buuctf——rot

原创

m0_46607055 于 2021-10-23 11:02:34 发布 263 收藏 1
分类专栏： CTF密码学 文章标签： 哈希

题目

```
破解下面的密文：

83 89 78 84 45 86 96 45 115 121 110 116 136 132 132 132 108 128 117 118 134 110 123 111 110 127 108 112 124

flag格式flag{}
```

看着像是 ascii 码。

但是有大于 127 的数字存在，所以要先处理。

题目名称为 rot，

```
ROT5、ROT13、ROT18、ROT47 编码是一种简单的码元位置顺序替换暗码。此类编码具有可逆性，可以自我解密，主要用于应对快速浏览，

ROT5 是 rotate by 5 places 的简写，意思是旋转5个位置，其它皆同。下面分别说说它们的编码方式：
ROT5：只对数字进行编码，用当前数字往前数的第5个数字替换当前数字，例如当前为0，编码后变成5，当前为1，编码后变成6，以此类推
ROT13：只对字母进行编码，用当前字母往前数的第13个字母替换当前字母，例如当前为A，编码后变成N，当前为B，编码后变成O，以此类
ROT18：这是一个异类，本来没有，它是将ROT5和ROT13组合在一起，为了好称呼，将其命名为ROT18。
ROT47：对数字、字母、常用符号进行编码，按照它们的ASCII值进行位置替换，用当前字符ASCII值往前数的第47位对应字符替换当前字
```

参考rot原理，将所有的数字 -13 后，再转ascii码

```
s = '83 89 78 84 45 86 96 45 115 121 110 116 136 132 132 132 108 128 117 118 134 110 123 111 110 127 108 11
l = s.split(" ")
for i in l:
    print(chr(int(i)-13),end='')
```

输出结果：

```
FLAG IS flag{www_shiyanbar_com_is_very_good_????}
MD5:38e4c352809e150186920aac37190cbc
```

看样子要 爆破 后四位，

```
demo='flag{www_shiyanbar_com_is_very_good_'
check = '38e4c352809e150186920aac37190cbc'

for i in range(32,126):
    for j in range(32,126):
        for k in range(32,126):
            for m in range(32,126):
                tmp = demo + chr(i) + chr(j) + chr(k) + chr(m) + '}'
                hash = hashlib.md5(tmp.encode('utf8')).hexdigest()
                if check == hash:
                    print(tmp)
                    exit()
```

运行结果

```
flag{www_shiyanbar_com_is_very_good_@8Mu}
```