

实验吧密码学WriteUp 一)

原创

再于杨超越 于 2018-11-13 17:54:12 发布 138 收藏

版权声明：本文为博主原创文章，遵循 [CC 4.0 BY-SA](#) 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_43679627/article/details/84033057

版权

分享一下我老师大神的人工智能教程！零基础，通俗易懂！<http://blog.csdn.net/jiangjunshow>

也欢迎大家转载本篇文章。分享知识，造福人民，实现我们中华民族伟大复兴！

这个系列的文章会将简单的题目放在一起介绍，稍难的题目会单独拿出来写，现在开始。

1.js(题目连接：<http://www.shiyanbar.com/ctf/1779>)

打开网页查看源码，复制源码至Chrome的console,将代码中的eval改为console.log，回车后显示

```
> console.log(function(p,a,c,k,e,d){e=function(c){return c?a?":e(parseInt(c/a)))+(c<=9a)>39?String.fromCharCode(c+29):c.toString(36)};if(!''.replace(/\s/,String)){while(c-->0){e(c)=k[c]||e(c);k={function(e){return d[e]};e=function(){return"\u06";c=1};while(c-->0){if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('c1 8=7/a">9(\\'0\\'3\\'2\\'5\\'4\\'1\\'b\\'i\\'h\\'k\\'j\\'0\\'g\\'d\\'c\\'f\\'0\\'e\\'</i>";21,21,"u0053|script|u006d|u0069|u0054|u0043|u0053|text|type|alert|;|javascript|u0046|u006f|u0063|u007d|u0064|u006e|u006a|u007b|u005f|u0073".split('|'),0,{}))</script type="text/javascript">alert('u0053|u0069|u006d|u0043|u0054|u0046|u007b|u006a|u0073|u005f|u0065|u006e|u0063|u006f|u0064|u0065|u007d');</script>
```

一看就知道是unicode编码，找网站在线解码即可

内容源文本框: Ascii字符补齐4位

```
\u0053\u0069\u006d\u0043\u0054\u0046\u007b\u006a\u0073\u005f\u0065\u006e\u0063\u006f\u0064\u0065\u007d
```

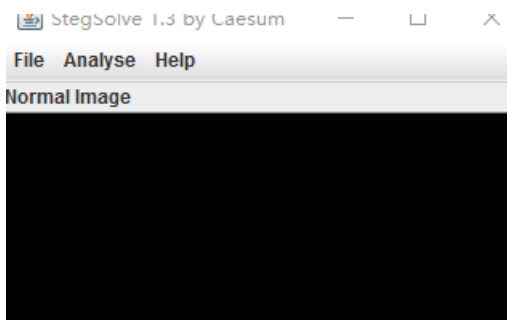
转Unicode编码(\uXXXX) 转换为(&#DDDDDD) 转换为&#XXXX 转换为汉字

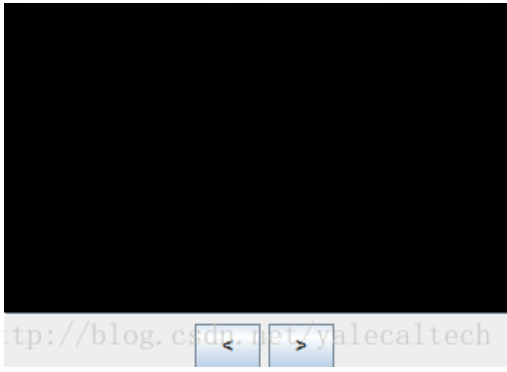
转换结果：

```
SimCTF{js_encode}
```

2.NSCTF crypto200(连接：<http://www.shiyanbar.com/ctf/1768>)

保存图片至本地，使用stegsolve打开





变换后得到



很像二维码是吧？不过这个二维码的黑白颜色完全相反，是扫不出来的，可以使用光影魔术手或者其他软件的反色功能，得到如下二维码，然后扫描即可得到flag



3.NSCTF crypto50 (链接: <http://www.shiyanbar.com/ctf/1758>)

题目做多了就有感觉了一看就知道是AES加密, 故在线AES解密得

高级加密标准AES在线工具 IDgui.com/AES

简约手机访问省流量, 常见到以“U2FsdGVkX1”的加密串, 这是有些信息只希望有密钥的人才能解密看到, 对原文进行了高级AES加密, 国家政府和银行常用, 有了下面的工具我们也可以用。使用步骤: 【1】写入原文和密钥解密。提示可交换后多次加密更安全。

◆待加密原文◆ [币域名 BTCym.com](#) [涂鸦 8doge.com](#)

f1ag{DISJV_Hej_UdShofjyed}

◆输入密钥: 【↑】

◆AES加密密文◆ [\[缩写为短字符串\]](#) [\[搜索原文\]](#)

U2FsdGVkX1+qtU8KKGmJwGgKcPUK3XBTdM+KhNRLHSCQL2nSXaW8++yBUkSy1Rp

<http://blog.csdn.net/yalecaltech>

直接提交, 答案错误

仔细观察, 感觉可能用了凯撒移位

前5个字母按照flag的规律应是NSCTF, 由此得到移位数

手工破解即可flag{NSCTF_Rot_EnCrypton}

4.黑客叔叔（雨袭团）内部交流题（第一季1.0.2）（题目链接：<http://www.shiyanbar.com/ctf/1744>）

先将字符放在同一行，因为编码里很少会出现汉字，故尝试将“等等”变化为“==”，汉字变化为“/”

使用TripleDes解密



接着Rabbit解密



（我也不知道为什么是这两个算法，多尝试几次看答案像的就是了，常见加密算法有AES DES RC4 Rabbit TripleDes 等等）

5.simple algorithm(题目链接：<http://www.shiyanbar.com/ctf/737>)

题目给了一个py脚本和一个密文文件，阅读源码可知：py脚本将明文转换为密文，现在需要将密文文件中的密文解密得到明文。很明显加密流程为将明文转换为16进制编码，在转化为10进制数，将每两位数字构成的数进行FAN函数运算，再拼接起来得到密文。

因此解密流程为：将0~99利用FAN函数求得加密值，建立加密值到原数的字典，在明文中查字典拼接得到10进制数，转化为16进制数，再求取字符串。

按照要求用python脚本跑即可

-- coding: utf8 --

原代码中的FAN()

```
def FAN(n, m):
    i = 0
    z = []
    s = 0
    while n > 0:
        if n % 2 != 0:
            z.append(2 - (n % 4))
        else:
            z.append(0)
        n = (n - z[i])/2
        i = i + 1
    z = z[::-1]
    l = len(z)
    for i in range(0, l):
        s += z[i] * m ** (l - 1 - i)
    return s
```

```
def foo():
    #读取密文
    s=open("enc.txt").read().strip()
```

```
#构造0~99对应的FAN()的值的字典dct={}for n in xrange(0,100):    #key为FAN()的结果, value为n(位数补足到2位)
```

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

```
if name == 'main':
```

```
    foo()
```

```
    print 'ok'
```

```
flag:SIS{a9ab115c488a311896dac4e8bc20a6d7}
```

6.密文 rot13(连接: <http://www.shiyanbar.com/ctf/728>)

直接rot13解码就行

编码/解码

制 Url UUEncode Quoted-Printable MD5,SHA Unicode 电子邮件 文字乱码 离线输入法 定时刷新网页

广告 X

紧急逃离: 股票测评低于60分 割肉也要抛
输入股票代码 立即诊股 zbyads.cn

rot13

```
57E9F980EABF49973F757CDB9F80D36C
```

Rot13 编码 Rot13 解码 拷贝 剪切 粘贴 清除

<http://blog.csdn.net/yalecaltech>

7.keyboard (链接: <http://www.shiyanbar.com/ctf/61>)

提示键盘了, 按照给出的字母顺序在键盘上画出字母的形状, 就是答案

8.凯撒是罗马共和国杰出的军事统帅 (连接: <http://www.shiyanbar.com/ctf/40>)

按照提示, 直接谈凯撒解密即可

9.摩擦摩擦 (链接: <http://www.shiyanbar.com/ctf/39>)

直接摩斯解密

10.最近听说刘翔离婚了 (链接: <http://www.shiyanbar.com/ctf/38>)

栅栏密码

其实写多了, 套路就知道了

肯定是keyis{simplexue}

给我老师的人工智能教程打call! <http://blog.csdn.net/jiangjunshow>

