[2023 JBUCTF] crypto

random\_primes

Write-Up

문제 개요

제공 파일 : random\_primes.py

텍스트, 스크린샷, 소프트웨어, 디스플레이이(가) 표시된 사진

자동 생성된 설명

gen\_prime\_list 함수로 소수들로 이루어진 리스트를 생성해서 그 리스트 중에서 랜덤으로 소수를 골라서 p, q 변수에 값을 저장한다.

그 후에 p, q를 RSA의 개인키로 이용하여 flag를 암호화하고, 그 암호화 한 값과, 생성한 리스트를 출력한다.

문제 풀이

RSA 암복호화 참고 : <https://url.kr/56ngfw>

소수 리스트의 크기가 총 4이고 이중에서 중복으로 2개의 소수를 선택하여 개인키 값을 정하기 때문에 4H2 = 5C2 = 10개의 조합으로 p, q 값을 정해서 RSA 복호화를 시도하면 10번의 시도중에서 flag를 획득할 수 있다.

exploit.py

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

FLAG

scpCTF{78de570e092fd854ff182094744b00f0a494c67ed03a20274b52b7733c01ca141cead68519637556619c7271a6bb00ad}