

Chapter 3

分组密码

Exercise 4

编程实现 DES 加解密算法，工作模式为 ECB 模式，填充模式，请选择一种填充模式做为加密时的缺省填充模式。编写算法实现说明文档。算法实现后用命令行的方式运行。

例如：

加密执行的命令: `descipher -e 1.txt key c1`

解密执行的命令: `descipher -d c1 key 2.txt`

其中：key 是保存密钥的二进制文件，c1 是密文二进制文件，1.txt 是原文的 txt 文件，2.txt 是解密后原文文本文件。

项目参考初始仓库<https://gitee.com/buuer/DESCipher.git>

提交截止时间：2020 年 4 月 6 日 8: 00 前

Exercise 5

编程实现 TDES(Triple DES) 加解密算法。