CRYPTO

密码学教室入门（一）

题目描述： 这是最著名的一种非对称加密密码体制

学习文档：https://en.wikipedia.org/wiki/RSA_(cryptosystem)

p:
0x9a724c6747de9eadccd33f4d60ada91754b8be8c65590cafe66f69a2f4afbfd359e47ca6fd2dbde8948062dc116bc574f4313ab99b2bb6d8ae47beaa0c1ebeddL

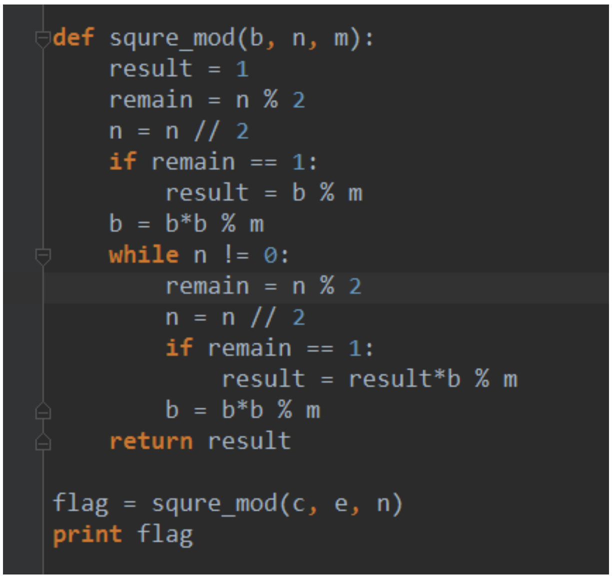
q:
0x8c1c81cc005ce3dd6d684ebb88151dc0c53b1cef8a29b1cb8121860fb57d93117bf449aac4300dc6103ac6211c6f8ae68987d99aff0dd8967a4afa00f2116873L

e:
0x190a000845e9c8c2059242835432326369aaf8c7ca85e685bba968b386155a91f1f7ca1019ff23d119222e1f0dfdeb0915d2e97601ef94bf15ca6d9211e984e9038f263f4984355c397ed22d67c26da6d31acfc4d599c70cba80859bee099e5a2dc3ab23aecf58f73f44d07318f70985c623d9612efefb15bf8dab77d5d54e85L

d: 0x28b95b7e3159a851cbf537e007ae49864b7dbb93fc370a5L

c:
0x23091e42fa7609c73f1941b320fad6d2ff6e47be588d1623f970f1fee7abd221c9834b208f3c888902fe87ca76ec1e1363757d93c6e25c49f1c61c72b141c0b8848b54a117427d8e30eeab89694eb5f849cafecb0e5361b9b2b0e3f89e0fdbcc66a6aad4a1a4a85d828083a01a5d569b7eeb6f91517944533 82b524aa52993f9L

利用模重复平方计算法



```
def squre_mod(b, n, m):
    result = 1
    remain = n % 2
    n = n // 2
    if remain == 1:
        result = b % m
    b = b*b % m
    while n != 0:
        remain = n % 2
        n = n // 2
        if remain == 1:
            result = result*b % m
        b = b*b % m
    return result

flag = squre_mod(c, e, n)
print flag
```

Flag：0x6867616d657b7273615f31735f737469316c5f653473795f6e6f77217dL

再按字符串读

Flag :hgame{rsa_1s_v3ry_e4sy!}

密码学教室入门（四）

n:
0x81cfc71c44c83faf3c5242fa81ae2e533fc945f3bef30bc13323ea4a55b3debc11301c6a9ecb8f7ef92fa169b157435af728a145497f2cdf75b3007b9732da4c47d67683f09ae1edc8f698f5ec7549593d9f1d06adafae4ad09514928bf0367a2719f7c171580318690dafc6a3d5385b3516b769f529c0a055ce25e68bc21395L
e: 0x01
c: 0x6867616d657b7273615f31735f737469316c5f653473795f6e6f77217dL

e = 1，所以 c = m;

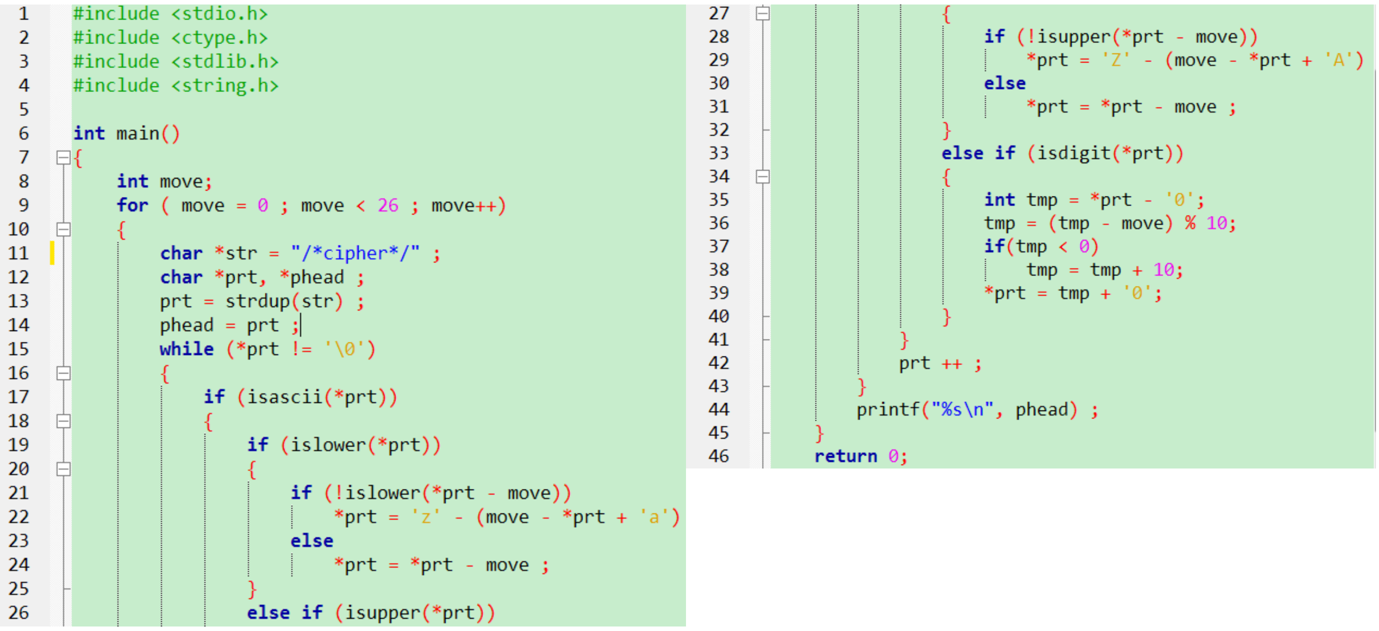
按字符串读 c

Flag :hgame{rsa_1s_sti1l_e4sy_now!}

密码学教室入门（二）

题目描述： 凯撒加密是一种古老的对称加密算法
mlfrj{Hfjxfw_hnumjw_8x_ozxy_ktw_kzs}

移位就好了,字母是 Z_{26} 数字是 Z_{10}



```c
#include <stdio.h>
#include <ctype.h>
#include <stdlib.h>
#include <string.h>

int main()
{
    int move;
    for ( move = 0 ; move < 26 ; move++)
    {
        char *str = "/*cipher*/" ;
        char *prt, *phead ;
        prt = strdup(str) ;
        phead = prt ;
        while (*prt != '\0')
        {
            if (isascii(*prt))
            {
                if (islower(*prt))
                {
                    if (!islower(*prt - move))
                        *prt = 'z' - (move - *prt + 'a')
                    else
                        *prt = *prt - move ;
                }
                else if (isupper(*prt))
                {
                    if (!isupper(*prt - move))
                        *prt = 'Z' - (move - *prt + 'A')
                    else
                        *prt = *prt - move ;
                }
                else if (isdigit(*prt))
                {
                    int tmp = *prt - '0';
                    tmp = (tmp - move) % 10;
                    if(tmp < 0)
                        tmp = tmp + 10;
                    *prt = tmp + '0';
                }
            }
            prt ++ ;
        }
        printf("%s\n", phead) ;
    }
    return 0;
```

Flag：hgame{Caesar_cipher_1s_just_for_fun}

密码学教室番外篇

题目描述： 昨天看大家凯撒密码疯狂试 flag，所以
yxrdv{uxwupytip19954902180//+/%}

同上

Flag：hgame{dgfdyhcry42287235413//+/%}

WEB

我是谁我在哪？？？

题目描述：**http://115.28.78.16:13333/web/web2/index.php**

在 index.php 的响应头里面

flag: `hctf{1t_iz_4_4mall_tr1ck}`

MISC

Explorer 的图库之一

题目描述： LoRexxar:z 神，我想打 CTF
Explorer 扭头从图库里掏出了一张图
http://115.28.78.16:13333/misc/d18d4b213fd71448f8c6f9780cb145a4
看看你能找到几个 flag???

Winhex 打开开头

Flag：hctf{2e3e3}