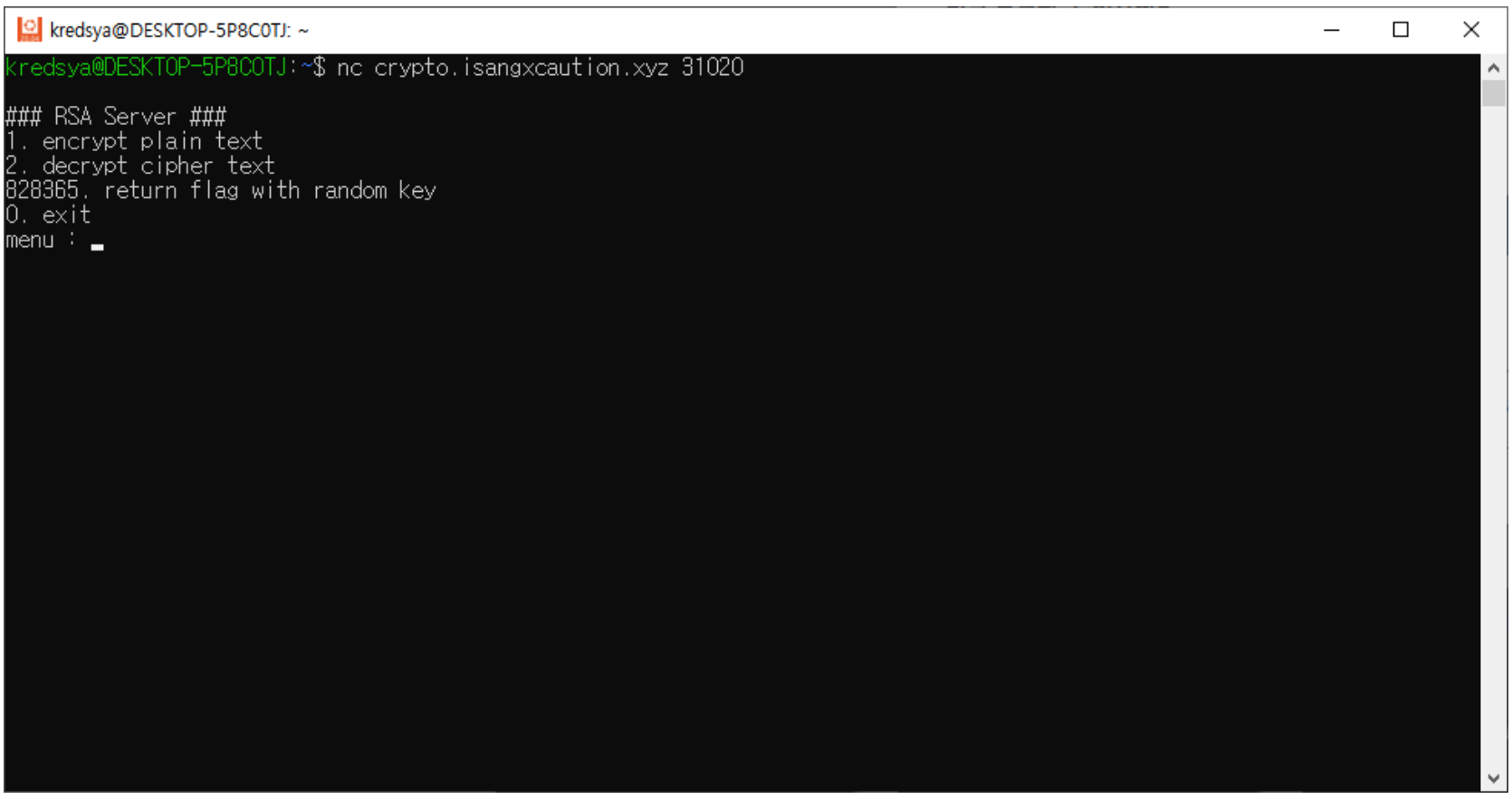
Where is my key

> M*ade by Kredsya*

nc crypto.isangxcaution.xyz 31020



나오는 메뉴 중 828365번 메뉴 진입

flag가 hex string으로, 연분수가 list로 주어진다.

일단 flag는 int로 바꿔서 cipher라고 명명해두겠다.

continued fraction은 원래는 d를 근사하기 위해서 $\frac{e}{N}$의 연분수 꼴을 list로 표현한 것이다.

https://en.wikipedia.org/wiki/Wiener's_attack#Example

Wiener’s attack 위키페이지에서 Example에 나오는 연분수를 list로 표현한 것을 참고.

```
frac = [...]
frac.reverse()

son = 1
```

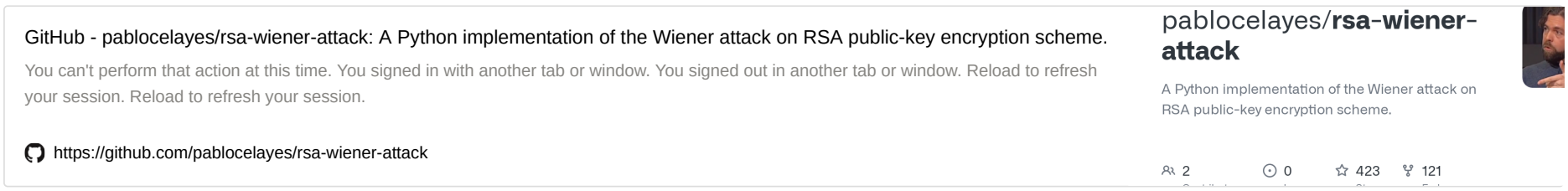
```
mom = frac[0]
for i in frac[1:-1]:
    son += i * mom
    son, mom = mom, son

print(son)
print(mom)
```

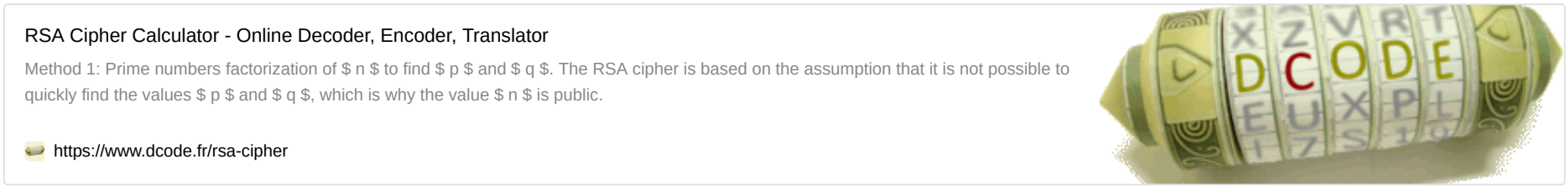
위 코드는 연분수에서 가장 아래 분수에서부터 차근차근 복구해서 올라오는 코드이다.

son은 분자, mom은 분모이다.

이걸 다시 역산해서 e랑 N을 구한다.

N은 1024비트지만 d는 254비트로 $\frac{N^{0.25}}{3}$보다 작으므로 wiener's attack을 사용할 수 있다.





d를 구하면 $\text{cipher}^d \equiv \text{flag} \pmod N$ 이 수식으로 flag를 구한다.

위 dcode.fr 에서도 복호화 할 수 있지만 기존 서버의 2번 메뉴를 통해 복호화 할 수 있다.