[2023 JBUCTF] crypto

same\_nonce\_1

Write-Up

문제 개요

제공 파일 : same\_nonce\_1.py

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

1번을 입력하면 base64 인코딩 된 data를 입력 받고, 입력 받은 data를 디코딩 후, AES-CTR 모드로 동일한 key, nonce를 사용해서 암호화 한 값을 base64 인코딩해서 출력을 한다.

2번을 입력하면 flag를 AES-CTR 모드로 동일한 key, nonce를 사용해서 암호화 한 값을 base64인코딩하여 출력한다.

문제 풀이

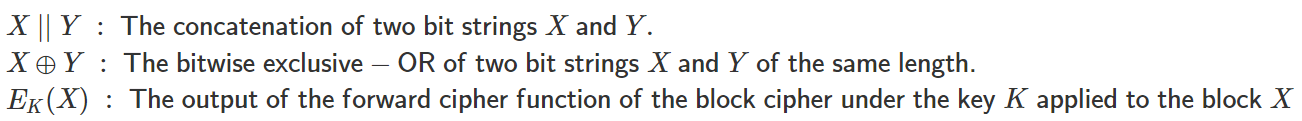
AES-CTR 참고 : <https://url.kr/lzcyk9>

CTR 운영모드는 nonce값과 counter값을 이어 붙여서 key로 블록 암호화를 한 결과를 평문과 xor해서 암호문을 생성해낸다.

문제에서는 입력 받은 값과 flag를 동일한 key와 nonce로 암호화한다.

즉 입력한 값의 암호문과 flag의 암호문은 동일한 값으로 xor되어 있는 상태이다.

따라서 flag와 동일한 길이의 평문을 암호화 한 값을 flag의 암호화 값에 xor하고 그 값에 평문을 다시 xor하면 flag 값을 알 수 있다.



텍스트, 폰트, 화이트, 대수학이(가) 표시된 사진

자동 생성된 설명

exploit.py

텍스트, 스크린샷, 소프트웨어, 멀티미디어 소프트웨어이(가) 표시된 사진

자동 생성된 설명

FLAG

scpCTF{5e9f0fc6422fb589154a7827204c5720c61347e629df}