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

이 문제는 RSA의 개인키 d가 낮아서 발생하는 취약점을 통해 개인키를 구하는 문제로, boneh Durfee attack을 사용하여 푸는 문제이다.

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

해당 사이트의 코드를 활용하여 개인키를 구할 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명

d: 23974584842546960047080386914966001070087596246662608796022581200084145416583

flag: CUHA{23974584842546960047080386914966001070087596246662608796022581200084145416583}