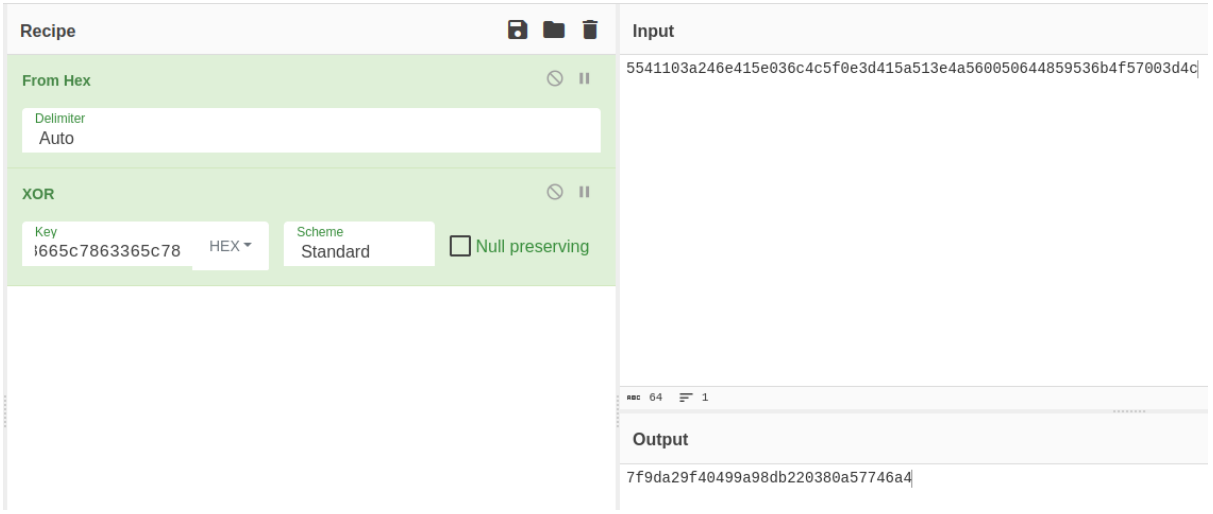
```
if stop >= KEY_LEN:
    stop = stop % KEY_LEN
    key = kf[start:] + kf[:stop]
else:
    key = kf[start:stop]
key_location = stop
```

Setelah saya memeriksa source code nya saya menemukan bagian looping perkondisian dimana jika inputan user melebihi **KEY_LEN** / panjang key(di source

code tertulis 50000) maka posisi key yang digunakan untuk dienkripsi akan kembali dari awal. Posisi key bertambah seiring ada inputan dari user, posisi key dimulai dari 0 namun diawal saat memulai program sudah terpakai sebanyak 32 byte untuk mengenkripsi flag. Jadi jika kita mengirim kembali 32 byte bilangan desimal contohnya ”\x00” disaat posisi key dimulai dari awal, lalu hasilnya di XOR dengan flag yang kita dapat maka akan dapat kunci aslinya

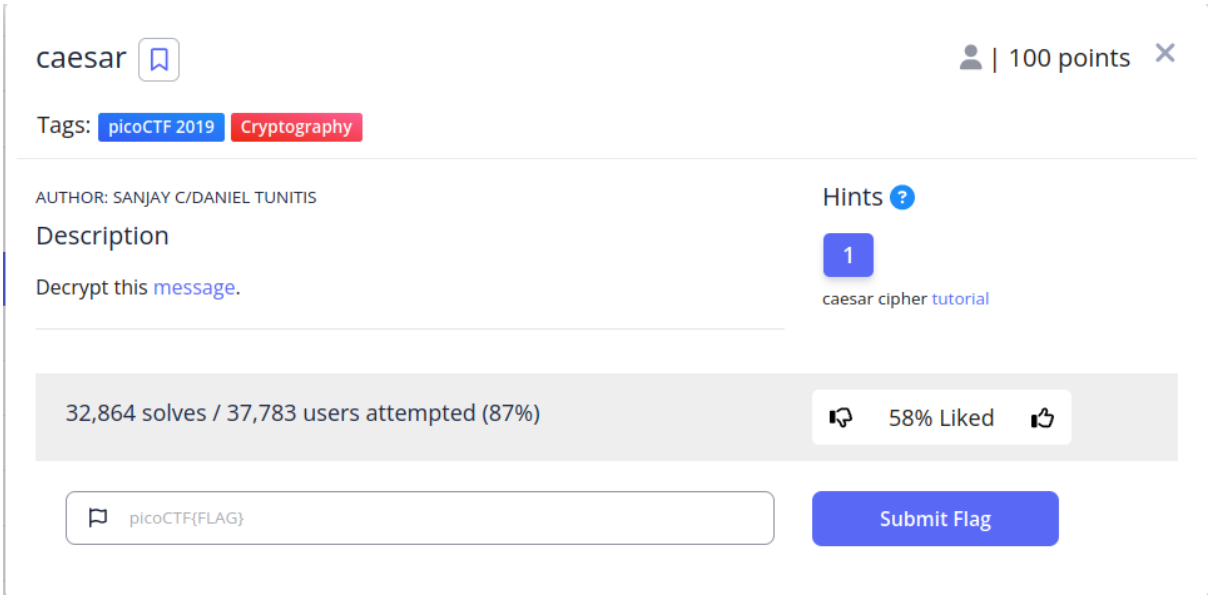
```
└─[$]> python3 -c "print('\x00'*(50000-32)+'\n'+'\x00'*32)" | nc mercury.picoctf.net
 36981
**********Welcome to our OTP implementation!**********
This is the encrypted flag!
5541103a246e415e036c4c5f0e3d415a513e4a560050644859536b4f57003d4c
```

```
What data would you like to encrypt? Here ya go!
6227295e455c7838375c7866375c7862355c786430635c7838665c7863365c78
```



Maka flagnya adalah: **picoCTF{7f9da29f40499a98db220380a57746a4}**

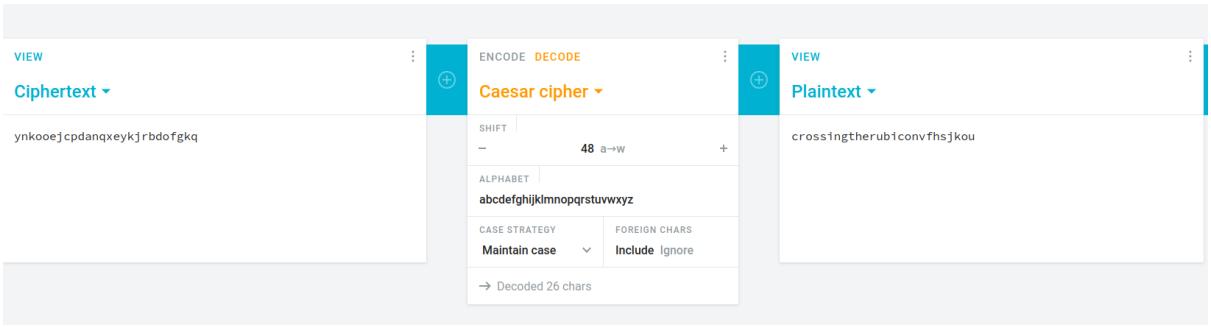
Caesar



Diberikan sebuah ciphertext yang berisi:

picoCTF{ynkooejcpdanqxeykjrbdofgkq}

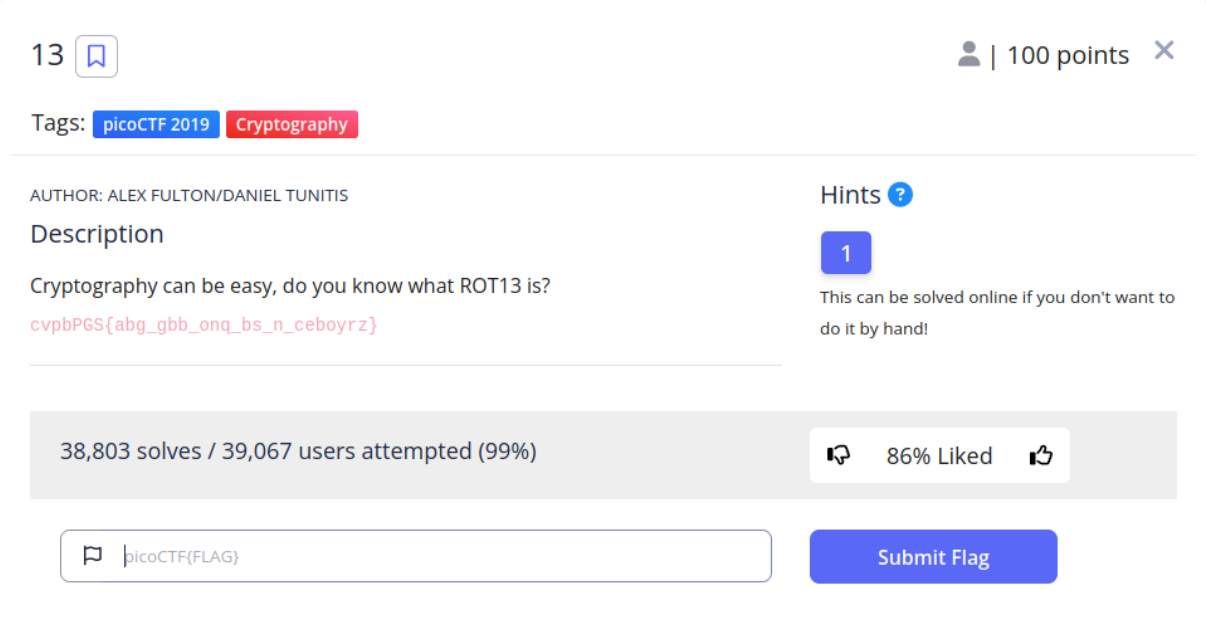
Berdasarkan dari hint jenis enkripsi yang digunakan adalah caesar cipher jadi saya mencari tools yang tersedia di online, lalu mencoba mendekripsi nya



Setelah mencari, saya menemukan kata yang tidak acak yang kemungkinan adalah flagnya, dan ternyata benar.

Maka flagnya adalah: **picoCTF{crossingtherubiconvfhsjkou}**

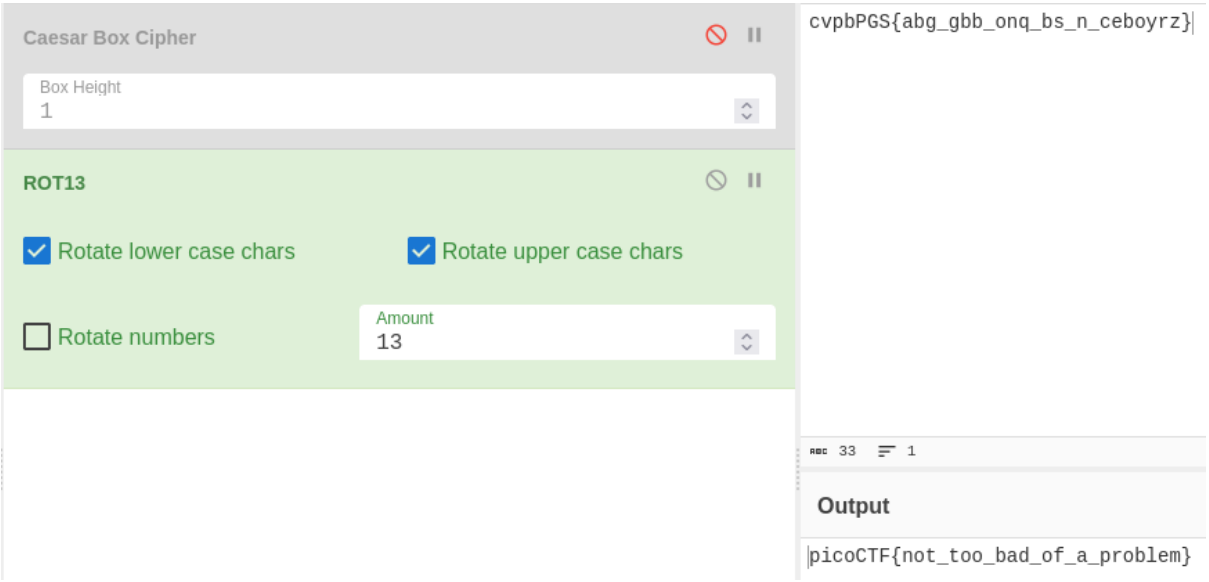
13



Diberikan sebuah flag yang dienkripsi menggunakan ROT13:

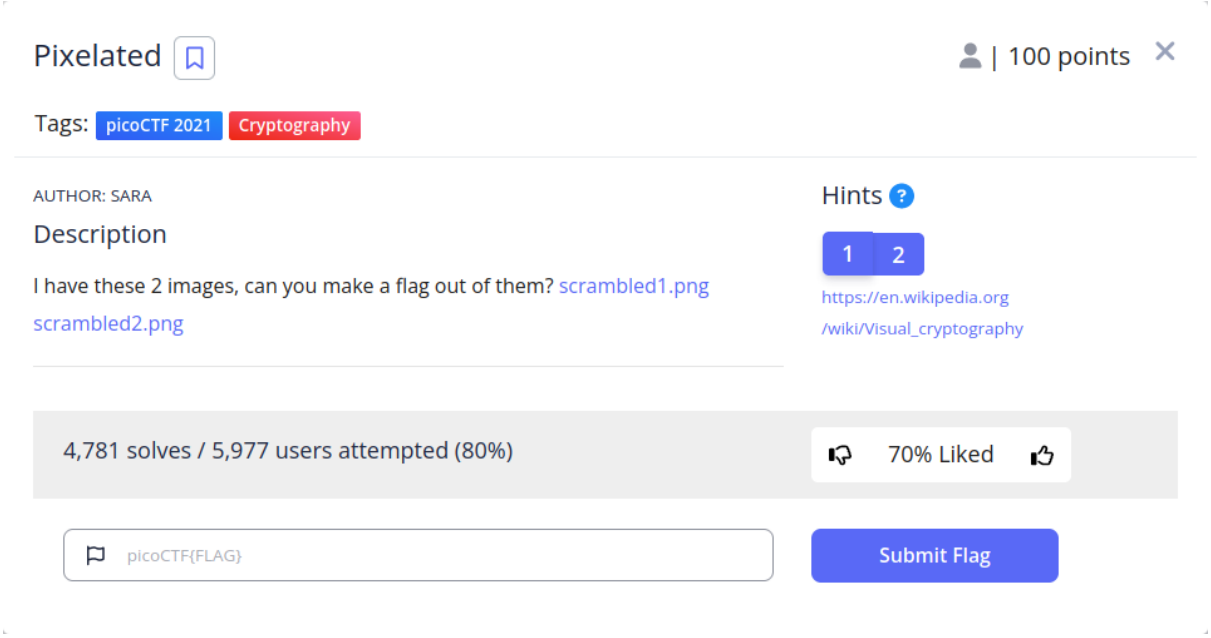
cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}

Karena sudah mengetahui jenis enkripsinya saya menggunakan cyberchef untuk mendekripsinya

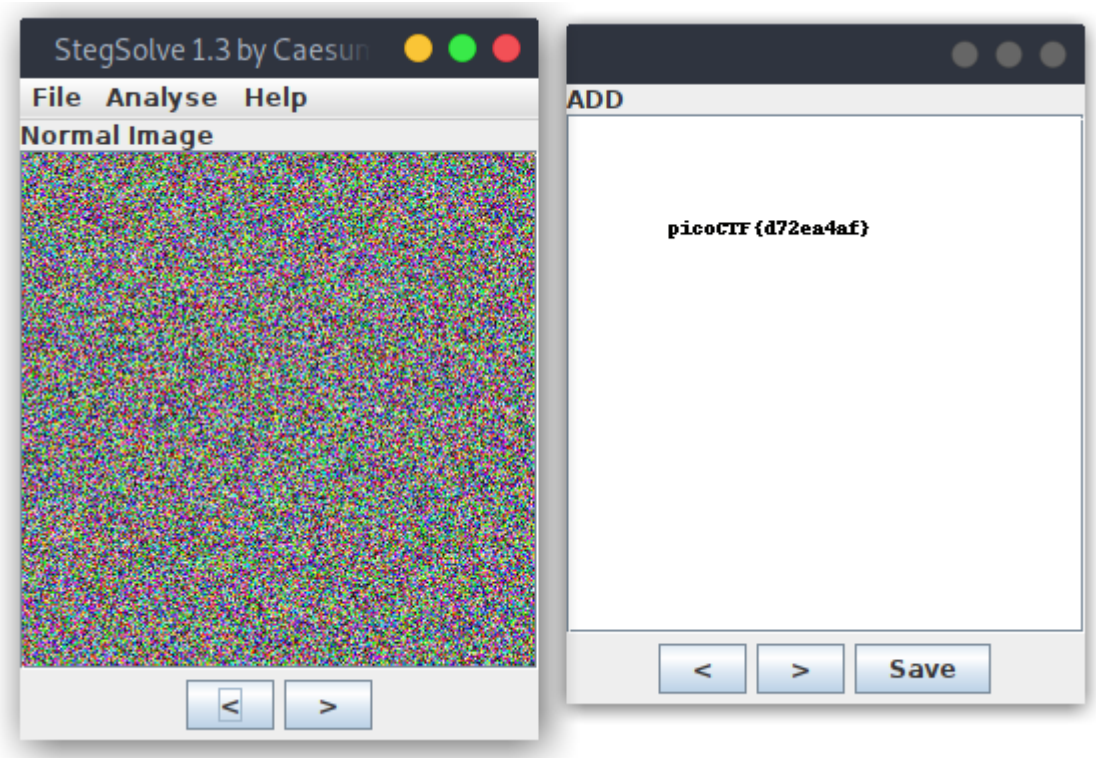


Maka flagnya adalah: **picoCTF{not_too_bad_of_a_problem}**

Pixelated

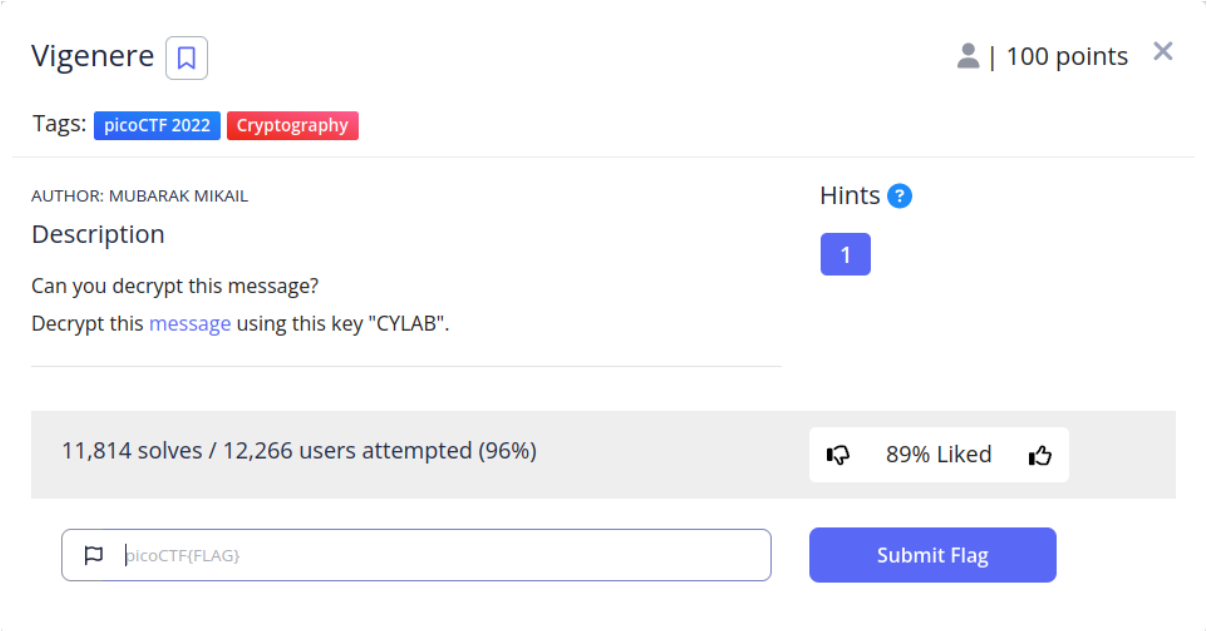


Diberikan 2 buah gambar yang diacak, saya coba memeriksanya dengan stegsolve image combiner, dan ternyata benar, ada flag didalamnya



Maka flagnya adalah: **picoCTF{d72ea4af}**

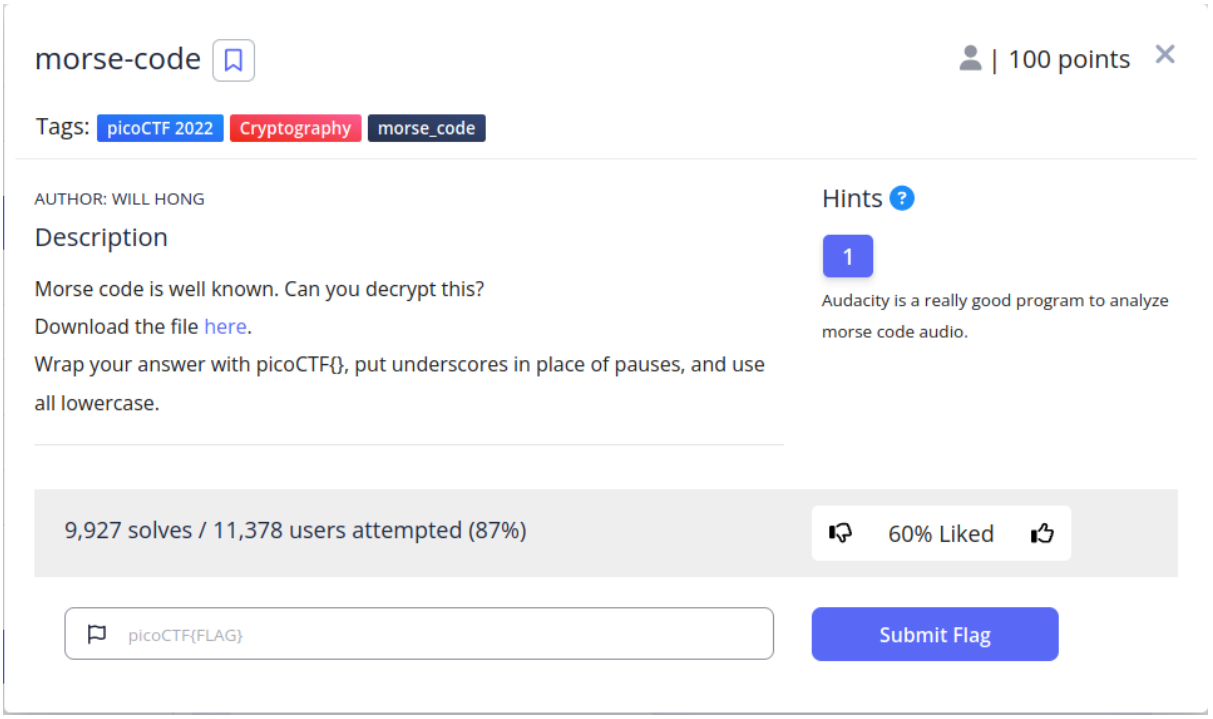
Vigenere



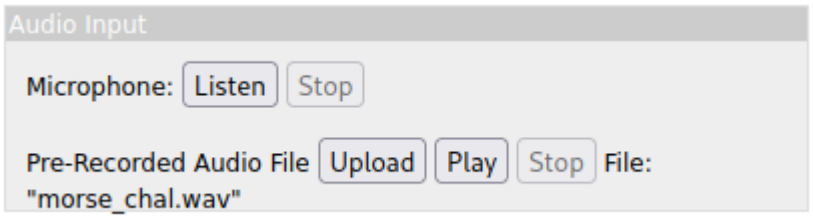
Diberikan sebuah pesan yang dienkripsi, dari judul saya langsung mengetahui bahwa itu adalah vigenere cipher, lalu langsung saja saya eksekusi menggunakan cyberchef

Maka flagnya adalah: **picoCTF{D0NT_US3_V1G3N3R3_C1PH3R_2951a89h}**

Morse-Code



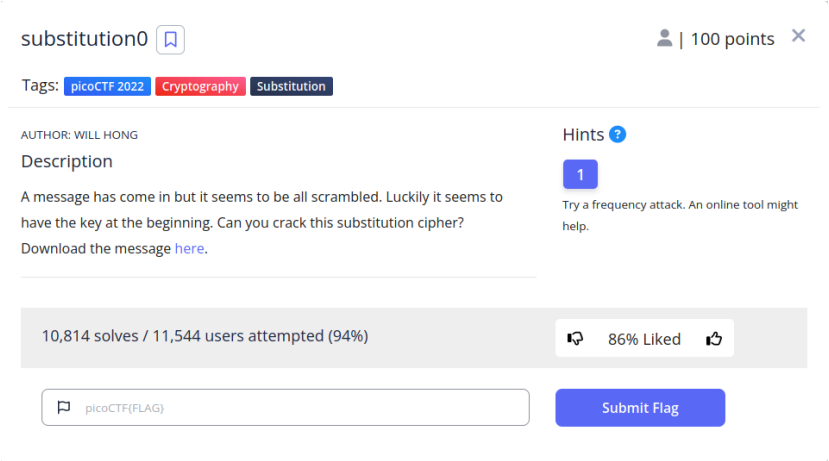
diberikan file .wav yang kemungkinan berupa kode morse, langsung saja saya cari decoder kode morse yang tersedia secara online



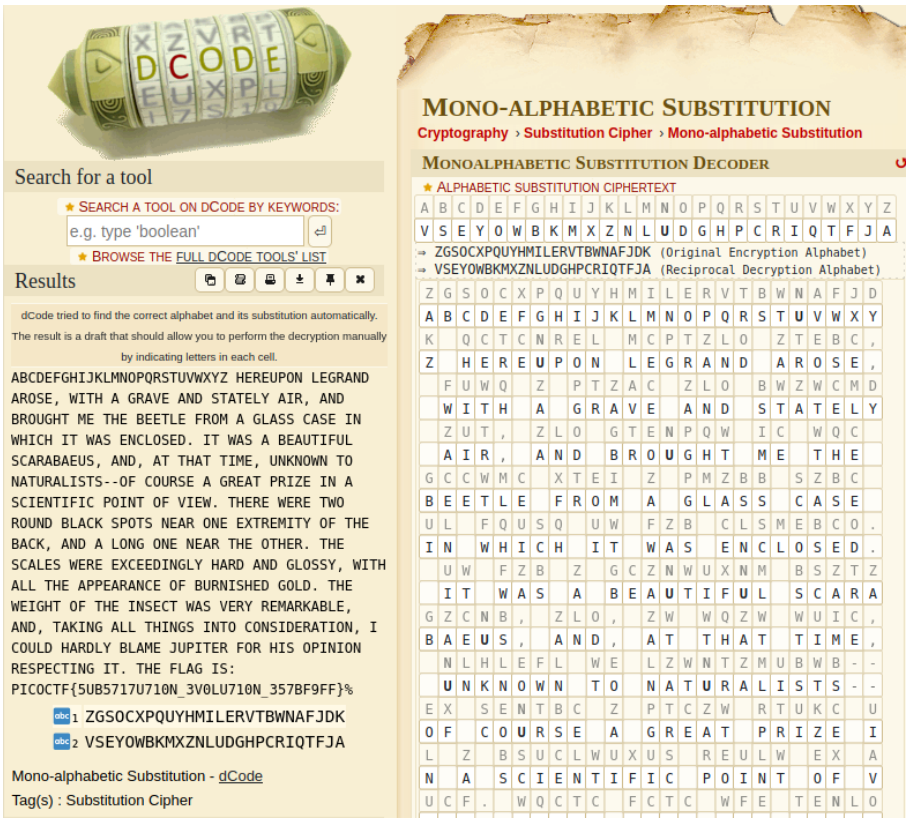
Setelah mendapatkan pesannya, lalu saya sesuaikan dengan format yang ada dideskripsi.

Maka flagnya adalah: **picoCTF{wh47_h47h_90d_w20u9h7}**

Substitution0



Diberikan sebuah pesan yang didekripsi, karena saya mengetahui bahwa pesan itu merupakan substitution cipher tapi tidak mengetahui jenis nya maka saya menggunakan cipher identifier tool yang tersedia secara online dan mendapatkan jenis nya yaitu Mono-alphabetic Substitution, lalu saya cari tool cipher solver yang tersedia secara online.



Maka dapat flagnya.

Maka flagnya adalah: **PICOCTF{5UB5717U710N_3V0LU710N_357BF9FF}**