Chapter 2

流密码

Exercise 3

编程实现流加密算法，其密钥由 32 位 LFSR 生成。算法对一个 txt 文件进行加密，加密后的信息存在二进制文件中，测试用 txt 文件内容为” 密码学是信息安全专业的一门基础课，北京联合大学开设了信息安全专业，所以北京联合大学开设了密码学课程。”。也可对加密后的二进制文件进行解密，解密后存位一个 txt 文件，执行命令时，用户可以指定 txt 文件名，和二进制文件名。seed 是存储种子值的二进制文件。

例如:

加密执行的命令: streamcipher -e 1.txt seed c1

解密执行的命令: streamcipher -d c1 seed 2.txt

项目参考初始仓库`https://gitee.com/buuer/streamcipher32lfsr.git`

提交截止时间：2020 年 3 月 23 日 8：00 前

说明

- 密钥是什么？本原多项是什么 (抽头序列是什么？Fibonacci 配置是什么？)，可以查阅相关材料。