BUUCTF 每日打卡 2021-05-12

原创

Σ2333! 于 2021-05-12 20:06:36 发布 169 收藏 2

分类专栏： crypto 文章标签： 密码学

本文链接：https://blog.csdn.net/weixin_52446095/article/details/116719649

引言

昨天爆肝完红帽杯 primegame 的 wp 解析，原本想举一反三一下做一下 cryptohack 的一道类似的题，但是太晚了，今天补上

至于另一道，想留到周末讲，周六还有国赛要打

[cryptohack]Real Eisenstein

yysy 这个题目描述给了跟没给一样

看加密代码：

```
import math
from decimal import *
getcontext().prec = 100

FLAG = "crypto{????????????????}"
PRIMES = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 1
03]

h = Decimal(0.0)

for i, c in enumerate(FLAG):
    h += ord(c) * Decimal(PRIMES[i]).sqrt()

ct = math.floor(h*16**64)
print(f"ciphertext: {ct}")

# ciphertext: 13509953979273556579567869556030124102600173448059980767028281603166950045884294 33
```

跟红帽杯的加密代码不能说毫不相干，只能说完全一样
唯二不一样的，就是把 primes 限定在 [0, 105]，把 ln() 换成了 sqrt()
直接上 sage 代码：

```
from decimal import *
import math

getcontext().prec = int(100)

primes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 1
03]

keys = []
for i in range(len(primes)):
    keys.append(Decimal(int(primes[i])).sqrt())

arr = []
for v in keys:
    arr.append(int(v * int(16) ** int(64)))

ct = 135099539792735565795678695560301241026001734480599807670282816031669500458842943 3

def encrypt(res):
    h = Decimal(int(0))
    for i in range(len(keys)):
        h += res[i] * keys[i]
    ct = int(h * int(16)**int(64))
    return ct

def f(N):
    ln = len(arr)
    A = Matrix(ZZ, ln + 1, ln + 1)
    for i in range(ln):
        A[i, i] = 1
        A[i, ln] = arr[i] // N
        A[ln, i] = 64

    A[ln, ln] = ct // N

    res = A.LLL()

    for i in range(ln + 1):
        flag = True
        for j in range(ln):
            if -64 <= res[i][j] < 64:
                continue
            flag = False
            break
        if flag:
            vec = [int(v + 64) for v in res[i][:-1]]
            ret = encrypt(vec)
            if ret == ct:
                print(N, bytes(vec))
            else:
                print("NO", ret, bytes(vec))

for i in range(2, 10000):
    print(i)
    f(i)
```

这里采用“原题”解法，比较方便
结果为：

```
2
3
NO 135099539792735565795678695500000000000000000000000000000000000000000000000000000000000000 b'crypto{r341_t0_23D_m4p}\x00\x00\x00\x00'
4
5
6
7
8
NO 135099539792735565795678695500000000000000000000000000000000000000000000000000000000000000 b'crypto{r341_t0_23D_m4p}\x00\x00\x00\x00'
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
NO 135099539792735565795678695500000000000000000000000000000000000000000000000000000000000000 b'crypto{r341_t0_23D_m4p}\x00\x00\x00\x00'
31
32
33
34
35
```


crypto{r34l_t0_23D_m4p}

编码与调制

直接把 wp 的地址放在题目里面我是没想到的。。。
看到这个题目，想到以前做的一道传感器
事实上也是考查曼彻斯特编码（当时迷惑的地方就是，如果出现“00”或“11”的情况怎么没有考虑，现在想想，加密的时候也不会出现啊）
将题目给的十六进制字符串转化成二进制，“10”（高电平转低电平）替换成“1”，“01”（低电平转高电平）替换成“0”，在转化成字符串就行了
代码如下：

```
from Crypto.Util.number import *

msg = 0x2559659965656a9a65656996696965a6695669a9695a699569666a5a6a6569666a59695a69aa696569666aa6
s = bin(msg)[2:]
r = ""
for i in range(len(s)//2):
    if s[i*2:i*2+2] == '10':
        r += '1'
    else:
        r += '0'
print(long_to_bytes(int(r, 2)))
```

结果为：BJD{DifManchestercode}

crypto-classic1

附件里面还有一个加密了的附件，给了一个附件密码的 hint：

哇，这里有压缩包的密码哦，于是我低下了头，看向了我的双手，试图从中找到某些规律

xdfv ujko98 edft54 xdfv pok,.; wsdr43

这是什么玩意？

低头看双手，键盘加密？

原来是键盘上对应字符包裹起来的字符

密码为：circle

加密附件文件名是 vigenere，所以是维吉尼亚密码，给了一个密文：SRLU{LZPL_S_UASHKXUPD_NXYTFTJT}

还需要密钥

由于题目来源于[ACTF新生赛2020]，推测 flag 格式为 actf{}

对应维吉尼亚表格：

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

前四位对应的密钥是：spsp

猜想密钥是 sp

解密结果为：

SRLU{LZPL_S_UASHKXUPD_NXYTFTJT}

密钥 sp 加密 解密

ACTF{TKXW_A_FIDPVFFXO_VIGENERE}

但是提交 flag 怎么都不对

只能找 wp

可以看到最后几个字符已经能成功解密为vigenere，所以秘钥没什么问题。但是中间的字符仍然没有意义。（S也正好对应为a，所以我感觉解密没问题）

提交flag不对，试了一下另外两个单独用古典密码凯撒栅栏rot13等解密，都没有结果。最后百度了一下

坑爹！

BUUCTF给的字符串是错的！！

```
#这才是原题！！！秘钥为sp，自己解密去吧。
SRLU{OWSI_S_RDPKHARSA_NXYTFTJT}
```


啊这。。。

正确的 flag 为：ACTF{WHAT_A_CLASSICAL_VIGENERE}

结语

希望继续坚持