

ctf 仿射

原创

[Generationofdonglin](#) 于 2018-12-11 11:45:49 发布 718 收藏 1

分类专栏: [ctf 信息安全技术](#) 文章标签: [ctf 仿射](#)

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/Generationofdonglin/article/details/84952567>

版权



[ctf](#) 同时被 2 个专栏收录

1 篇文章 0 订阅

订阅专栏



[信息安全技术](#)

4 篇文章 0 订阅

订阅专栏

仿射 (提交你找到的字符串的MD5值)

先下载附件, 由于忘了网址, 所以直接给内容:

名称	修改日期	类型	大小
Ciphertext.txt	2018-8-8 16:16	文本文档	1 KB
hint.txt	2018-8-8 15:41	文本文档	1 KB

Ciphertext.txt 中的内容是:

`achjbnpdfherebjsw`

hint.txt 中的内容是:

`b=7`

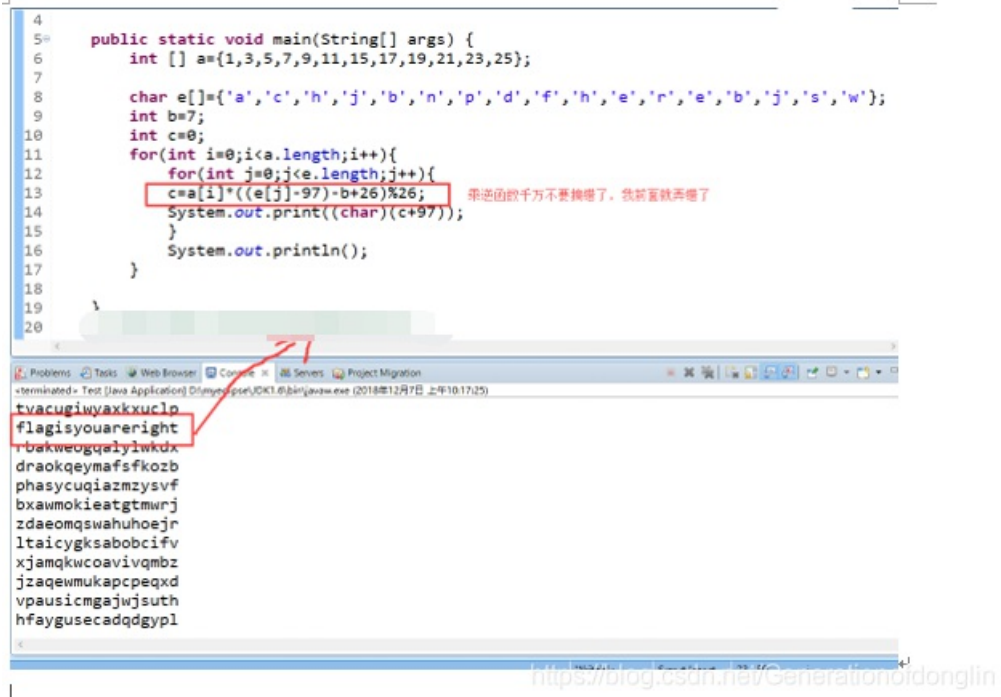
解题步骤: 首先要知道仿射密码函数: $c=(ax+b)\%26$

已知一字符串 `achjbnpdfherebjsw`, 和 $b=7$

猜想 x 取值 `achjbnpdfherebjsw`和 $b=7$, 现在需要 a 的取值。

仿射原理, a 必然和26互质, 所以 a 有多个取值1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25。

需要写个代码, 下列为Java代码:



看到有个字符串 flagisyouareright

再在网上用你MD5工具，就可以得到结果（答案略）

ctf 仿射