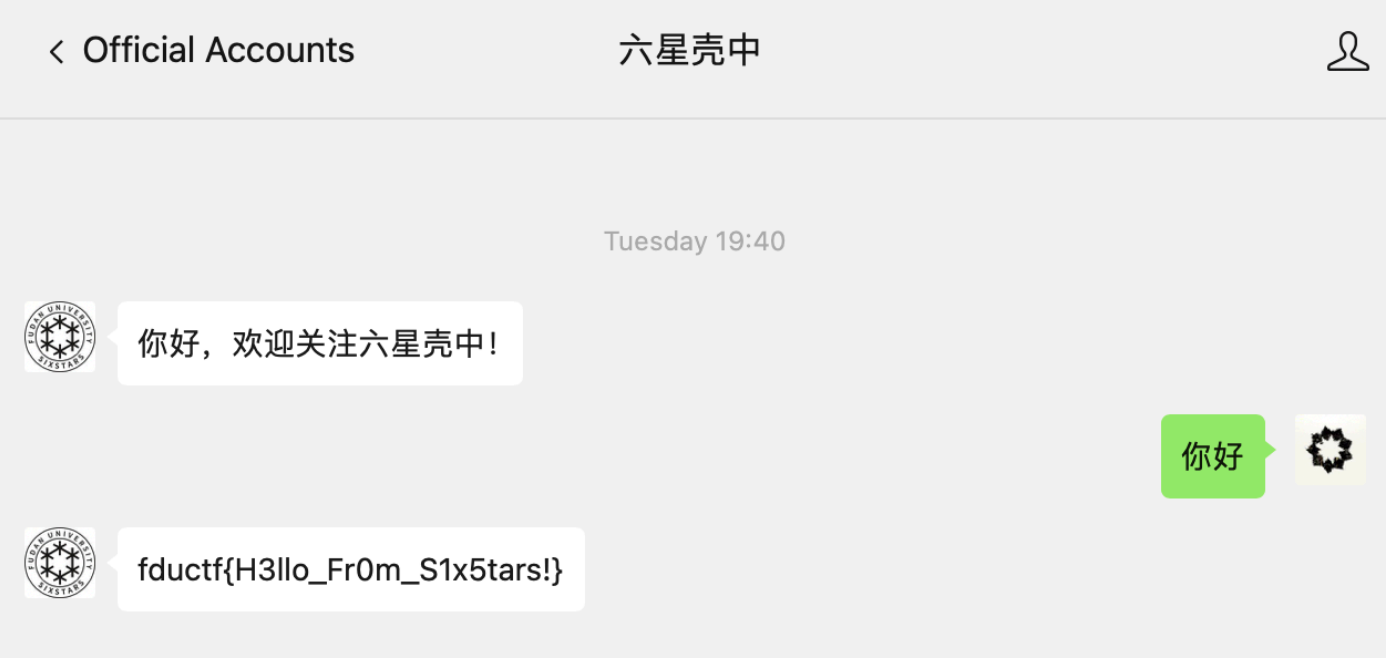


# FDUCTF 2024 Writeup

By 8u-nekoyellow

## 签到

签到。



## Alice与Bob的小纸条

使用词频分析 (<http://quipqiup.com>) 。

Not Secure — quipqiup.com

automatically selected statistics mode; you can override by using the drop down menu next to the solve button.

```
0 -1.446 Father of suspect in Georgia school shooting arrested The father of a 14yearold boy accused of killing four people at a high school in the US state of Georgia has been arrested. Colin Gray, 54, is facing four charges of involuntary manslaughter, two counts of seconddegree murder and eight of cruelty to children, said the Georgia Bureau of Investigation GBI. GBI Director Chris Hosey said on Thursday evening the charges were directly connected to his sons actions and allowing him to possess a weapon. The son, Colt Gray, is accused of killing two teachers and two students in Wednesdays shooting at Apalachee High School in Winder, near Atlanta. He is due in court on Friday charged as an adult with four counts of murder. Authorities are investigating whether Colin Gray bought the ARstyle weapon as a gift for his son in December 2023, law enforcement sources told CBS News, the BBCs US partner. In May 2023, the FBI alerted local police to online threats about a school shooting, associated with an email address linked to the suspect. A sheriffs deputy went to interview the boy, who was 13 at the time. His father told police he had guns in the house, but his son did not have unsupervised access to them, the FBI said in a statement on Wednesday. Officials say the threats were made on Discord, a social media platform popular with video gamers, and contained images of guns. The accounts profile name was in Russian and translated to the surname of the attacker who killed 26 people at Sandy Hook Elementary School in Connecticut in 2012. A police incident report describing last years interview with the boy and his father was released on Thursday. In the report, a deputy described the boy as reserved and calm and said he assured me he never made any threats to shoot up any school. They said he claimed to have deleted his Discord account because it was repeatedly hacked. Colin Gray also told police his son was getting picked on at school and had been struggling with his parents separation. Police records reveal that the boys mother and father were in the process of divorcing, and he was staying with his father during the split. The teen often hunted with his father, who told police he had photographed his son with a deers blood on his cheeks. The boys maternal grandfather told the New York Times he partly blames the tumultuous home life after Mr Grays split from his daughter. "I understand my grandson did a horrendous thing theres no question about it, and hes going to pay the price for it, Charlie Polhamus told the newspaper. My grandson did what he did because of the environment that he lived in, he added. During the news conference on Thursday, Barrow County Sheriff Jud Smith said all nine of those injured were expected to make a full recovery. Several victims had already left hospital, he said. The flag begins with fductf. Then comes the left brace. Contents inside two braces are WrodFerqeuncy, which indicates you should analyze word frequency to solve this problem. And dont forget the right brace. That is, fductf, left brace, WrodFerqeuncy, and right brace. Students Mason Schermerhorn and Christian Angulo, both 14, and teachers Richard Aspinwall, 39, and Christina Irimie, 53, died in the attack. Witnesses said the suspect left an algebra lesson on Wednesday morning only to return later and try to reenter the classroom. Some students went to open the locked door, but apparently saw the weapon and backed away. Witnesses said they then heard a barrage of 1015 gunshots. Two school police officers quickly challenged the boy and he immediately surrendered. These are not the first charges against the parents of a suspect in a school shooting. In April. the parents of a Michigan teenager who killed four students with a gun they bought for him
```

Thanks for using quipqiup.com! The code and website are (C) 2014-2020 by Edwin Olson, [ebolson@umich.edu](mailto:ebolson@umich.edu). Quotes were compiled by James F Thompson.

# Jeff Dean

进行RSA解密。已知public key  $e, n$ ，需要推出private exponent  $d = e^{-1} \mod \phi(n)$ ，即 $e$ 在模 $\phi(n)$ 意义下的逆元。

$\phi(n)$ 是欧拉函数，表示的是小于等于  $n$  和  $n$  互质的数。如果已知 $n$ 的质因数分解 $n = \prod_i p_i^{k_i}$ ，可以用公式  $\phi(n) = n \times \prod_i \frac{p_i - 1}{p_i}$  计算得到。

对 $n$ 分解质因数：

```
from sympy import factorint
print(factorint(n))
```

得到

```
# n = p * q
p = 8193423899118349
q =
918549832129642631217357209306156789342787361268206093941796483383789484542708798597295010
966934663904150064134172470988102552209051513911732043909262052289347076966590217809538667
560583127015378375359
```

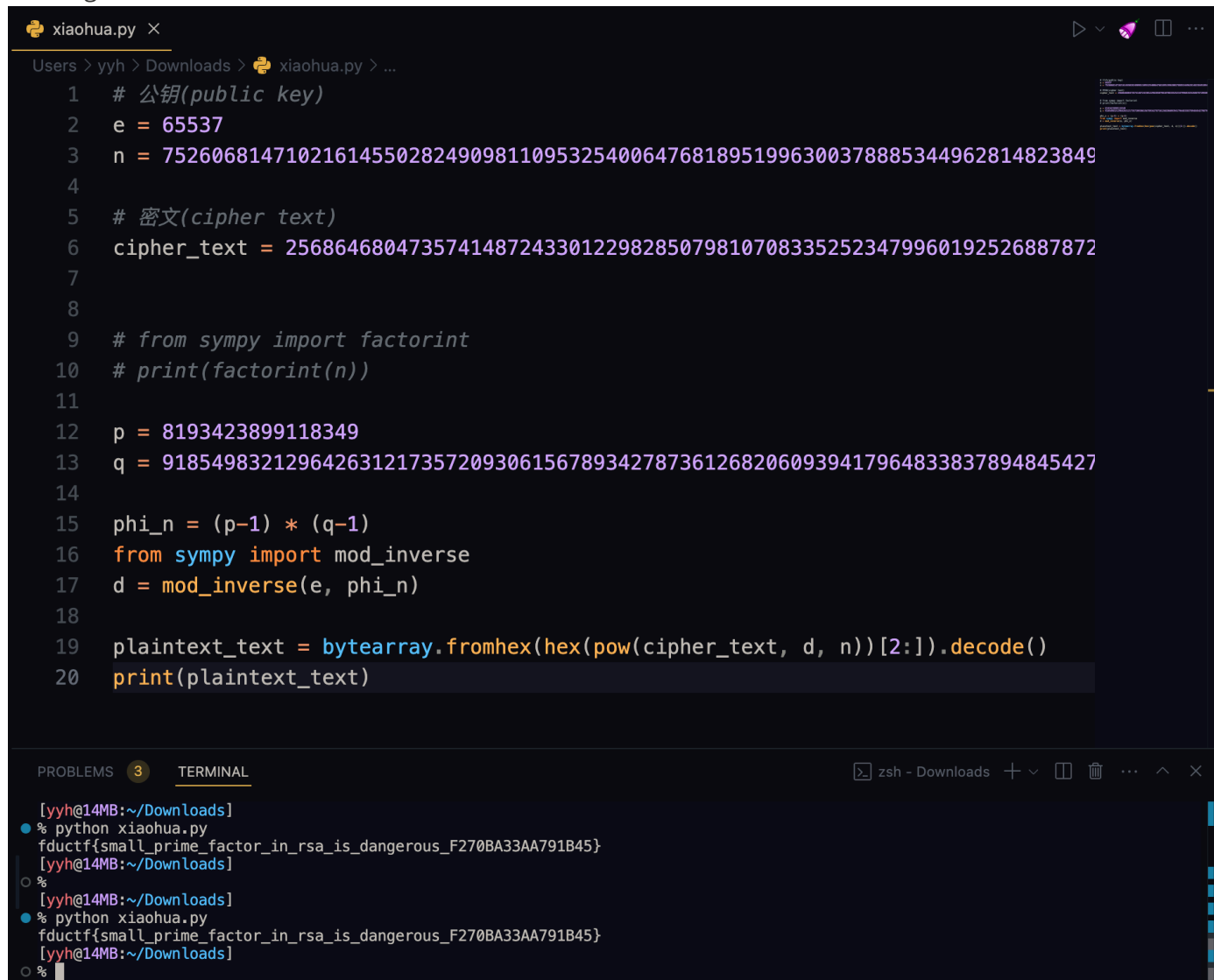
因此

```
phi_n = (p-1) * (q-1)
from sympy import mod_inverse
d = mod_inverse(e, phi_n)
```

最后用 $c^d \bmod n$ 解密

```
plaintext_text = bytearray.fromhex(hex(pow(cipher_text, d, n))[2:]).decode()
print(plaintext_text)
```

得到flag:



```
xiaohua.py x
Users > yyh > Downloads > xiaohua.py > ...
1  # 公钥(public key)
2  e = 65537
3  n = 7526068147102161455028249098110953254006476818951996300378885344962814823849
4
5  # 密文(cipher text)
6  cipher_text = 256864680473574148724330122982850798107083352523479960192526887872
7
8
9  # from sympy import factorint
10 # print(factorint(n))
11
12 p = 8193423899118349
13 q = 9185498321296426312173572093061567893427873612682060939417964833837894845427
14
15 phi_n = (p-1) * (q-1)
16 from sympy import mod_inverse
17 d = mod_inverse(e, phi_n)
18
19 plaintext_text = bytearray.fromhex(hex(pow(cipher_text, d, n))[2:]).decode()
20 print(plaintext_text)
```

PROBLEMS 3 TERMINAL

```
[yyh@14MB:~/Downloads]
% python xiaohua.py
fductf{small_prime_factor_in_rsa_is_dangerous_F270BA33AA791B45}
[yyh@14MB:~/Downloads]
%
[yyh@14MB:~/Downloads]
% python xiaohua.py
fductf{small_prime_factor_in_rsa_is_dangerous_F270BA33AA791B45}
[yyh@14MB:~/Downloads]
%
% 
```

## 草率的毕业设计

任务是从源码破解用户名和密码。分析 `main.py` 可以直接知道用户名为admin

(`base64.b64decode("YWRtaW4=").decode('utf-8')`)，主要是找密码。分析知道密码会被逐位concat一个4位的salt哈希后与secret数组比较。使用的哈希算法SHA512目前无法破解（无逆运算、冲突概率极小），所以只能考虑暴力。

由于salt长度很短，枚举空间不大 ( $\sim 100^4$ )，首先用如下代码穷举找salt：

```
from functools import reduce
```

```

from itertools import product

for s in product(string.digits + string.ascii_letters, repeat=4):
    s = reduce(lambda x, y: x + y, s)
    ok = True
    for i in range(2): # 看前两位 (之前代码写成第一位匹配就过了, 不过也得到了正确答案)
        flag = False
        for c in string.ascii_letters + string.digits + "_{}":
            flag |= (sha512(c + s) == secret[i])
        ok &= flag
    if ok:
        salt = s
        break

```

得到 salt = 95qW。

接下来只要逐位找匹配的字符即可找到密码：

```

for i in range(n):
    flag = False
    for c in string.ascii_letters + string.digits + "_{}":
        if sha512(c + salt) == secret[i]:
            ans += c
            flag = True
            break
    assert flag

```

得到flag：

```

73 # salt = s
74 # break
75
76 salt = '95qW'
77 ans = ''
78
79 for i in range(n):
80     flag = False
81     for c in string.ascii_letters + string.digits + "_{}":
82         if sha512(c + salt) == secret[i]:
83             ans += c
84             flag = True
85             break
86     assert flag
87
88 print(ans)

```

```

% python solve.py
130
admin
[yyh@14MB:~/Downloads/web1]
% python solve.py
admin
[yyh@14MB:~/Downloads/web1]
% python solve.py
admin
[yyh@14MB:~/Downloads/web1]
% python solve.py
admin
fductf{salt_is_too_short_40Ecc8BC06e0Fb8f}
[yyh@14MB:~/Downloads/web1]
%

```