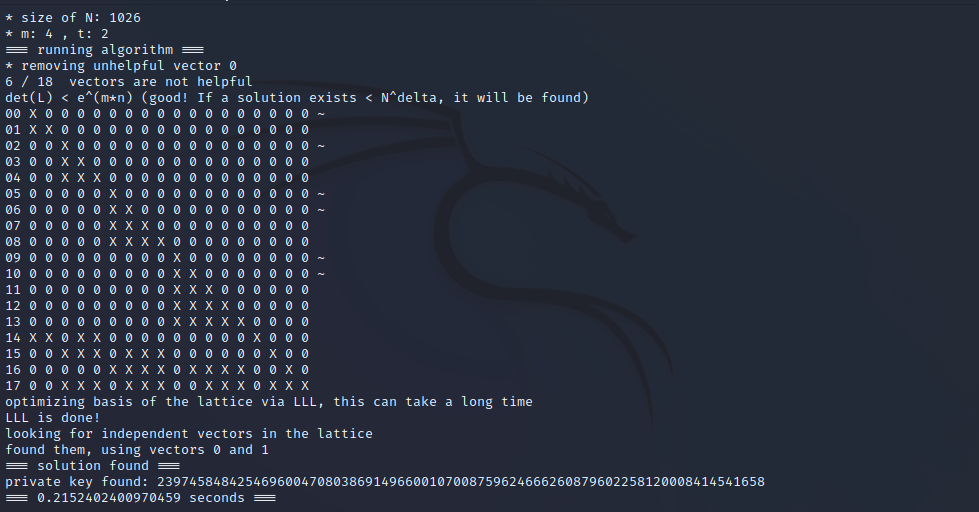
Exploit code 참고 URL: <https://github.com/mimoo/RSA-and-LLL-attacks/blob/master/boneh_durfee.sage>

이 문제는 RSA의 개인키 d가 작아서 발생하는 취약점을 통해 개인키를 구하는 문제로, boneh Durfee attack을 사용하여 풀 수 있다.

<https://github.com/mimoo/RSA-and-LLL-attacks/blob/master/boneh_durfee.sage>

해당 사이트의 코드를 활용하여 개인키를 구할 수 있다.



d: 2397458484254696004708038691496600107008759624666260879602258120008414541658

flag: CUHA{2397458484254696004708038691496600107008759624666260879602258120008414541658}