FDUCTF 2024 writeup -xxuurruuii

Misc

二维码的瘦身

裁剪把定位符删掉了，但是懒得研究二维码版本啥的，自己造了个二维码拼上去

```
flag='fductf{helloctfhelloctfhelloctfhelloctfhelloctfhelloctfhelloctfhelloctfhelloctfhelloctfhelloctfhe
lloctf}'
img = np.array(qr.make_image(), dtype=np.float64)#[16:, 16:]
```

然后把左边和上面的部分裁下来拼到原二维码上

FDUKindergarten

```
__import__('os').system('cat flag')
```

FDUJail

```
eval(input(id(float())))
```

什么是Cimbar码

搜索Cimbar，找到一个安卓用的解码器，遂拿出我打明日方舟用的安卓模拟器（没有安卓手机）装了一个，扫出来一个0.368758文件

识别出来是png文件，打开有一张图，中间是神秘Lynchpin文本，上下有一串/\，看起来就很像答案，于是丢进焖肉面分析一下发现是摩斯密码，剩几个焖肉面处理不了的特殊字符手动处理一下

只有两个字符，开始二值分析

尝试莫斯

/为点，\为长：fductf*lynchpin*haven*t*be*s01ved*yet*please*stand*by*h3r*side*
\为点，/为长：qwg*eq*yla**xma**n*ta*e*jt*o56*tw*lte*x6tnot*oenaw*jl**8k*omwt*

笑话：有猪以为前缀是flag，疑惑了半天\为什么是{

~~题外话：出题人怎么有舟p啊~~

Crypto

Alice与Bob的小纸条

丢进quipqiup秒了

Jeff Dean笑话

自己手搓的找因数找半天找不到以为是常规rsa导致卡了半天。感觉自己是个笑话

```
from sympy import *
factorint(752606814710216145502824909811095325400647681895199630037888534496281482384910945833079966321514084125672153129770372232201877370150886715790534267020466234594125815024465235220853464303891503108117369336632008636229 1)
{8193423899118349: 1, 9185498321296426312173572093061567893427873612682060939417964833837894845427087985972950109669346639041500641341724709881025522090515139117320439092620522893470769665902178095386675605831270153783753591: 1}
```

eazy_sage

看了半天代码发现password套了个凯撒就摆上来了，其他啥用没有，遂爆

感觉神金题，puzzlehunt都限制20次提交怎么你要26次

```
fductf{ym1x1xhwd9y0}
fductf{zn1y1yixe9z0}
fductf{ao1z1zjyf9a0}
fductf{bp1a1akzg9b0}
fductf{cq1b1blah9c0}
fductf{dr1c1cmbi9d0}
fductf{es1d1dncj9e0}
fductf{ft1e1eodk9f0}
fductf{gu1f1fpel9g0}
fductf{hv1g1gqfm9h0}
fductf{iw1h1hrgn9i0}
fductf{jx1i1isho9j0}
fductf{ky1j1jtip9k0}
fductf{lz1k1kujq9l0}
fductf{ma1l1lvkr9m0}
fductf{nb1m1mwls9n0}
fductf{oc1n1nxmt9o0}
fductf{pd1o1oynu9p0}
fductf{qe1p1pzov9q0}
fductf{rf1q1qapw9r0}
fductf{sg1r1rbqx9s0}
fductf{th1s1scry9t0}
fductf{ui1t1tdsz9u0}
fductf{vj1u1ueta9v0}
fductf{wk1v1vfub9w0}
fductf{xl1w1wgvc9x0}
```

看图算数II

参考文献：https://www.bilibili.com/video/BV1gR4y1i7ZF

计算过程在控制台和草稿纸上所以丢了，总之算出来椭圆曲线是y$^{2=-11440*x}$3/3+3988*x^2/9-116*x/9+1/9

代的初值是(a,b,c)=(6,1,0)，(x,y)=(1/49,5/343)

贴一份我已经看不懂了的代码

```
x1=[Rational(1,49)]
y1=[Rational(5,7**3)]
while True:
    k=(y1[0]-y1[-1])/(x1[0]-x1[-1])
    if len(x1)==1:k=Rational(1558,105)
    t=y1[0]-k*x1[0]
    x1.append(((Rational(3988,9)-k**2)*9/34320-x1[0]-x1[-1]).simplify())
    if f1.subs({x:x1[-1]})<0:continue
    y1.append(-k*x1[-1]-t)
    a1=(x1[-1]+y1[-1])/2
    b1=(x1[-1]-y1[-1])/2
    c1=(49*x1[-1]-1)/6
    if (a1>0 and b1>0 and c1>0) or (a1<0 and b1<0 and c1<0):break
```

迭代了28次才出，运气一般

解：

37486359199196619338400127185681241149820571252744532805519511658329907966259558795
56597930265916667338103966335474834242581597270129832657306459827133974708821122153
43816163594873306917846324822415176684896898759758688129013535172113802844352729893
20601681275920690746634038144825788639038583165095548082638544159010352180253277471
26262127081397388668974828649810016437821108431371281211861828110920022757455622170
85663270262194755353857612910135638933989170870337202492518817028517512805469732135
59605760188379989461626070935885956228763413950130548040232885684458154312081217034
79189806056881247721832118382020881491060379461131878370922487681986547823980240907
85388111599123059956035454271039000959933276197366557529208945524004431024339837397
08048247992617184580313451565253290234086125247379523406683583872730605016522098169
61504603231674084136684592524782325721802771876345670870359629376053215460037544252
87111209353770118208030673485400569382049403758871289903497967466414206709594 9

53014679071038993163635650158542451737280263437279248458095865439637721633237379254
86049039297595764510884543432773086265055247723471990690058598323116833981191209356
23913157647107292336126417403586083587465081882481418495626383125045324324689547265
58825704561359099309441290528572004411731351853309089124432820075375670331843116948
94644252331293727351641757791848134154800186956022119912311973441087381719414443681
54332370396844651138116335563855669543068599032901211080728538753097876492620577125
69338898488617376217559817899629723089761387757344197372372583435754551661274550142
30702251521555727263121272498717849537122909531013297103138120594729227286192537200
94125822652967233274330062790139070641323605583957101168580516899957639187649068070
56334645401162023893130143709541075674686261457572580284930764597598128919582737636
52405488134014202988256415305292144136714364893610329954876868191905522275266918497
67908418258187366913852000316762552048346693548156428482145863510818746748184 4

54415992747931198147887422316210704086968211460461645197096965358947535227110545710
89129586119494112091697385594996798709125350246844830671165112552778060222090144334
05146320741081777571647202983052126247023925294704677585323814449164644841586396990
72157564312811748097229412716415361547361029528400678193033058598818499323384842344
90378899330597690845936116405677957713843325181290610649839567872478940874551296848
16830020935671468709939110878219530052036137143008835420690538739521555505751963954
28088756372413546627957260262414143205021725009720979628745277653545586904873050324
95949627195483313330073430624676224692300874242097645642115237425167282073756186313
74564940786939004714760540563845238647986801504401484597999571631886556141424100895
31831914152271709237665564007539789670333339435698638876312220535039498746787658336
10197729431886227140037822283322041902532723309925998799295017022970958489476753540
45147235704089168036456651549768619077946056556637828297942906134610023154522 50

Pwn

丫丫历险记

往数组的0-8和15试了一遍然后看到程序里有个-1特判就试了-1然后就过了。暂时不知道为什么

Reverse

baby64

其实我完全没找到关键在哪，但是fductf过一遍base64得到的ZmR1Y3Rm长得和程序里的YnQ0Z2Qn看起来差一个异或1，然后就手动搓了个BADCFE...zy1032547698/+跑base64

解出来是

```
fductf{M4in_1s_n0t_the_fir3t_0ne}
```

怎么回事呢，我完全没找到处理这串key的地方（

Web

草率的毕业设计

观察代码发现salt4位，每次使用的password只有一位，取secret的第一项直接爆破

```
for i1 in s:
    for i2 in s:
        for i3 in s:
            for i4 in s:
                for i5 in s:
                    if sha512(i1+i2+i3+i4+i5)==secret:
                        print(i1+i2+i3+i4+i5)
#f95qW
```

于是得到了salt="95qW"，然后就是逐位爆破password了

```
for i in secret:
    for x in s+'{}_':
        if sha512(x+salt)==i:print(end=x)
#fductf{salt_is_too_short_40Ecc8BC06e0Fb8f}
```

所以这题为什么放在Web分类里，建议滚去Crypto（