《应用密码学》课程实践

实践题目 2　DES 的实现

实践要求：

1. 分别实现 ECB、CBC、CFB、OFB 这四种操作模式的 DES。每种操作模式都有一组对应的测试数据，以便检查程序的正确性。其中，CFB 操作模式为 8 位 CFB 操作模式，OFB 操作模式为 8 位 OFB 操作模式。

2. 要求以命令行的形式，指定明文文件、密钥文件、初始化向量文件的位置和名称、加密的操作模式以及加密完成后密文文件的位置和名称。加密时先分别从指定的明文文件、密钥文件和初始化向量文件中读取有关信息，然后按指定的操作模式进行加密，最后将密文（用 16 进制表示）写入指定的密文文件。

命令行的具体格式如下：

e1des -p plainfile -k keyfile [-v vifile] -m mode -c cipherfile

参数：

-p plainfile　指定明文文件的位置和名称
-k keyfile　指定密钥文件的位置和名称
-v vifile　指定初始化向量文件的位置和名称
-m mode　指定加密的操作模式
-c cipherfile　指定密文文件的位置和名称。

3. 分别实现对每种操作模式下加密及解密速度的测试，要求在程序中生成 5MB 的随机测试数据（不要求使用随机数发生器），连续加密、解密 20 次，记录并报告每种模式的加密和解密的总时间（毫秒）和速度（MByte/秒）。

4. 用 C 和/或 C++语言完成程序。

5. 最终上交的作业包括：电子版的实践报告和程序源代码，要求由源代码能重新正确生成可执行代码。

6. 实践报告应包括以下内容：作业标题、学号、姓名、E-mail、作业内容描述、实验环境描述、实验过程简述、实验结果（实验的正确性以及每种操作模式下加密和解密速度的测试结果）、作业的收获和体会。

附录：测试数据

明文：(16 个字节，128bit，用 16 进制表示)
4E6574776F726B205365637572697479　(明文文件如：des_plain.txt)

密钥：(8 个字节，64bit，用 16 进制表示)
57696C6C69616D53　(密钥文件如：des_key.txt)

初始化向量 VI（在 CBC、CFB、OFB 模式中使用）：(8 个字节，64bit，用 16 进制表示)
5072656E74696365　(初始化向量文件如：des_iv.txt)

密文：(16 个字节，128bit，用 16 进制表示)
ECB 模式：958920B1358EF1972B9EE4548DC08E8A
CBC 模式：5EB15B91506B9AE7CEB65954AE115E03
CFB 模式：F70F01584ACF4D966ADC143EB240C962
OFB 模式：F7B0FFCDC0B9BBA76092B929D769417A

密文文件： (如：des_ Cipher.txt)