[2023 JBUCTF] crypto

slide

Write-Up

문제 개요

제공 파일 : myCrypto.py, slide.py

slide.py

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

myCrypto 클래스의 인스턴스인 crypto를 랜덤한 16byte키로 초기화 해서 생성한다.

그리고 flag를 myCrypto 클래스의 encrypt 함수로 암호화 한 결과를 enc\_flag 변수에 저장한다.

1 입력

입력 받은 문자열을 base64 디코딩 후, pad함수로 패딩을 하고, myCrypto 클래스의 encrypt 함수로 암호화 한 결과를 base64 인코딩 해서 출력한다.

2 입력

1을 입력한 것과 동작이 비슷하지만 encrypt 함수가 아닌 round함수를 사용한 결과를 출력한다.

3 입력

enc\_flag 값을 base64인코딩해서 출력한다.

4 입력

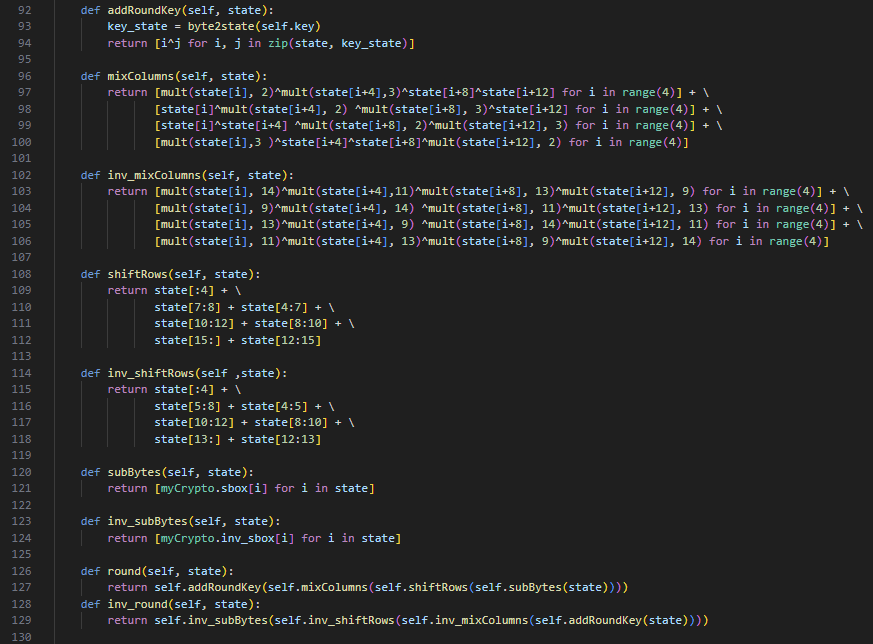
프로그램을 종료한다.

myCrypto.py

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명스크린샷, 텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

아래의 함수들은 16byte 또는 길이가 16인 값을 인자로 갖는다.

패딩 참고

# Wikipedia Padding (cryptography) : <https://url.kr/v76dwc>

# IBM PKCS padding method : <https://url.kr/rblvmy>

def pad(byte, block\_size) : PKCS#7 Padding

def unpad(byte, block\_size) : PKCS#7 UnPadding

def byte2list(byte) : Byte To List

def list2byte(arr) : List To Byte

def list2state(arr) : List To State

def state2list(state) : State To List

def byte2state(byte) : Byte To State

def state2byte(state) : State To Byte

def mult(x, y) : GF(2^8) Multiplication

myCrypto 클래스 함수

def addRoundKey(self, state)

def mixColumns(self, state)

def inv\_mixColumns(self, state)

def shiftRows(self, state)

def inv\_shiftRows(self ,state)

def subBytes(self, state)

def inv\_subBytes(self, state)

위 함수들은 AES의 연산을 구현한 함수들이다. 자세한 내용은 아래 링크를 참고하자.

# Advanced Encryption Standard (AES) : <https://url.kr/9nw6t2>

def round(self, state) : addRoundKey(mixColumns(shiftRows(subBytes(state))))를 계산한다.

def inv\_round(self, state) : round함수의 역연산이다.

def encrypt(self, state) : 입력 받은 값을 16byte씩 나눠서 round함수를 20번 수행한다.

def decrypt(self, state) 입력 받은 값을 16byte씩 나눠서 inv\_round 함수를 20번 수행한다.

문제 풀이

2번을 입력 시 원하는 문자열을 한번의 round함수를 거친 값을 알 수 있다.

입력한 문자열을 A라 할 때, A에 round함수를 적용하면

subBytes, shiftRows, mixColumns, addRoundKey 순으로 함수가 적용된다.

따라서 A에 round함수가 적용된 값을 B라 하면

B = addRoundKey(mixColumns(shiftRows(subBytes(A)))) 이다.

이때 subBytes, shiftRows, mixColumns 함수는 addRoundKey 함수처럼 key와 같은 비밀 값을 사용하지 않는 함수이므로 mixColumns(shiftRows(subBytes(A)))는 계산이 가능하다.

이 값을 A’ 이라고 하면 B = addRoundKey(A’) 이다.

addRoundKey연산은 key와 매개변수 값을 xor연산을 하는 함수이므로

B = addRoundKey(A’) = A’ xor Key이고, B = A’ xor key 이므로 B xor A’ = key이다.

즉 key를 알아낼 수 있다.

이제 구한 key값으로 myCrypto 인스턴스를 생성해서 enc\_flag를 복호화 하면 flag값이 나온다.

주의 사항 : 문제 풀이 코드 작성시 state, byte 변환을 신경 써서 해야 한다.

exploit.py

텍스트, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

FLAG

scpCTF{83e19dccdeba1b0f16fabf44165da7d23dbe82a4d7f983db4631fb5191­­29}