

Where is my key

Made by Kredsya

nc crypto.isangxcaution.xyz 31020

```
kredsya@DESKTOP-5P8C0TJ: ~
kredsya@DESKTOP-5P8C0TJ:~$ nc crypto.isangxcaution.xyz 31020

### RSA Server ###
1. encrypt plain text
2. decrypt cipher text
828365. return flag with random key
0. exit
menu : _
```

나오는 메뉴 중 828365번 메뉴 진입

```
kredsya@DESKTOP-5P8C0TJ: ~
828365. return flag with random key
0. exit
menu : 828365
flag = 0b6ed1ad1d9635e25d68be95ec14b222b871b325a80ea65fb85d0014da577db6629f02fb9d005f0f2e5e20cc06341d200a54be54706fb0cf9
55d8d22f94e55833a7c5b2506b8bb3ca2b23915ab2a40bdf3fbc433e252652c1edb4a83350b37e19c20e5dbd589a353ea0e6ed6890c5e9e2d66dc1a1
9d3546cc66888be1a9e07af
continued fraction = [0, 5, 2, 6, 457, 2, 1, 1, 2, 1, 1, 9, 3, 1, 9, 1, 4, 1, 8, 1, 1, 1, 1, 3, 3, 2, 2, 1, 3, 2, 5, 3,
1, 1, 1, 29, 15, 1, 695, 2, 9, 4, 1, 4, 2, 1, 1, 1, 2, 1, 2, 1, 3, 2, 2, 7, 3, 1, 3, 2, 1, 13, 22, 1, 1, 1, 2, 1, 2, 1,
5, 1, 2, 6, 57, 1, 3, 2, 1, 1, 1, 10, 1, 27, 1, 1, 15, 1, 2, 7, 1, 40, 3, 1, 1, 1, 1, 1, 2, 7, 2, 15, 2, 11, 8, 1, 2, 2,
7, 2, 4, 1, 6, 2, 6, 1, 7, 1, 1, 1, 13, 1, 208, 2, 1, 1, 1, 2, 3, 2, 9, 1, 4, 56, 3, 1, 1, 5, 84, 1, 1, 1, 2, 2, 1, 2,
1, 1, 3, 37, 60, 2, 2, 2, 6, 40, 1, 3, 1, 2, 4, 2, 1, 1, 1, 2, 4, 4, 4, 1, 1, 5, 1, 7, 1, 7, 261, 1, 1, 8, 41, 1, 59, 1,
6, 11, 13, 3, 1, 2, 1, 7, 11, 1, 1, 8, 8, 1, 1, 1, 1, 1, 2, 1, 2, 4, 5, 1, 2, 1, 9, 1, 2, 3, 1, 1, 19, 1, 1, 1, 3, 2, 1,
7, 8, 29, 1, 5, 1, 2, 1, 353, 1, 4, 4, 1, 1, 2, 2, 13, 1, 1, 2, 1, 52, 1, 9, 1, 35, 1, 1, 1, 6, 1, 1, 1, 1, 6, 2, 2, 31,
2, 3, 4, 1, 1, 90, 1, 1, 3, 4, 1, 1, 6, 2, 2, 1, 5, 2, 1, 1, 1, 2, 1, 8, 2, 5, 6, 1, 1, 61, 3, 2, 26, 1, 3, 2, 1, 6, 12,
, 2, 15, 1, 2, 4, 1, 3, 15, 4, 1, 31, 1, 7, 1, 2, 9, 3, 18, 1, 25, 2, 1, 1, 4, 1, 9, 1, 1, 1, 6, 3, 1, 1, 1, 1, 2, 2, 1,
2, 2, 3, 9, 60, 1, 1, 2, 40, 1, 3, 1, 3, 1, 2, 9, 11, 1, 4, 3, 2, 1, 15, 1, 2, 1, 1, 1, 3, 1, 4, 1, 1, 10, 1, 5, 2, 2,
18, 1, 5, 1, 1, 1, 5, 1, 1, 1, 1, 5, 2, 41, 1, 1, 1, 1, 5, 9, 2, 8, 10, 13, 2, 1, 1, 1, 1, 1, 1, 2, 2, 14, 1, 1, 2, 1, 1,
, 286, 2, 4, 6, 16, 10, 1, 3, 2, 6, 12, 1, 8, 1, 3, 6, 1, 5, 1, 1, 1, 7, 1, 6, 1, 46, 1, 1, 1, 4, 5, 6, 4, 1, 1, 2, 1, 3,
, 3, 2, 1, 1, 19, 4, 3, 104, 6, 2, 2, 1, 4, 2, 2, 4, 4, 4, 1, 1, 1, 6, 19, 3, 1, 6, 2, 2, 2, 10, 2, 1, 1, 4, 2, 1, 1, 1,
6, 80, 1, 96, 1, 8, 2, 2, 1, 1, 7, 2, 1, 1, 1, 3, 143, 1, 39, 1, 6, 5, 3, 2, 2, 5, 16, 1, 3, 1, 3, 1, 1, 2, 1, 1, 1, 11,
, 5, 4, 1, 1, 1, 1, 1, 1, 3, 1, 1, 1, 1, 3, 1, 1, 19, 1, 1, 3, 3, 3, 5, 10, 1, 2, 1, 3, 61, 11, 1, 2, 1, 1, 39, 1, 6, 6,
1, 7, 10, 1, 1, 1, 7, 1, 5, 1, 1, 23, 1, 6, 1, 9, 1, 1, 1, 7, 3, 1, 2, 1, 2, 10, 2, 2, 15, 1, 3, 1, 18, 2, 2, 3, 2, 1,
2, 1, 1, 1, 3]
```

```
### RSA Server ###
1. encrypt plain text
2. decrypt cipher text
828365. return flag with random key
0. exit
menu : _
```

flag가 hex string으로, 연분수가 list로 주어진다.

일단 flag는 int로 바꿔서 cipher라고 명명해두겠다.

continued fraction은 원래는 d를 근사하기 위해서 $\frac{c}{N}$ 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.

GitHub - pablocelayes/rsa-wiener-attack: A Python implementation of the Wiener attack on RSA public-key encryption scheme.

You can't perform that action at this time. You signed in with another tab or window. You signed out in another tab or window. Reload to refresh your session. Reload to refresh your session.

<https://github.com/pablocelayes/rsa-wiener-attack>

pablocelayes/rsa-wiener-attack

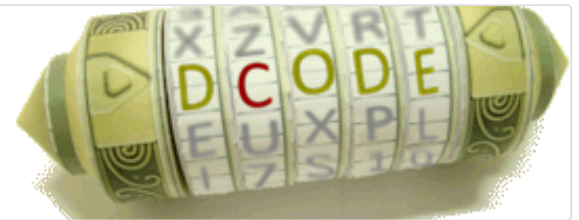
A Python implementation of the Wiener attack on RSA public-key encryption scheme.

2 0 423 121

RSA Cipher Calculator - Online Decoder, Encoder, Translator

Method 1: Prime numbers factorization of \$ n \$ to find \$ p \$ and \$ q \$. The RSA cipher is based on the assumption that it is not possible to quickly find the values \$ p \$ and \$ q \$, which is why the value \$ n \$ is public.

<https://www.dcode.fr/rsa-cipher>



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

위 [dcode.fr](https://www.dcode.fr) 에서도 복호화 할 수 있지만 기존 서버의 2번 메뉴를 통해 복호화 할 수 있다.

```
kredsya@DESKTOP-5P8C0TJ: ~
3, 24, 3, 17, 2, 5, 3, 66, 1, 2, 9, 2, 5, 7, 1, 4, 1, 5, 9, 1, 1, 1, 9728, 1, 2, 2, 2, 2, 1, 2, 13, 1, 1, 9, 28, 4, 27,
2, 300, 94, 6, 1, 2, 1, 1, 1, 1, 1, 1, 1, 4, 1, 3, 1, 1, 6, 2, 8, 12, 28, 6, 2, 1, 5, 2, 40, 1, 2, 5, 8, 5, 1, 2, 1, 5,
3, 4, 8, 4, 1, 4, 1, 2, 1, 3, 1, 1, 2, 3, 3, 1, 1, 1, 34, 1, 2, 34, 1, 7, 2, 2, 4, 1, 32, 3, 1, 1, 1, 36, 1, 7, 1, 3, 1,
3, 1, 52, 5, 1, 6, 10, 1, 1, 1, 4, 2, 7, 1, 38, 12, 1, 26, 2, 4, 5, 2, 3, 376, 1, 4, 1, 106, 5, 2, 6, 2, 2, 10, 1, 1,
2, 4, 1, 7, 2, 1, 8, 2, 2, 1, 4, 1, 1, 13, 2, 5, 1, 3, 1, 1, 10, 2, 1, 2, 1, 3, 3, 1, 1, 1, 1, 2, 1, 2, 3, 1, 1, 1, 12,
11, 2, 1, 2, 6, 5, 2, 1, 30, 1, 4, 4, 1, 5, 2, 2, 10, 1, 6, 2, 2, 2, 6, 1, 1, 1, 13, 1, 3, 4, 7, 4, 1, 2, 5, 1, 1, 20, 1,
1, 1, 7, 1, 7, 1, 1, 7, 1, 1, 1, 1, 1, 1, 25, 3, 2]

### RSA Server ###
1. encrypt plain text
2. decrypt cipher text
828365. return flag with random key
0. exit
menu : 2
N = 68580233122498150159310439204652664449334654722917652754057332129609194464017405220017907958661026880338865203881718
413433787171329811436867260581943486460593371969819503395077406649016759153040942948281230012476453393079770177449485214
006359945925422444537920727096117090190172406219564490904633440751272761
d = 22803293553655943998558655638863844774392575378128569984353938158829446355079
cipher text(hex) = 30727e6b2646c0a2e7a2cd0e97f538fb32958973eca16460fc964fa80609dfaa53d8bfa617d7842bc7d7e254128b93a7ba584
be8503715f987957c31d29f597ee03d5e248b25a3804cec8b579757c779f4a08879d6fa3d835ae79e1e9c271abaa8261a3fd7d59ebba44bc2454a623
a2d2a5cf205799e251be5dbf1301e655edf
plain text = lxC{l_thlnk_wieners_att4ck_is_g00d_to_5tudy}

### RSA Server ###
1. encrypt plain text
2. decrypt cipher text
828365. return flag with random key
0. exit
menu : 0
```