谜题一

# 1. 加密算法描述

## 1）加密对象

加密对象为一段有意义的英文文本，不含空格、标点符号等字符，只包含英文字母。我们将26个字母依次对应成整数. 假设明文为.

## 2）密钥

密钥有个字母和，其中分别和26互素，*.*

## 3）加密过程

首先循环利用(进行加密：

,

然后循环利用(进行加密：

,

密文为.

## 4）解密过程

,

,

其中

# 2. 攻击方式

唯密文攻击，恢复密钥（字母形式）：你将得到一串密文，要求恢复出对应的明文.

# 3. 时间限制

2021年10月10日之前完成. 成功满分20分，每超一天扣1分；失败保底(5分)；实在解不出来，可以做理论分析(满分16分).

# 4. 题号

所有同学待解密的密文放在“ciphertext.txt”文件中。

解的谜题题号为：（**系统编号**

以下是系统编号. 例如白曜宁同学的系统编号是1号，题号则是。

同学的系统编号见下页附录。

# 5.发送方式

答案发送给助教 郭婷婷（[guotingting@iie.ac.cn](mailto:guotingting@iie.ac.cn)）. 邮件正文写明姓名+系统编号，恢复的明文放在格式为txt文档的附件中，该txt文档命名为题号。如系统编号1的白曜宁同学的附件命名为“21.txt”。（如果实在解不出明文，做理论分析的话，不必以txt文件形式发送，可以将解答以word/pdf/手写后拍摄照片等形式放在附录中发送。）

# 6.附录

|  |  |
| --- | --- |
| 1 | 白曜宁 |
| 2 | 包家玮 |
| 3 | 蔡东澍 |
| 4 | 曹纵 |
| 5 | 陈凯 |
| 6 | 陈兴 |
| 7 | 陈阳恭 |
| 8 | 程逸飞 |
| 9 | 程轶涵 |
| 10 | 杜剑峰 |
| 11 | 顾辉 |
| 12 | 韩天硕 |
| 13 | 侯铖安 |
| 14 | 胡呈睿 |
| 15 | 黄春早 |
| 16 | 姜陈浩 |
| 17 | 李安逸 |
| 18 | 李晨宇 |
| 19 | 李浩然 |
| 20 | 李敏彰 |
| 21 | 李志伟 |
| 22 | 廖鹤明 |
| 23 | 刘方舟 |
| 24 | 刘玉婷 |
| 25 | 冉东川 |
| 26 | 任峥 |
| 27 | 涂亦驰 |
| 28 | 涂云庆 |
| 29 | 魏克婷 |
| 30 | 吴瑞宸 |
| 31 | 夏琦清 |
| 32 | 肖震宇 |
| 33 | 徐若洲 |
| 34 | 许淑扬 |
| 35 | 延晓龙 |
| 36 | 杨涵显 |
| 37 | 殷佳伟 |
| 38 | 尹勇荐 |
| 39 | 袁誉飞 |
| 40 | 曾御柏 |
| 41 | 张宇光 |
| 42 | 张振超 |
| 43 | 张振铎 |
| 44 | 朱泽烁 |
| 45 | 朱骞 |