《应用密码学》课程实践

实践题目 3　　AES 的实现

实践要求：

1. 只要求实现块长为 128 位、密钥长为 128 位的 AES，分别实现 ECB、CBC、CFB、OFB 这四种操作模式。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：

e2aes -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：(32 个字节，256bit，用 16 进制表示)

43727970746F677261706879206 16E64204E6574776F726B5365637572697479

（明文文件如：AES_plain.txt）

密钥：(16 个字节，128bit，用 16 进制表示)　57696C6C69616D5374616C6C696E6773

（密钥文件如：AES_key.txt）

初始化向量 VI（在 CBC、CFB、OFB 模式中使用）：(16 个字节，128bit，用 16 进制表示)

5072656E7469636548616C6C496E632E　　（初始化向量文件如：AES_iv.txt）

密文：(32 个字节，256bit，用 16 进制表示)

ECB 模式：DB727AC6624F3699CBFC4F0F890832B8A4B1DCA1F52EF8E4CE0FD12E307476C6

CBC 模式：9B0048990511252F5E1088663F8CB038A21952EAC6D2C27546369FCA0136BF04

CFB 模式：EAC2DD6334E8FA07FDAB477ABA1628A93AFAAAD753B7E05CD59548A2927BDA97

OFB 模式：EA4641614F3CDECD2161737A39551FE2E43A54E563ED8E6B7580879BE72A5391

（密文文件如 AES_ Cipher.txt）