

# 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:  $c=(ax+b)\%26$

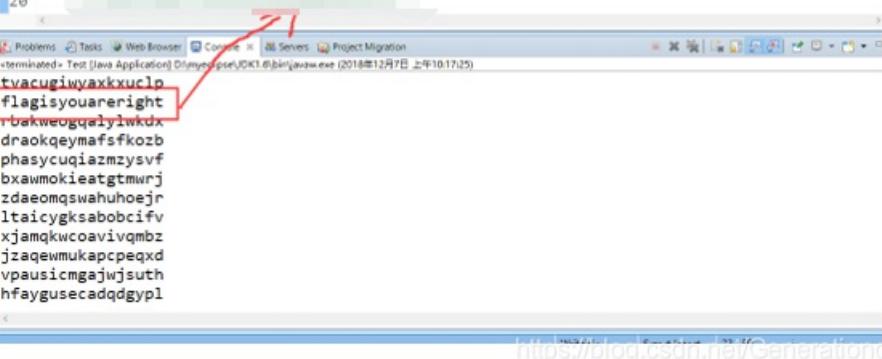
已知一字符串 achjbnpdfherebjsw, 和  $b=7$

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:

```
4
5  public static void main(String[] args) {
6      int [] a={1,3,5,7,9,11,15,17,19,21,23,25};
7
8      char e[]={‘a’,‘c’,‘h’,‘j’,‘b’,‘n’,‘p’,‘d’,‘f’,‘h’,‘e’,‘r’,‘e’,‘b’,‘j’,‘s’,‘w’};
9      int b=7;
10     int c=0;
11     for(int i=0;i<a.length;i++){
12         for(int j=0;j<e.length;j++){
13             c=a[i]*((e[j]-97)-b+26)%26; // 逆向的千万不要搞错了，我前面对应错了
14             System.out.print((char)(c+97));
15         }
16         System.out.println();
17     }
18
19
20 }
```



tvacugiywaxkxulp  
flagisyousuareright  
tvakwiegqelyzkwdx  
draokqeymafstkozb  
phasycuqiazmzysvf  
bxawmokieatgtmwrij  
zdaemqswahuhoejr  
ltacygksabobcifv  
xjamqkwcoavivqmbz  
jzaqewmukapcpceqxd  
vpausicmgajwjjsuth  
hfaygusecadqdgypl

看到有个字符串 flagisyousuareright

再在网上用你MD5工具，就可以得到结果（答案略）

ctf 仿射