

Blinding

Made by Kredsya

nc crypto.isangxcaution.xyz 31000

```
kredsya@DESKTOP-5P8C0TJ: ~  
kredsya@DESKTOP-5P8C0TJ:~$ nc crypto.isangxcaution.xyz 31000  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : _
```

우선 1번 메뉴로 N과 e에 대한 정보를 얻어준다.

```
kredsya@DESKTOP-5P8C0TJ: ~  
kredsya@DESKTOP-5P8C0TJ:~$ nc crypto.isangxcaution.xyz 31000  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : 1  
N = 12179240231912957710652629140697312342572279559135786977849308861185306000393456141214439159483830342450421166754413  
952059919197626538377007363325448669537124919669428514518428439213823617017946859864142768900197905523229799342077855230  
3215215396869788343418719570650668321384637581417834374430937003824834151  
e = 13  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : _
```

e는 항상 13으로 고정이다.

우리가 원하는건 4번 메뉴에서 “Alice”의 서명을 제출해서 flag를 받는 것이다.

그래서 2번 메뉴인 make signature에서 서명을 해야 하는데, “Alice”의 hex string인 416c696365를 그대로 넣으면 Don't cheat라는 메시지가 나온다.

```
kredsya@DESKTOP-5P8C0TJ: ~  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : 1  
N = 12179240231912957710652629140697312342572279559135786977849308861185306000393456141214439159483830342450421166754413  
952059919197626538377007363325448669537124919669428514518428439213823617017946859864142768900197905523229799342077855230  
3215215396869788343418719570650668321384637581417834374430937003824834151  
e = 13  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : 2  
msg(hex) : 416c696365  
Don't cheat :<  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode :
```

따라서 그대로 넣지 않고 2^e 을 곱해서 서명을 요청할 것이다. (2가 아니라 다른 랜덤한 수 r 이어도 괜찮지만 수가 너무 커지므로 2를 권장한다)

```
kredsya@DESKTOP-5P8C0TJ: ~  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : 2  
msg(hex) : 416c696365  
Don't cheat :<  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : 2  
msg(hex) : 82d8d2c6ca000  
89068ab76cc1836600ab2eec7b25fcb836ac40b804a4768d5b548b8ad88c6c1b1fd9ef105f146ee4af88840aad4a8d8cc10e2c022dd4abff3fdd0d04  
1e1c3cc1941e7bac911816df6ea26ca663ee5ddfcfcb74a11487a0c9dde2a42bb3aa6437db8034bab675b1d51133e5947befd8e4aab07ecff2725788  
1f505be34a5a69cb  
=== Welcome to Alice's server ===  
1. get information  
2. make signature  
3. verify signature  
4. challenge  
0. exit  
mode : _
```

서명이 왔다.

이걸 int로 바꿔서 2의 역수를 곱해주면 원래 우리가 원하던 “Alice”의 서명이 된다.

$$(2^e M)^d \equiv 2^{ed} M^d \equiv 2^{\phi(N)-1} M^d \equiv 2^{-1} M^d \equiv S^d \pmod{N}$$

아래는 제출 결과이다.

```
kredsya@DESKTOP-5P8COTJ: ~
3. verify signature
4. challenge
0. exit
mode : 3
msg(hex) : 426f62
sign(hex) : 43882486217779c0f7f30f71ddcc00dcaa75ba408b3764eb7bf01e5cfd566362ba6345e8e8a7dbfee570ed009e061b25dc38730fbc33
2a1a982484a4b4d3b15d86a5bd80c5e58c4102ad34ed557fe2c6a067d30b0f10437bd030cb3d3ea44a34d79c468087a3b0a573866d5b0144d1e15370
6efeebadb78ab224bd0af8dc216c
verifying success

=== Welcome to Alice's server ===
1. get information
2. make signature
3. verify signature
4. challenge
0. exit
mode : 4
sign : 9b3b5a43529a076f89a62ad11935723f625065333c65f2c0cf6ff1a267e5714d11d57924fe9d009637abf5537aafc4ab3e51919c5e787ee74
09ce2355828a6a7b3ed9f4f7c8b5ca6f2c7d37adcbf259dbb813fd6afa24f1939391d0b1828c1781708dda6995878582b2e98194d61e12039e4e9873
2320f26f12f0e920f1fa819
Here is flag
b'!xC{Blinding_i5_on3_of_the_3lment4r7_att4cks}'

=== Welcome to Alice's server ===
1. get information
2. make signature
3. verify signature
4. challenge
0. exit
mode :
```