

bugku-writeup-Crypto-小山丘的秘密

原创

dark2019 于 2021-06-22 16:15:53 发布 53 收藏

分类专栏: [信息安全 wp](#) 文章标签: [密码学 bugku](#)

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/qq_22597955/article/details/118109210

版权



[信息安全](#) 同时被 2 个专栏收录

53 篇文章 1 订阅

订阅专栏



[wp](#)

31 篇文章 0 订阅

订阅专栏

题目: 小山丘的秘密

小山丘的秘密

Crypto

已解决

分数: 15 金币: 2

题目作者: doge

一血: dotast

一血奖励: 2金币

解决: 631

提示:

描述: hill能有什么秘密呢

其他: [↓小山丘的秘密.zip](#)

请输入flag

提交

https://blog.csdn.net/qq_22597955

01—找线索

flag.txt - 记事本

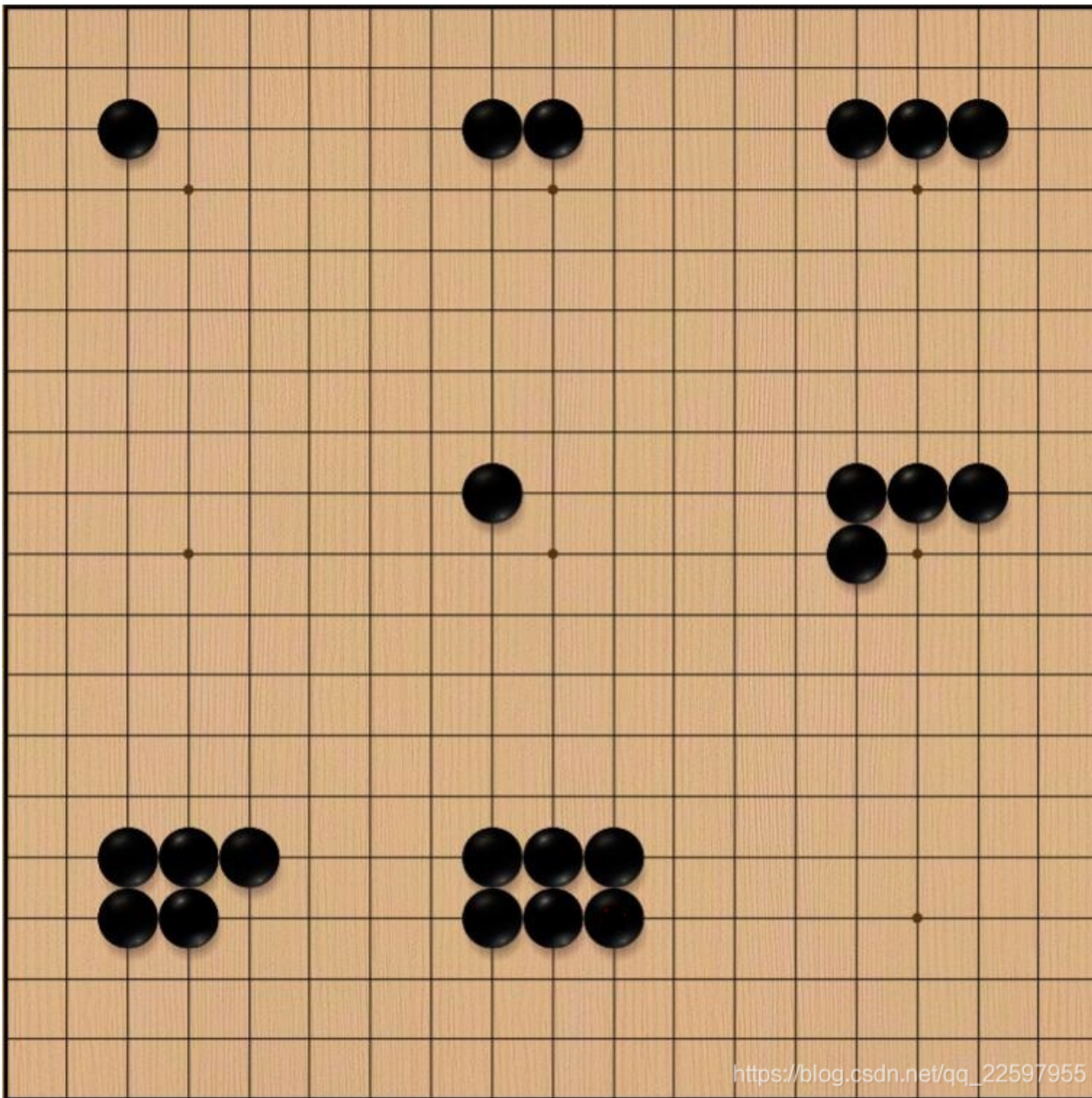
文件(E) 编辑(E) 格式(O) 查看(V) 帮助(H)

bugku{PLGTGBQHM}

其中A=1, flag全为小写

题目描述为“hill能有什么秘密?”因此考虑此题考查hill密码。flag.txt中提示A=1,而hill密码中A=0,需要调整一下排布: Z=0,A=1,B=2,C=3...

hill密码解密还需要密钥，题目中还给出一个棋盘，从上而下棋子数量依次为1 2 3 1 4 5 6，可表示为**ABCADEF**



02—解密

应用 翻译 百度一下，你就知道 学习资料

一个工具箱 - 好用的在线工具都在这里! 会员登录 搜索工具

希尔密码加密/解密

字母表 zabcdefghijklmnopqrstuwxvxy

plaintext: plgtgbqhm

密钥: abcdef

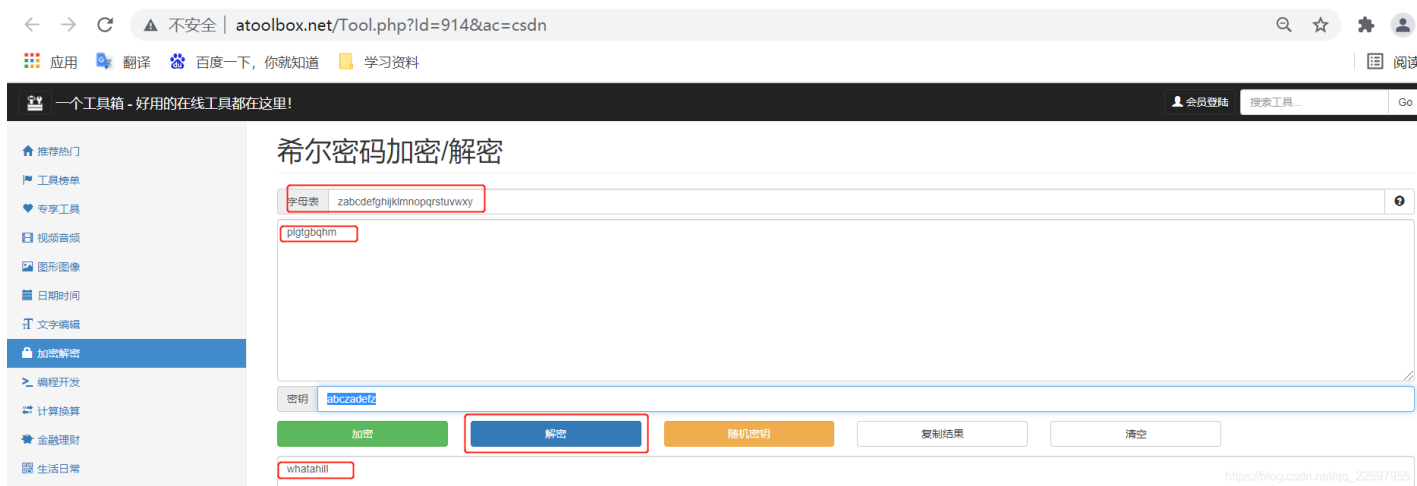
加密 解密 随机密钥 复制结果 清空

这里是解密/加密的结果

Wrong key. Key length should be square of integer.

https://blog.csdn.net/qq_22597955

由于flag.txt中提示flag全为小写，因此调整字母表为zabcdefghijklmnopqrstuvwxy，密钥为abczadefz,发现报错密钥必须为方阵，因此密钥应该为9位，棋盘上没有棋子的黑点位置为0，调整密钥为abczadefz,解密：



得到flag: bugku{whatahill}。