

Bugku Crypto affine wp

原创

shifaziran2007 于 2021-09-09 22:47:06 发布 179 收藏

分类专栏: [wp-crypt](#) 文章标签: [python](#) [安全](#)

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/shifaziran2007/article/details/120211570>

版权



[wp-crypt](#) 专栏收录该内容

9 篇文章 0 订阅

订阅专栏

$y = 17x - 8$

flag{szyfimhyzd}

答案格式: flag{*}

来源: 第七届山东省大学生网络安全技能大赛

仿射密码解密过程:

$$x = 17^{-1}(y + 8) \bmod 26$$

其中, $17^{-1} = 23 \bmod 26$

python实现:

```
import gmpy2

# 构造alphabet
alp = []
for i in range(26):
    alp.append(chr(ord('a') + i))

# 映射a--->0, b--->1...
map_a_0 = {}
for i in range(26):
    map_a_0[alp[i]] = i

flag = list("szyfimhyzd")

_17_inv = gmpy2.invert(17, 26)

y = ""
for c in flag:
    y += alp[(23 * (map_a_0[c] + 8)) % 26]

print("flag{%s}" % y)
```



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)