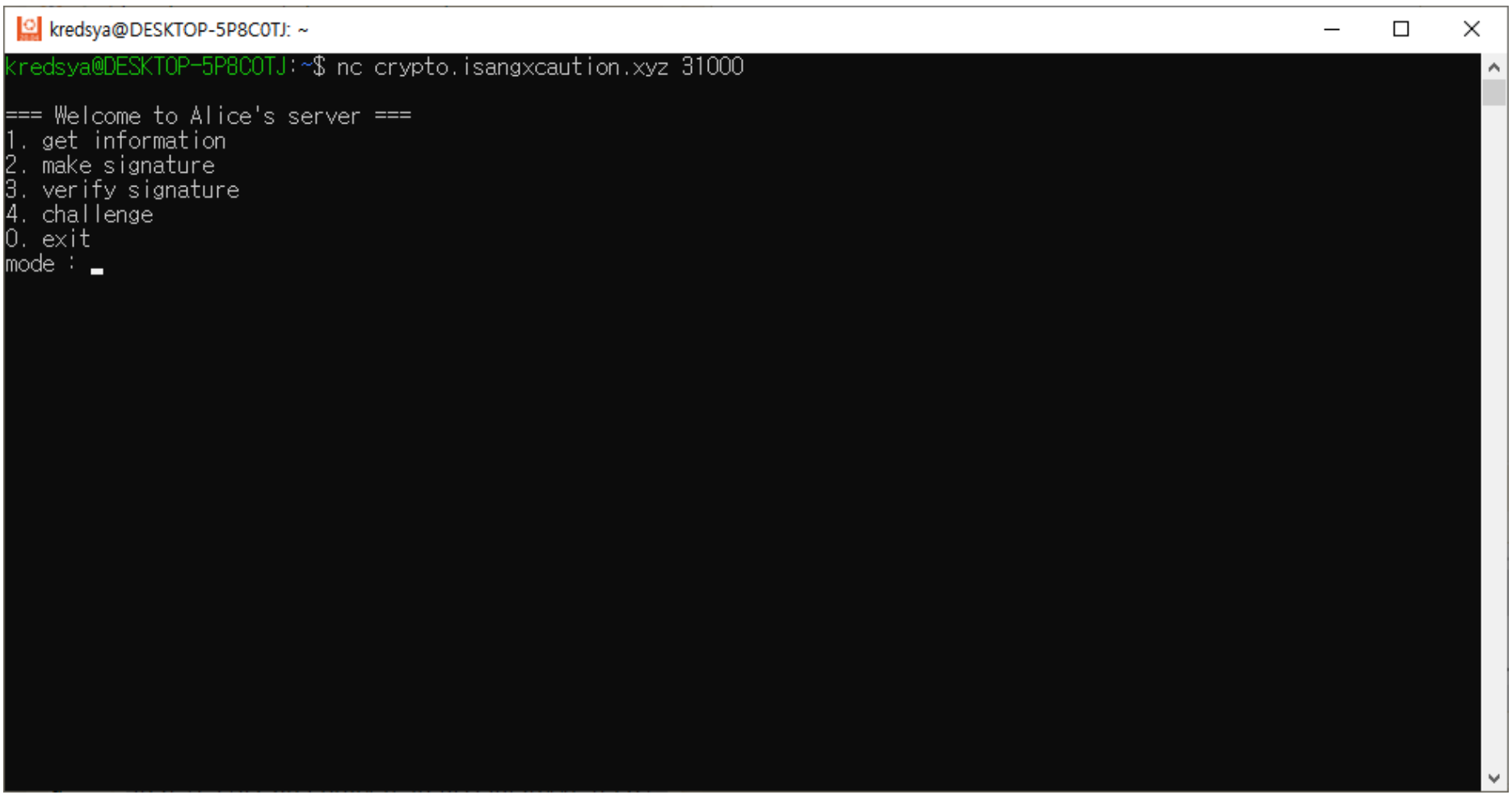
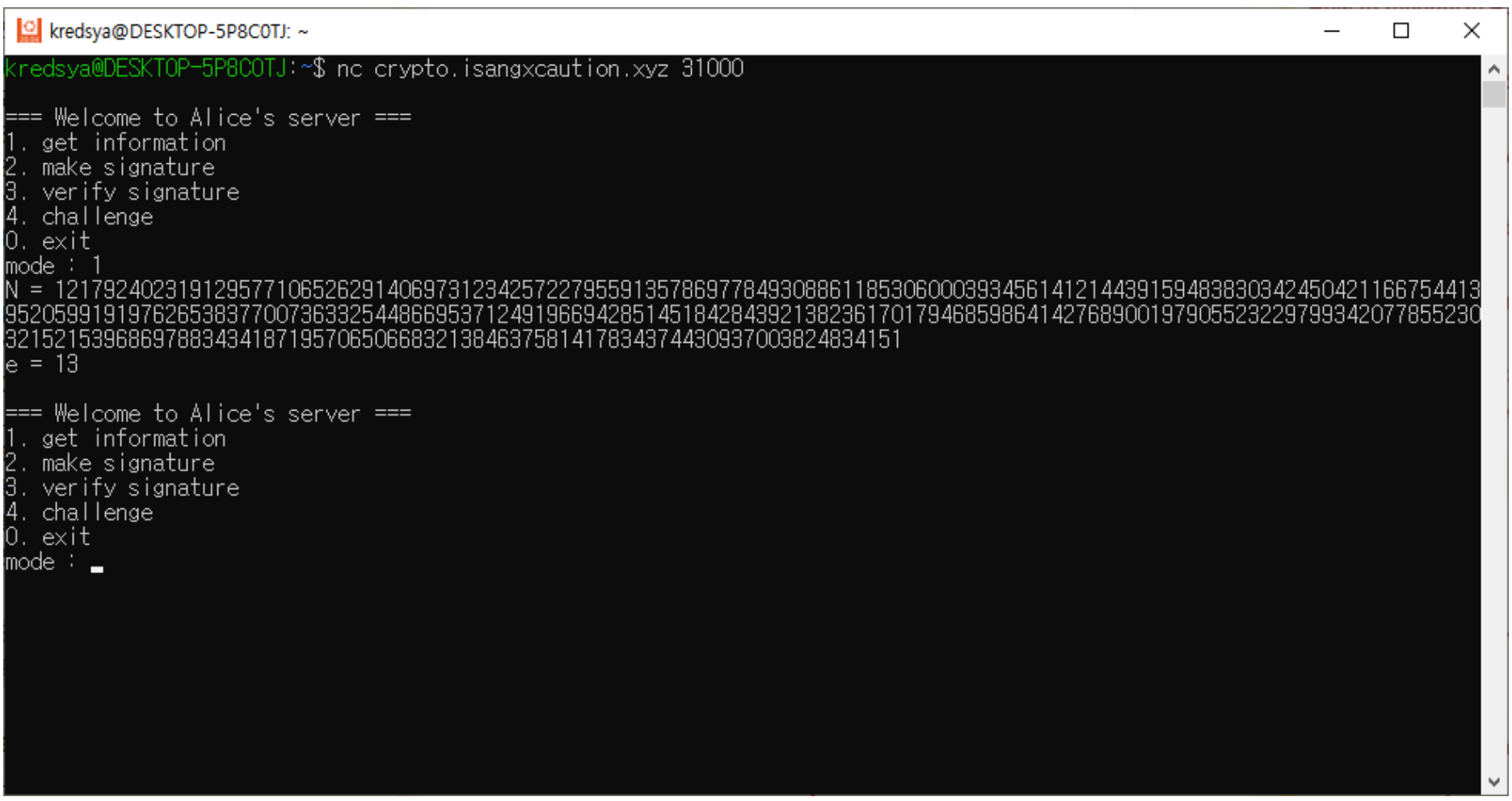
Blinding

> M*ade by Kredsya*

nc crypto.isangxcaution.xyz 31000



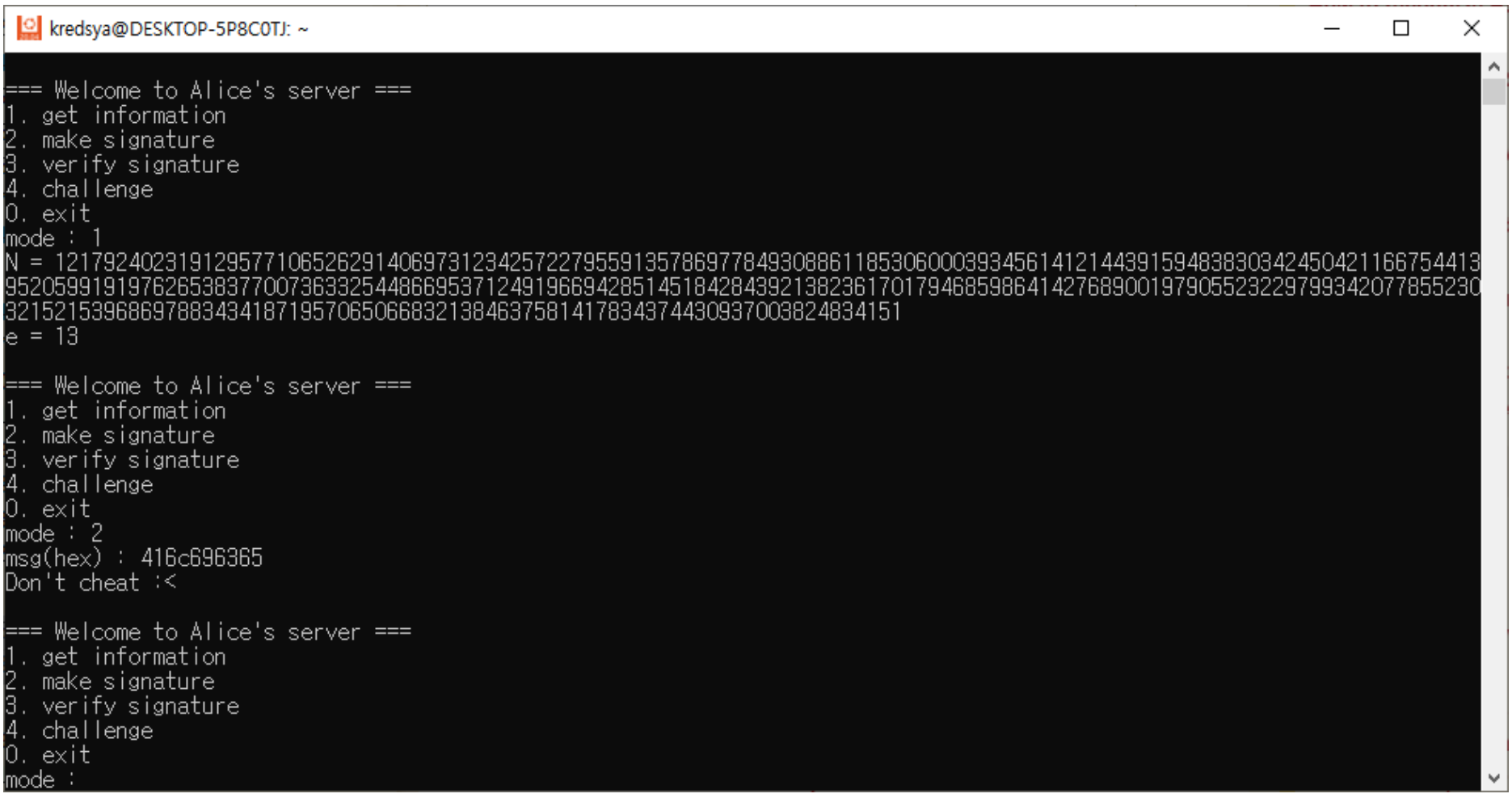
우선 1번 메뉴로 N과 e에 대한 정보를 얻어준다.



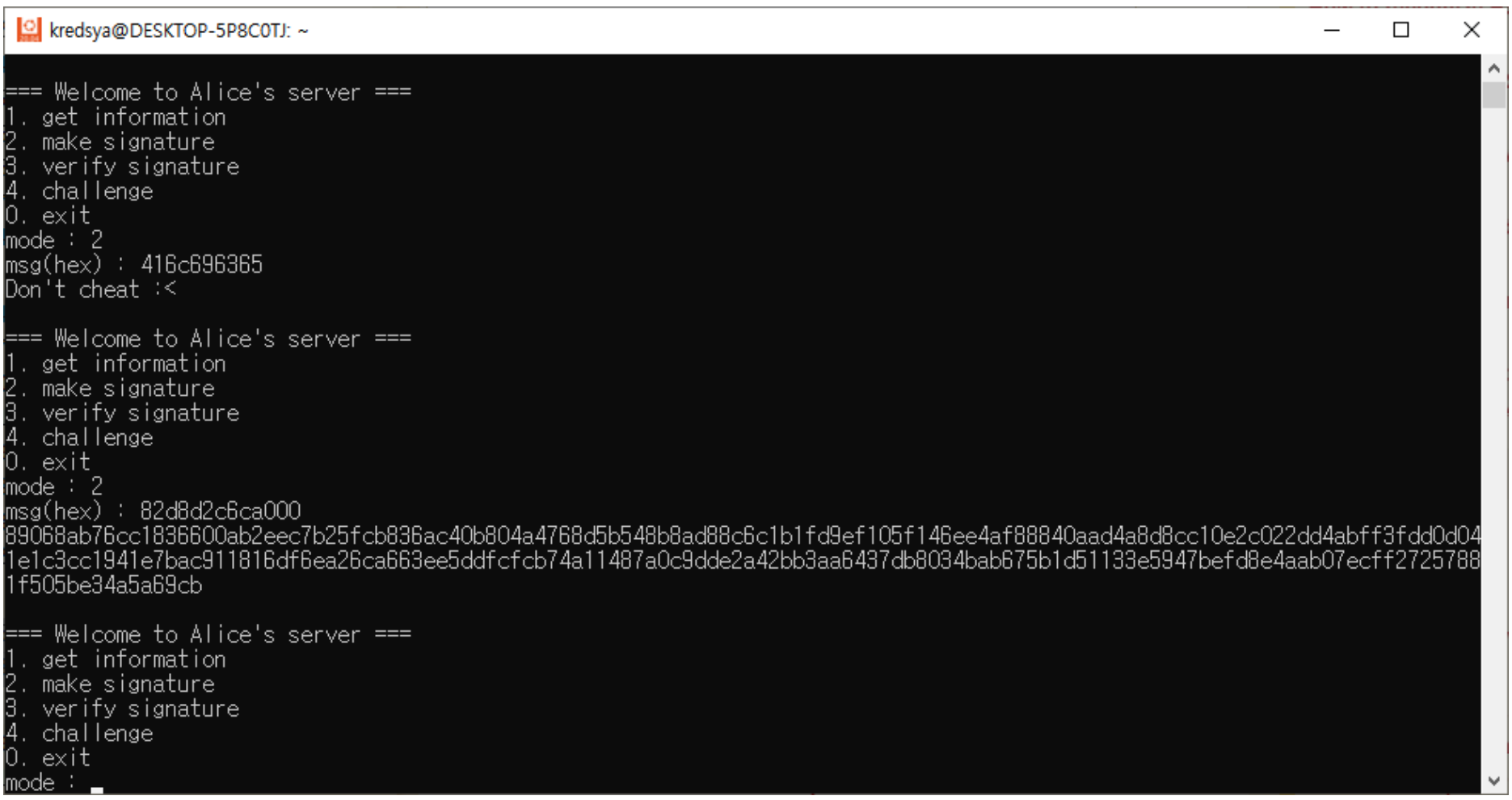
e는 항상 13으로 고정이다.

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

그래서 2번 메뉴인 make signature에서 서명을 해야 하는데, “Alice”의 hex string인 416c696365을 그대로 넣으면 Don’t cheat라는 메시지가 나온다.



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

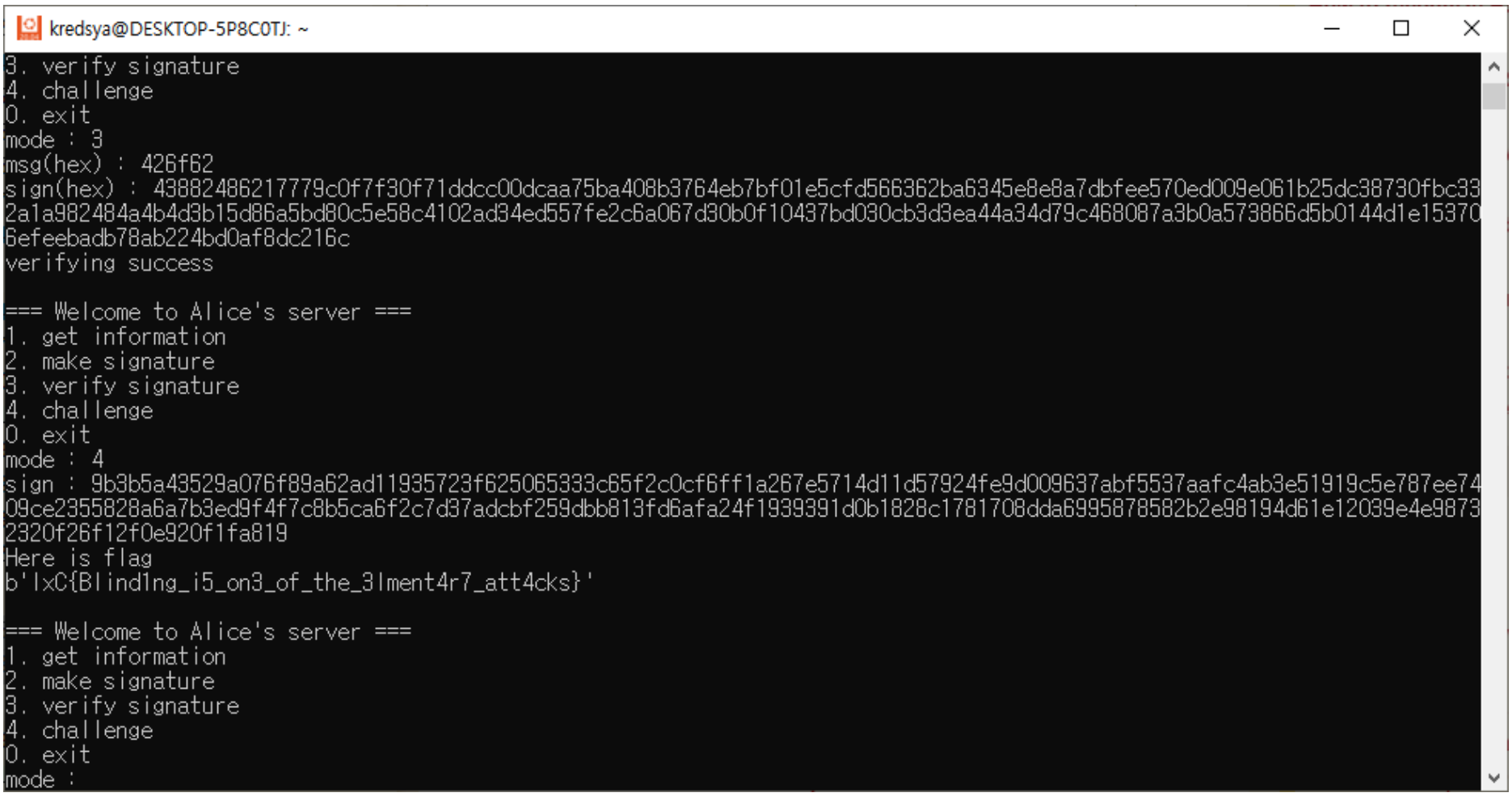


서명이 왔다.

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-5P8C0TJ: ~
3. verify signature
4. challenge
0. exit
mode : 3
msg(hex) : 426f62
sign(hex) : 438824862177779c0f7f30f71ddcc00dcaa75ba408b3764eb7bf01e5cfd566362ba6345e8e8a7dbfee570ed009e061b25dc38730fbc33
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'lxC{Blindlng_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 :