

Chapter 5

哈希函数

Exercise 6

编程实现 MD5 算法，参考 RFC1321，生成的 hash 值用 16 进制的数的表述方式写到你指定的一个 txt 文件中。并用一个常用的软件对计算结果对比，以此来说明你算法实现的正确性，可以使用 openssl，或者 windows 中的 certutil 等等。程序编写完成后，按给定的文档格式编写实验报告，将此文档的 pdf 格式上传到你的 gitee 仓库中。

例如：

生成摘要：md5hash file1 1.txt

其中：file1 文件中的内容是要生成摘要的内容，1.txt 文件时一个文本文件，file1 文件摘要的 16 进制形式的表述写到这个文件中。

项目参考初始仓库<https://gitee.com/buuer/md5-hash>

在提交时，digest.txt 存储的是对 plain_buu_intr.docx 中的内容做哈希计算后结果的 16 进制数的表示。也就是说，如果计算出来的摘要二进制是“0100 0010 1000 1111”，那么在 digest.txt 中就以文本方式存储的是“428F”。