

CTF-----Crypto(仿射密码解密)

原创

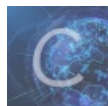
[Sallyyyym](#) 于 2019-04-19 00:06:59 发布 4274 收藏 2

分类专栏: [CTF](#) 文章标签: [Crypto](#) [仿射解密](#)

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/Sallyyyym/article/details/89391087>

版权



[CTF 专栏收录该内容](#)

2 篇文章 0 订阅

订阅专栏

CTF-----Crypto此密文是通过函数 $y=5x+12$ 得到的, 请解密。flag为明文的MD5值, 答案格式: flag{xxx}。RgYDMllaKzGC

由题可知: 该加密方式是仿射加密, 反推解密函数 ($D(x)=5^{-1}(y-12) \bmod 26$)

先用python 代码解密

```
def affine(a, b):
    pwd_dic = {}
    for i in range(26):
        pwd[chr(((a*i+b)%26)+97)] = chr(i+97)
    return pwd
if name == 'main':
    pwd = {}
    pwd1 = "rgydmlakzgc"
    plain = []
    pwd = affine(5, 12)
    for i in pwd1:
        plain.append(pwd[i])
    print ("Flag:"+"".join(plain))
```

得到flag (注意: 对应大写哦)

![在这里插入图片描述]

```
Run: affair x
"C:\Program Files\Python36\python.exe" D:/untitled/affair.py
Flag:bestaffikney
Process finished with exit code 0
https://blog.csdn.net/Sallyyyym
```

最后一步就是MD5加密啦 (是32位的哦)