CTF-Crypto题目分析__1

原创

建议密码为123456 于 2021-04-12 18:30:09 发布 1590 收藏

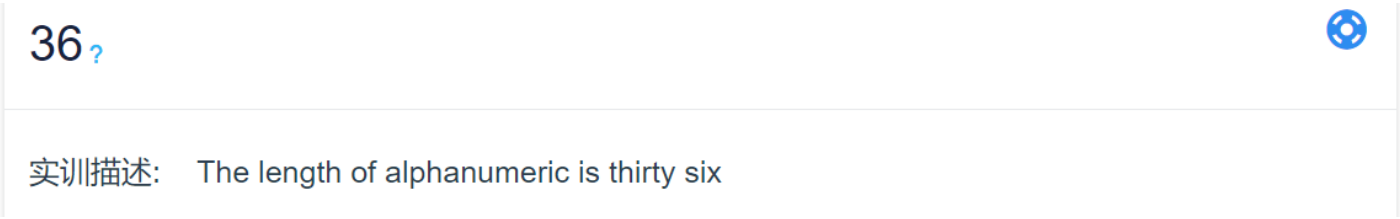
分类专栏： ctf-crypto题目分析 文章标签： 信息安全 安全

本文链接：https://blog.csdn.net/a6b6c6d5488/article/details/115633553

CTF-Crypto题目分析__1

以下所有题目提交flag的格式为SeBaFi{}

第一题：考察base36编码



下载附件后可得：597142166468670232704404065453992639482284357949191392729 31

根据提示可以推测可能是base36编码，用python解码

```
#!/usr/bin/env python
# -*- coding:utf-8 -*-
import base36

num = 597142166468670232704404065453992639482284357949191392729 31
print(base36.dumps(num))
```

得到字符串：flagis2fya2r884fnoekustyxmecv7a98blhwj。

最后可得flag：SeBaFi{2fya2r884fnoekustyxmecv7a98blhwj}

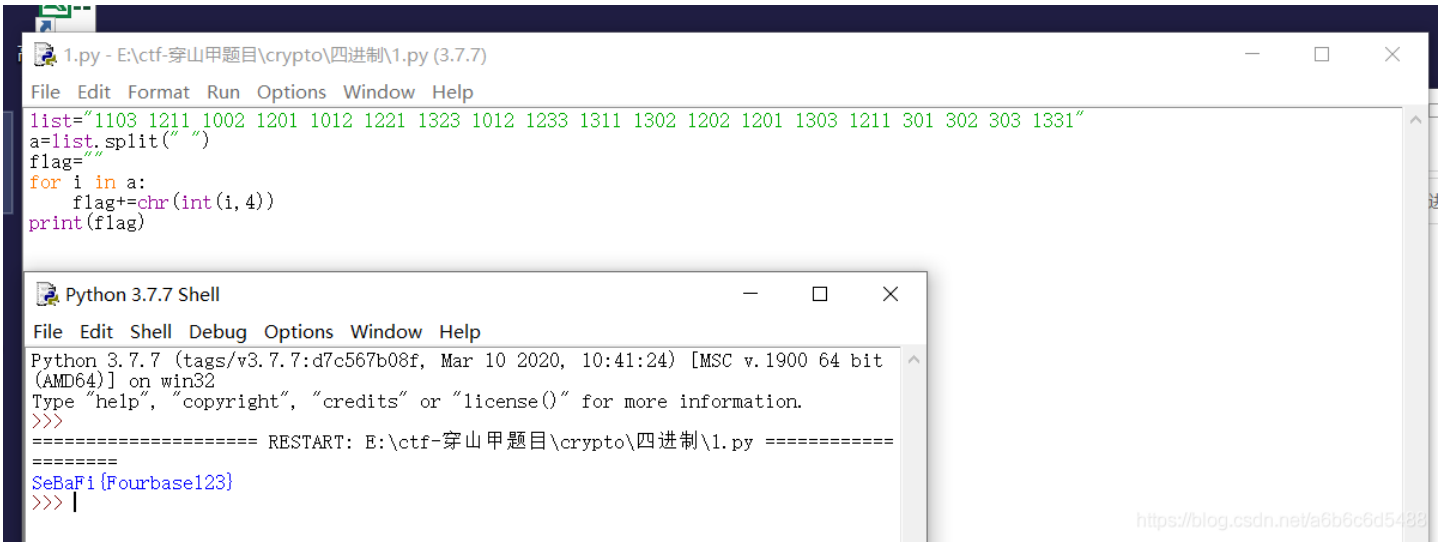
第二题：考察四进制

4进制

实训描述:　你知道4进制吗?

下载附件后得：1103 1211 1002 1201 1012 1221 1323 1012 1233 1311 1302 1202 1201 1303 1211 301 302 303 1331

没有超过四的，判断为四进制，py脚本四进制转十进制，十进制ASCII码，得到flag



python脚本如下：

```
list="1103 1211 1002 1201 1012 1221 1323 1012 1233 1311 1302 1202 1201 1303 1211 301 302 303 1331"
a=list.split(" ") //以空格切片，放入数组a
flag=""
for i in a:
flag+=chr(int(i,4)) //通过ascii码转四进制
print(flag)
```

具体split用法见 https://www.runoob.com/python/att-string-split.html

第三题：a1z26解密

a1z26

实训描述:　游戏里面好像藏了东西,解出题目的时候记得加上SeBaFi{}提交

下载后发现有一个"猜数字游戏2.py"

点击运行

猜数字游戏2.py - E:\ctf-穿山甲题目\crypto\a1z26\a1z26\猜数字游戏2.py (3....

File Edit Format Run Options Window Help

```
import random
secher = random.randint(1,20)
print("--------猜数字游戏----------")
temp = input("开始游戏:")
guess = int(temp)
while guess != secher:
    temp = input("不对不对，继续：")
    guess = int(temp)
    if guess == secher:
        print("你真棒！")
    else:
        if guess > secher:
            print("大了，太大了")
        else:
            print("小了，这个数字太小了")
print("游戏结束，不玩啦！")
1-4-4-1-4-1-1-4-4-4-23-4-14-11-10-22-4-6
```


发现程序底下存在与上面无关的一串数字，猜测可能这串数字的加密方式可能为题目a1z26的加密方式，复制到在线网站进行解密

a1z26加密在线网站 http://ctf.ssleye.com/a1z26.html

最后可得flag：SeBaFi{addadaadddwdnkjvdf}

第四题：仿射密码

题目名字是Affine，我们猜测是仿射密码
y=ax+b，有题目可知a=3，b=7

通过在线网站解密，可得flag：SeBaFi{affineisverygood}

第五题：一步之遥，位移密码>base64

小明说b3W6f3FzOHKkZ3KiN{B5NkSmZXJ5[ERxNUZ5Z3ZyZ{Gn[kWigR>>
说完，然后他就以64m每秒的速度溜了。

考察移位密码，题目提示64m/s的速度，联想到base64编码。>>联想到==，ascii码差了一位题目本身也提示一步（A Step），所以移动位数为1位。

编写python脚本，再base64解码得到flag

```
a="b3W6f3FzOHKkZ3KiN{B5NkSmZXJ5[ERxNUZ5Z3ZyZ{Gn[kWigR>>"
s=[""]*len(a)
for j in range(26):
    for i in range(len(a)):
        s[i]=chr(ord(a[i])-j)
    print ("".join(s))
```

flag：SeBaFi{a24bccba30824eab8d40168cf1c1ff5a}