vishwaCTF

CHALLENGE NAME : [HAPPY VALENTINE’S DAY]

DEV : [PUSHKAR DEORE]

CATEGORY : [CRYPTOGRAPHY]

LEVEL : [EASY]

2024

Description:

My girlfriend and I captured our best moments of Valentine's Day in a portable graphics network. But unfortunately, I am not able to open it as I accidentally ended up encrypting it. Can you help me get my memories back?

Solution:

We are given this python source code:

```
from PIL import Image
from itertools import cycle
def xor(a, b):
    return [i^j for i, j in zip(a, cycle(b))]
f = open("original.png", "rb").read()
key = [f[0], f[1], f[2], f[3], f[4], f[5], f[6], f[7]]
enc = bytearray(xor(f,key))
open('enc.txt', 'wb').write(enc)
```

Here we can see that the encryption algorithm used is XORing the original byte array of original image cyclically with first 8 bytes for of the image. The original image is of PNG format and first 8 bytes of PNG files is fixed, i.e., `137 80 78 71 13 10 26 10`.

One of the properties of XOR is:

A ^ B = C

C ^ B = A

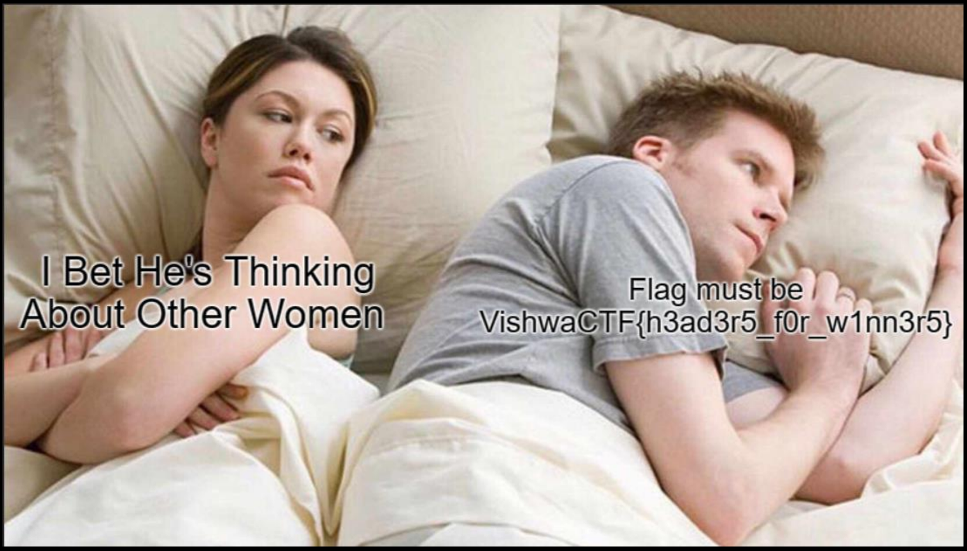
According to this, if we XOR the encrypted image with the fixed PNG bytes, we will get the original image back.

So we have to write the following script:

```
from PIL import Image
from itertools import cycle

def xor(a, b):
    return [i^j for i, j in zip(a, cycle(b))]
f = open("enc.txt", "rb").read()
key = [137 , 80 , 78 , 71 , 13 , 10 , 26 , 10]
print(key)
```

```
enc = bytearray(xor(f,key))
open('original.png', 'wb').write(enc)
Image.open('original.png').show()
```



Flag:

VishwaCTF{h3ad3r5_f0r_w1nn3r5}