N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N 00b_ScRiptKid

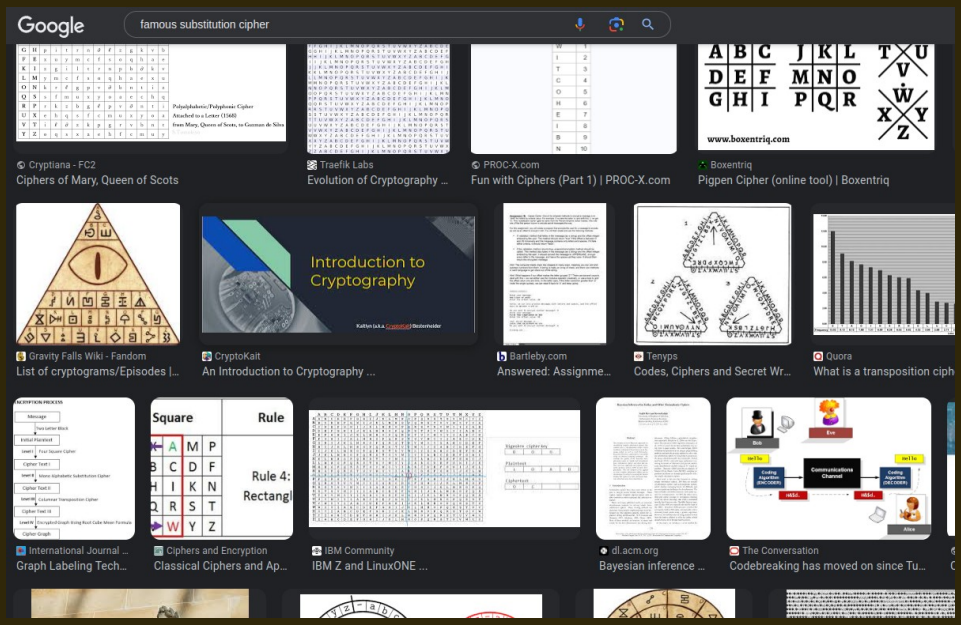
N00b_ScRiptKidS

Crypto

Warm Up 1

When I Look at given image,I know it is one of substitution cipher.But I don't know the name of cipher.So,I searched "famous substitution cipher" on google and it gave me many of things.

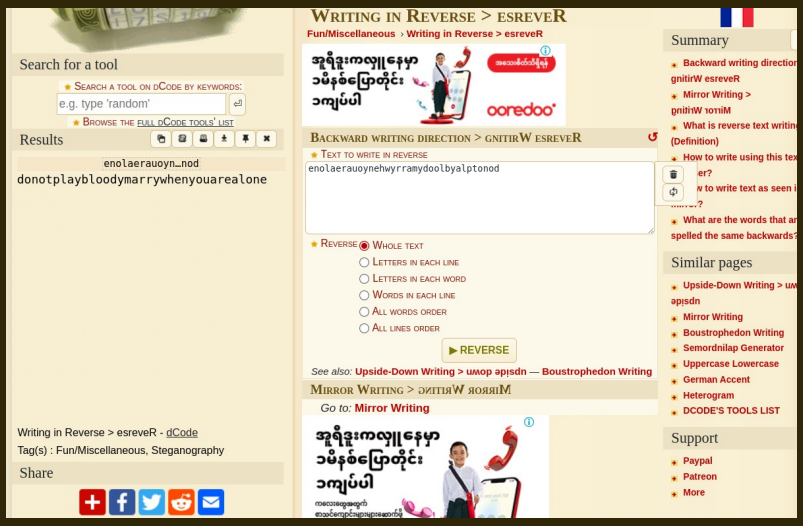
So I went to image section to recognize.In somewhere,the image catched my eye.



"Gravity Falls Wiki" It is so similar our image.So I research about this.In last,I know it is gravity falls cipher.And then,I go to decode.fr to decrypt it.And then,I got JOHN WICk.

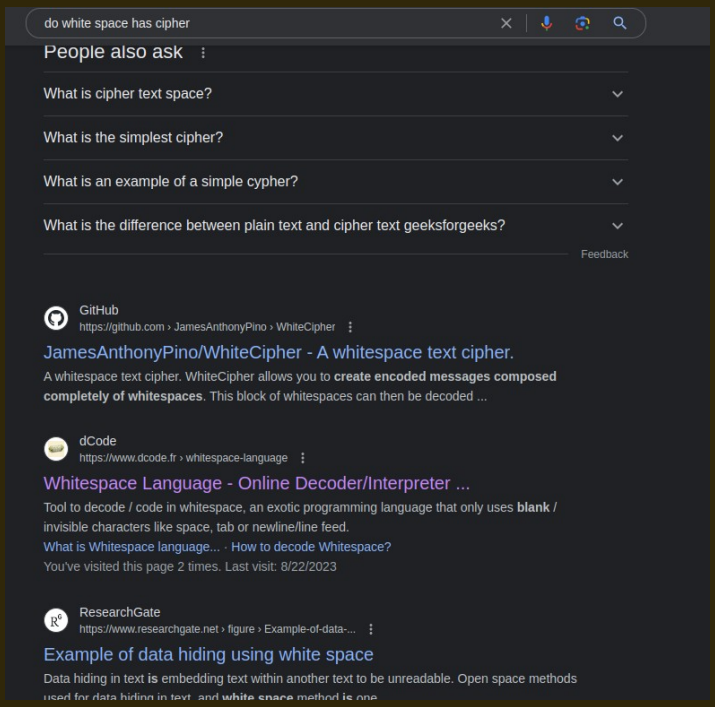
Game

Game is very easy bcz I think it is reversed text.So I tested on decode.fr about reverse text and then I got original text.

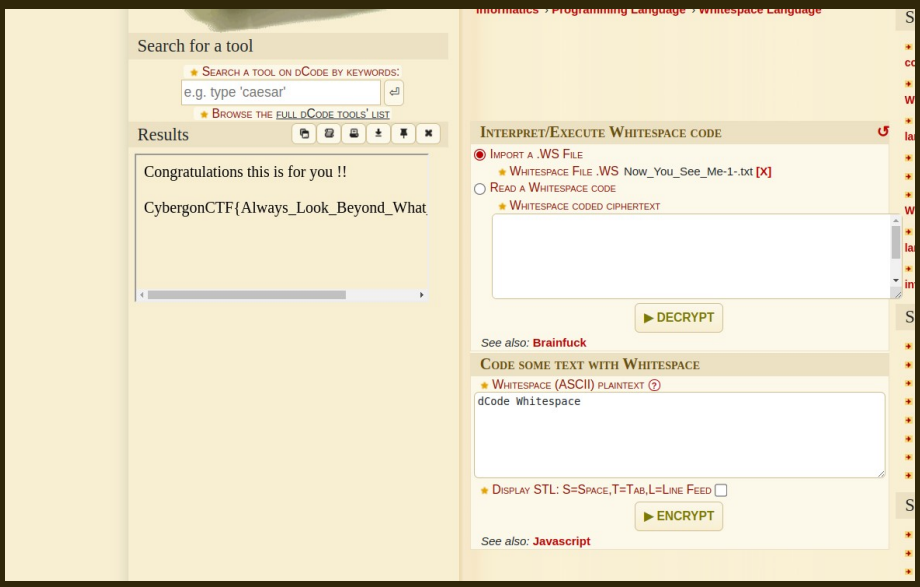


Now You see me

At first,I got txt file.I didn't saw nothing in file.But I noticed white space there.So.I check out on google by typing "Do white space has cipher".I saw the link.

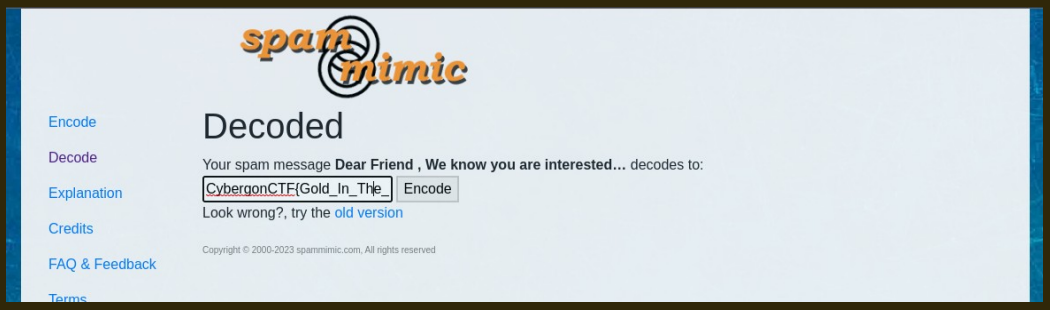


And after decrypted we got flag.



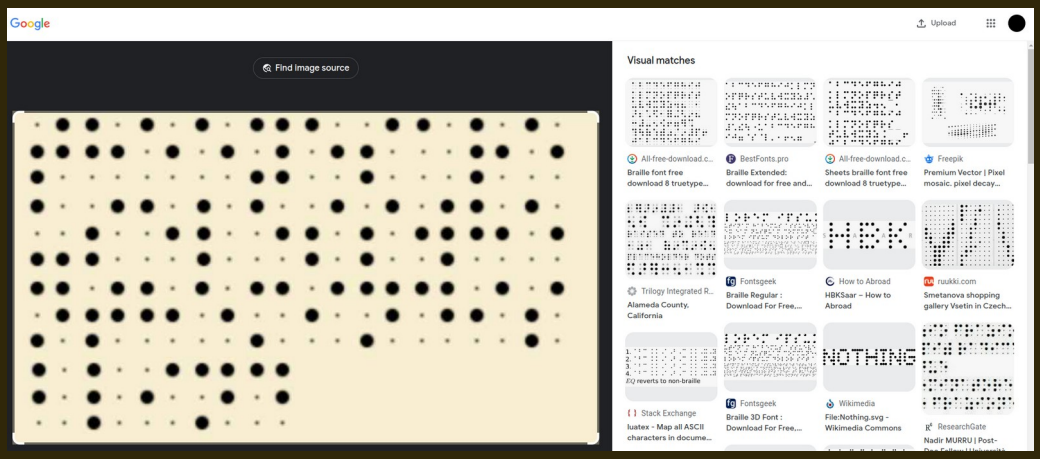
Now You see me 2

In this challenge also has txt file.And I found long paragraph and then,I confuse with this paragraph.So,i copy and paste out in google this paragraph and research it.In suddenly,i saw the link about "Spamming decoder".After decrypted,I got flag.

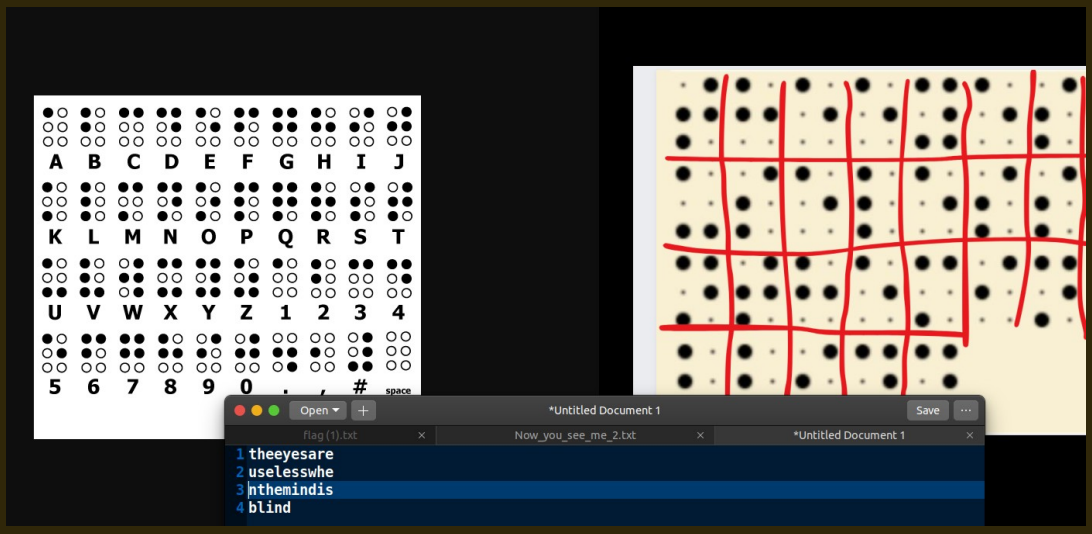


Dots

This challenge has the hint.”Connected the dots”,So I thinked it is morse code when I connected dot.But it doesn’t work.I got many tension.So,I used google image search to find out what it is.In few seconds,I knew it is braille font.



And I dcode manually.After I decoded I got plain text.It is flag



EZ Rsa

At first,we have two files from challenge.One file is python encryption file and other file is encrypted output file.And it is RSA encrption method.But in this challenge not same original rsa encryption bcz p and q are multiply by one random numbers.But we don't know this num.

Firstly,,I needed to rewatch formula.

Formula reference : https://www.cs.utexas.edu/~mitra/honors/soln.html

At first,we have **c,n,p and q.**

To get m, formula is **m=c^d%n**

<!----In py : **m=pow(c,d,n)**)-->

To get d,Formula is **d = e^(-1) mod φ(n)**

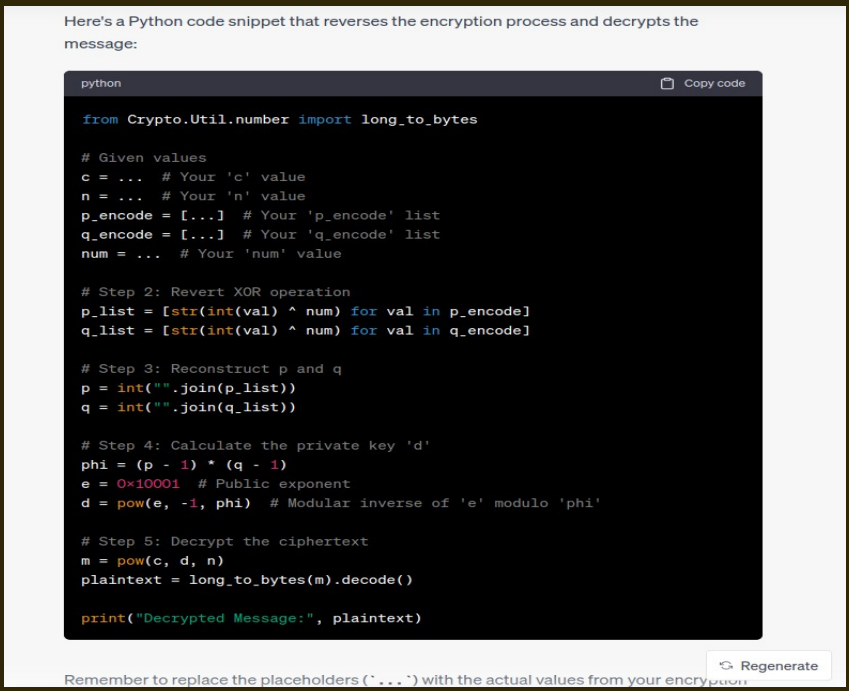
<!---mod is same %,It is remainder. So , In code , **d = pow(e, -1, φ(n))** →

Next step : we don't have φ(n).

To get φ(n),Formula is **φ(n) = (p - 1) * (q – 1)**

In case,p and q are multiply by random one number.

But I don't know how to get back this number.So,I went to openai and I asked by pasting code.It showed me : look at image



Here's a Python code snippet that reverses the encryption process and decrypts the message:

python — Copy code

```
from Crypto.Util.number import long_to_bytes

# Given values
c = ...  # Your 'c' value
n = ...  # Your 'n' value
p_encode = [...]  # Your 'p_encode' list
q_encode = [...]  # Your 'q_encode' list
num = ...  # Your 'num' value

# Step 2: Revert XOR operation
p_list = [str(int(val) ^ num) for val in p_encode]
q_list = [str(int(val) ^ num) for val in q_encode]

# Step 3: Reconstruct p and q
p = int("".join(p_list))
q = int("".join(q_list))

# Step 4: Calculate the private key 'd'
phi = (p - 1) * (q - 1)
e = 0x10001  # Public exponent
d = pow(e, -1, phi)  # Modular inverse of 'e' modulo 'phi'

# Step 5: Decrypt the ciphertext
m = pow(c, d, n)
plaintext = long_to_bytes(m).decode()

print("Decrypted Message:", plaintext)
```

Regenerate

Remember to replace the placeholders (`...`) with the actual values from your encryption

The write up for this challenge can complex or confuse your mind because my weak Eng unable explanation to get clearly.

And after analysic,I made script with python.In this way,when multiply number is not correct,you will get error.So,I used try except function to escaped this error in python.

Final result code : https://pastebin.com/raw/1RsZVvA0

Decryption formula:

Step 1 → φ(n) = (p - 1) * (q - 1)

step 2 → d = e^(-1) mod φ(n)

Step 3 → m=c^d%n

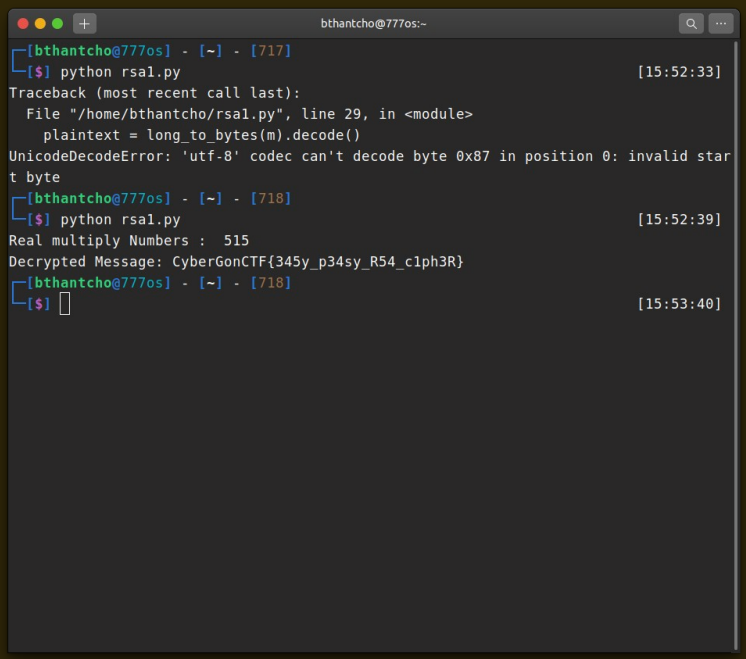
Explanation or assign value

e=0x10001

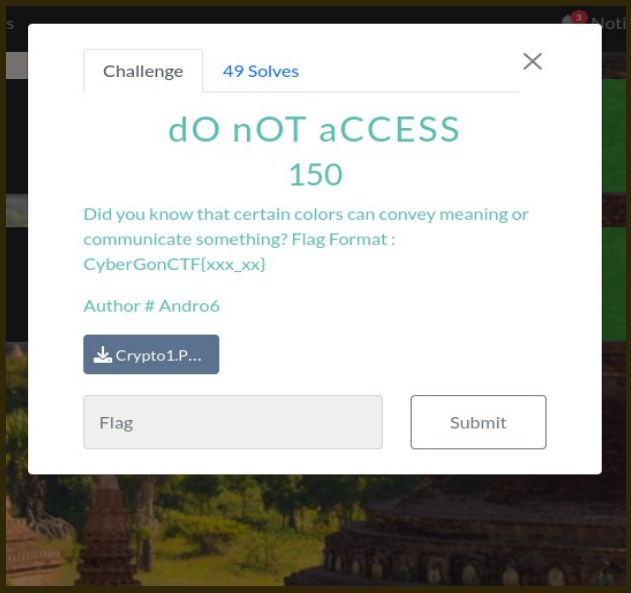
φ(n)=phi_n

Note : φ(n) is represent to phi.

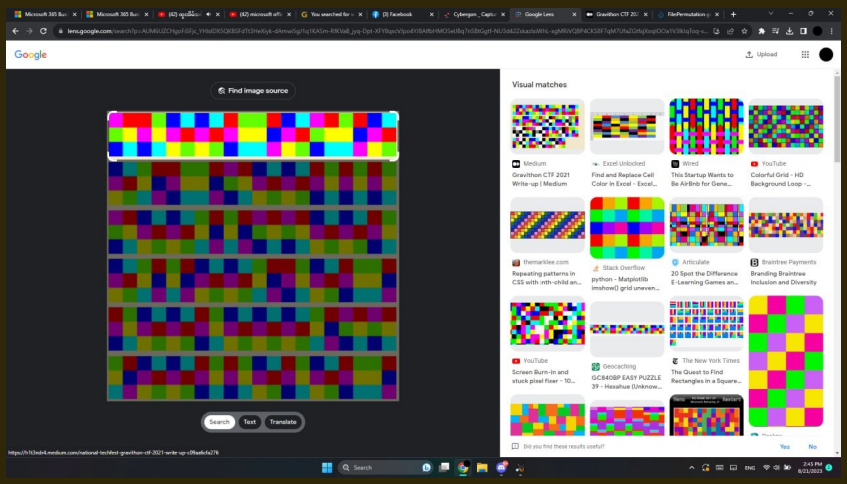
Result :



DO Not Access



At First, we got from image and recognize what it is. I use Google image search and I found one interesting link that is medium link.

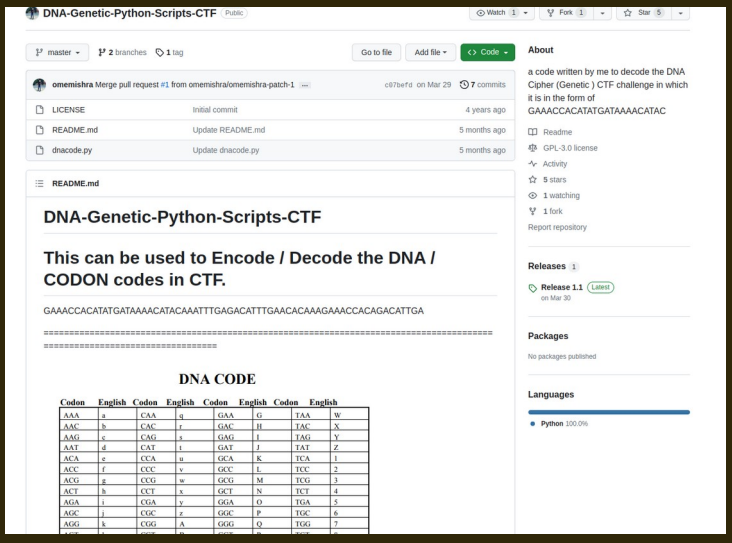


I read carefully and then I know what is that. So,I changed to plain text from this image with Hexahue Cipher.

And I got long text.WTH is that! I use decode fr tool to recognize what it is. I found genetic code

So I decode all of about this and found nothing. And next,I had idea to search by adding "CTF" after "Genetic code". So,I saw one GitHub link and found image that is include DNA code in this link.

The Link : https://github.com/omemishra/DNA-Genetic-Python-Scripts-CTF



Then,I got plaintext and flag after decrypted.

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N00b_ScRiptKidS

N 00b_ScRiptKid

N00b_ScRiptKidS