

Crypto简单入门

原创

上官大大 于 2021-10-12 20:25:29 发布 122 收藏

分类专栏: [密码学](#) 文章标签: [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/haoshangguan/article/details/120730903>

版权



[密码学](#) 专栏收录该内容

2 篇文章 0 订阅

订阅专栏

Crypto

古典密码

凯撒密码:

将明文字母向后移n位。

解决方法:

□ 凯撒密码加解密方法:

- 手动解密
- 在线工具
- 使用python的pycipher模块
- `$pip install pycipher #安装pip工具`
`$python`
`>>> from pycipher import Caesar`
`>>> Caesar(key=5).encipher("HELLOCAESAR")`
`'MJQQTHFJXFW'`
`>>> Caesar(key=5).decipher("MJQQTHFJXFW")`
`'HELLOCAESAR'`

CSDN @上官大大

ROT13: 将明文字母向后移13位 (特殊的凯撒密码)

栅栏密码:

将要加密的信息分为n组, 依次取各组的第1, 2, 3...位。

弗吉尼亚密码:

使用二位表单查找密码。

对称加密算法

算法有DES、3DES、AES等。

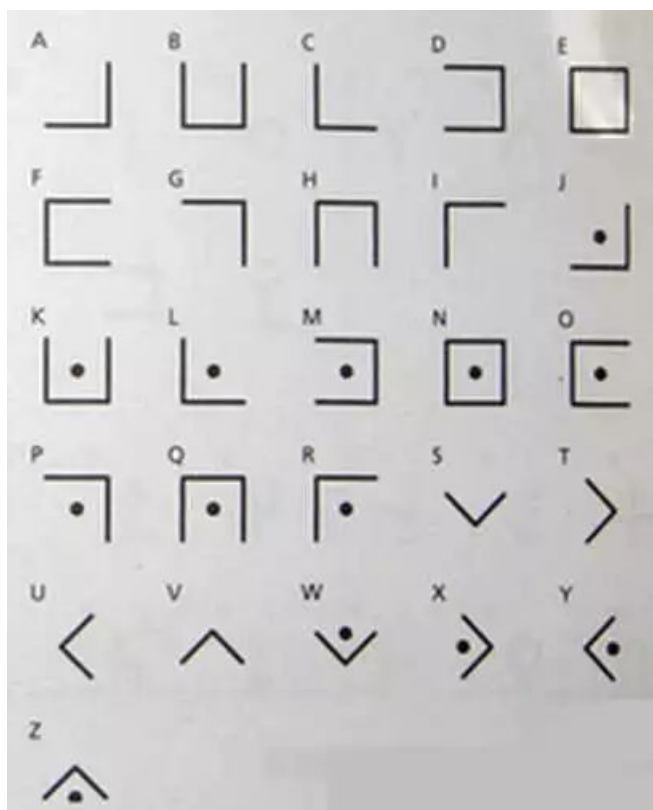
一般都是在线工具进行加解密。

非对称加密算法

公钥与私钥分别进行加解密。

CTF中的常用密码

猪圈密码：格子图形对应字母



培根密码：一种由五位的a和b的组合构成的替换密码

键盘密码：电脑键盘的位置模拟画出图案