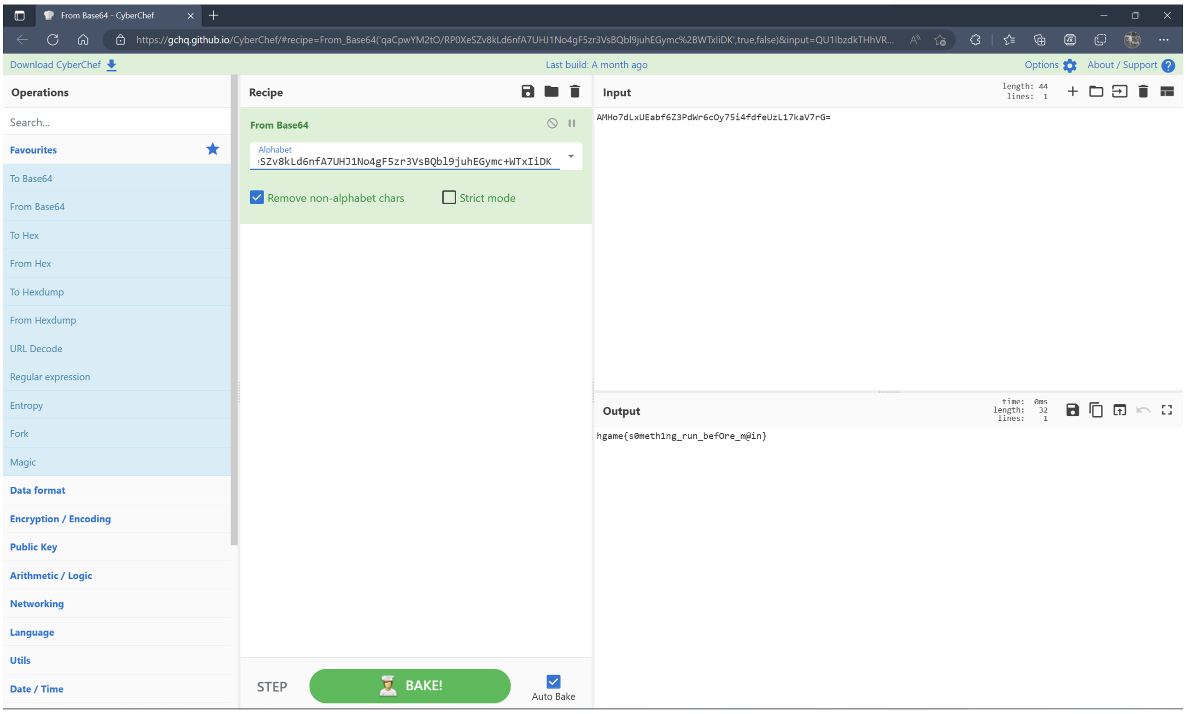
hgame Week2

Reverse

before main

base64换表藏了一个函数把表又换了一下



https://gchq.github.io/CyberChef/#recipe=From_Base64('qaCpwYM2tO/RP0XeSZv8kLd6nfA7UHJ1No4gF5zr3VsBQbl9juhEGymc%2BWTxIiDK',true,false)&input=QU1IbzdkTHhVR...

Recipe

From Base64

Alphabet

:SZv8kLd6nfA7UHJ1No4gF5zr3VsBQbl9juhEGymc+WTxIiDK

☑ Remove non-alphabet chars ☐ Strict mode

Input

length: 44
lines: 1

```
AMHo7dLxUEabf6Z3PdWr6cOy75i4fdfeUzL17kaV7rG=
```

Output

time: 0ms
length: 32
lines: 1

```
hgame{s0meth1ng_run_befOre_m@in}
```

hgame{s0meth1ng_run_befOre_m@in}

stream

首先一系列操作搞出python源码，之后明显有一个base64

这题可以直接修改源码得到flag的

```python
import base64

def gen(key):
    s = list(range(256))
    j = 0
    for i in range(256):
        j = (j + s[i] + ord(key[i % len(key)])) % 256
        tmp = s[i]
        s[i] = s[j]
        s[j] = tmp
    i = j = 0
    data = []
    for _ in range(50):
        i = (i + 1) % 256
        j = (j + s[i]) % 256
        tmp = s[i]
        s[i] = s[j]
        s[j] = tmp
        data.append(s[(s[i] + s[j]) % 256])
    return data


def dncrypt(key):
    box=gen(key)
    for i in range(len(xbox)):
        print(chr(xbox[i]^box[i]),end='')

text = input('Flag: ')
xbox=
[189,149,87,18,249,152,220,29,160,105,237,50,75,207,22,122,106,150,201,132,188,3
4,187,40,206,106,235,118,6,215,29,233,170,189,33,253,53,47,46,123,237,181,229,]
key = 'As_we_do_as_you_know'
dncrypt(key)
# if enc ==
'wr3ClVcSw7nCmMOcHcKgacOtMkvDjxZ6asKWw4nChMK8IsK7KMOOasOrdgbDlx3DqcKqwr0hw701Ly5
7w63CtcOl':
#     print('yes!')
enc =
'wr3ClVcSw7nCmMOcHcKgacOtMkvDjxZ6asKWw4nChMK8IsK7KMOOasOrdgbDlx3DqcKqwr0hw701Ly5
7w63CtcOl'
enc=base64.b64decode(enc.encode()).decode()
for i in xbox:
    print(ord(i),end=',')
```

math

没法逆向

只能正面z3爆破

看起来像线代

```
from z3 import *
v8=[0]*25
v11=[0]*25
v10=[0]*25
v8[0]=126
v8[1]=225
v8[2]=62
v8[3]=40
v8[4]=216
v8[5]=253
v8[6]=20
v8[7]=124
v8[8]=232
v8[9]=122
v8[10]=62
v8[11]=23
v8[12]=100
v8[13]=161
v8[14]=36
v8[15]=118
v8[16]=21
```

```
v8[17]=184
v8[18]=26
v8[19]=142
v8[20]=59
v8[21]=31
v8[22]=186
v8[23]=82
v8[24]=79
v10[0]=63998
v10[1]=33111
v10[2]=67762
v10[3]=54789
v10[4]=61979
v10[5]=69619
v10[6]=37190
v10[7]=70162
v10[8]=53110
v10[9]=68678
v10[10]=63339
v10[11]=30687
v10[12]=66494
v10[13]=50936
v10[14]=60810
v10[15]=48784
v10[16]=30188
v10[17]=60104
v10[18]=44599
v10[19]=52265
v10[20]=43048
v10[21]=23660
v10[22]=43850
v10[23]=33646
v10[24]=44270
s=Solver()
flag=[Int('flag%s' % i) for i in range(25)]
for i in range(5):
    for j in range(5):
        for k in range(5):
            v11[5*i+j]+=flag[5*i+k]*v8[5*k+j]
# s.add(flag[0] == ord('h'))
# s.add(flag[1] == ord('g'))
# s.add(flag[2] == ord('a'))
# s.add(flag[3] == ord('m'))
# s.add(flag[4] == ord('e'))
# s.add(flag[5] == ord('{'))
# s.add(flag[24] == ord('}'))
for i in range(25):
    s.add(v11[i]==v10[i])
s.check()
s.model()
print(s.model())
```

```
flag=[0]*25
flag[1]=103
flag[3]=109
```

```
flag[4]=101
flag[6]=121
flag[17]=115
flag[18]=95
flag[10]=95
flag[8]=117
flag[23]=125
flag[16]=49
flag[21]=48
flag[12]=64
flag[24]=0
flag[15]=95
flag[22]=100
flag[14]=104
flag[0]=104
flag[19]=103
flag[9]=114
flag[2]=97
flag[7]=48
flag[13]=116
flag[20]=79
flag[11]=109
flag[5]=123
for i in flag:
    print(chr(i),end='')
```

hgame{y0ur_m@th_1s_gO0d}

vidar camera

这道题我只能用诡异来形容

魔改xtea，加密轮数也改了，是33让我抓狂了好久

```
#include <stdio.h>
#include <stdint.h>
void decipher(unsigned int num_rounds, uint32_t v[2], uint32_t const key[4]) {
  unsigned int i;
  uint32_t v0 = v[0], v1 = v[1], delta = 878077251, sum = delta * num_rounds;
  for (i = 0; i < num_rounds; i++) {
    sum -= delta;
    v1 -= (((v0 << 4) ^ (v0 >> 5)) + v0) ^ (sum + key[(sum >> 11) & 3]);
    v0 -= sum^(((v1 << 4) ^ (v1 >> 5)) + v1) ^ (sum + key[sum & 3]);
    }
  v[0] = v0; v[1] = v1;
}
int main()
{
  int enc[10] = { 637666042, 457511012, -2038734351, 578827205, -245529892,
-1652281167, 435335655, 733644188, 705177885, -596608744 };
  int v[10];
    uint32_t const k[4] = { 2233,4455,6677,8899 };
  unsigned int r = 33;
  for (int i = 8; i>=0; i--) {
        decipher(r, &enc[i], k);
    }
    printf("%s\n", v);
    return 0;
}
```