

# BUUCTF-Crypto-password+变异凯撒题解

原创

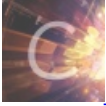
ASSOINT 于 2020-12-10 20:07:08 发布 1178 收藏 1

分类专栏: [Crypto](#)

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/weixin\\_47869330/article/details/110967574](https://blog.csdn.net/weixin_47869330/article/details/110967574)

版权



[Crypto](#) 专栏收录该内容

22 篇文章 3 订阅

订阅专栏

解题:

password:

1. 题目:

姓名: 张三

生日: 19900315

key格式为key{xxxxxxxx}

2. 就靠自己瞎猜:

解题格式为:

```
flag{姓名首拼小写+出生年月日}
```

(气死了气死了 我首先还用了九键对应的数字、将姓名化成zhangsan一个字母一个数字对应想用base解密)

3.flag: `flag{zs19900315}`

变异凯撒:

1. 题目: `afZ_r9VYfSc0eO_UL^RWUc`

2. 解题思路:

不管怎么样先用密码机器在线解密一波, 结果各种可能性都试过了发现行不通。

于是开始分析题目, 对照ASCII码表将题目前几位的 `afZ_r` 转成 `flag{`, 看对应的数字之间存在什么规律。

```
题目`afZ_r`:  
97\102\90\95\114  
明文`flag`:  
102\108\97\103\123  
相差:  
5\6\7\8\9
```

从5到26, 可以验证最后一个正是闭花括号: "}"

3. 写c代码:

```
#include<stdio.h>
int main()
{
    int i;
    char c[]="afZ_r9VYfSc0eO_UL^RWUc";
    for(i=0;c[i]!='\0';i++)
    {
        c[i]=i+5+c[i];
    }
    printf("%s",c);
}
```

解密得到flag:

```
flag{Caesar_variation}
```

## 小结:

1. 以后看到类似的姓名+生辰，套公式:

```
flag{姓名首拼小写+出生年月日}
```

2. 变异凯撒\凯撒密码: 先分析前五个字母, 看看有什么规律, 如果可以看出来先用工具大概套一下, 如果工具不行就写脚本
3. (如果以后不这么菜鸡了, 直接写脚本就好了) 抹泪

好耶!