实验一 Many Time Pad

编程语言

- Python（推荐）或者 C/C++/java

实验目的

- 了解流密码的结构特点；
- 掌握One-time Pad的一般具体实现；
- 通过使用Python（推荐）或者C/C++/java，编程实现一个流密码加密示例的破解，进一步认识在流密码加密中多次使用相同密钥导致的问题

实验内容

- 在掌握流密码结构的基础上，通过本实验观察使用相同流密码密钥加密多个明文导致的严重后果。
- 附件ciphertext.txt有11个十六进制编码的密文，它们是使用流密码加密11个明文的结果，所有密文都使用相同的流密码密钥。
- 实验的目标是解密最后一个密文，并提交明文消息。
- 提示：
    - 对密文进行异或，并考虑当空格与[a~z,A~Z]中的字符进行异或时会发生什么。
    2. 附件encrypt.py是用于生成密文的Python示例程序（不影响实验，仅供参考）。

实验要求

- 在线提交源码和实验报告，实验报告需要包含实验结果即最后一个密文的解密结果、原理分析以及重要代码段解释
- 报告提交截止时间为：2021年4月10日0点。
- 禁止抄袭，一经发现0分处理。

实验时间与地点

- 时间：本周五晚上6:30-9:30（即4月2日）
- 地点：思贤楼303教室
- 每次实验都设有小助教（具体的余老师上课讲过），最多只接受9名【C++和java各1名，python7名】，按照能够完整完成实验并在助教或余老师处检查合格的顺序。要求小助教实验课时都在实验教室帮助学生完成实验