**第二次大作业**

计65 2016011367 胡壮飞

1. **AES算法**

根据要求，实现了AES-128, AES-192和AES-256加密标准，并验证了结果的正确性；同时，实现了CBC方式加密的AES，并测试了程序在随机产生的信息和给定密钥下的性能。采用了-O2和-msse编译选项进行了加速。代码见附件。

明文：**0xe54b04099c6c16ba14a0e25f4fb68dd4**

密钥：**0x000102030405060708090a0b0c0d0e0f** （128比特）

**0x000102030405060708090a0b0c0d0e0f1011121314151617** （192比特）

**0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f**  （256比特）

输出结果（加密结果）如下：

**AES-128: 90ad55ba79384012f1ce8663498190f4**

**AES-192: a1d1d291adacd6dd4f272b267b520194**

**AES-256: 6ffc34aaff86389008a1cb22d0da94c7**

随机产生16KB和1MB的消息，利用给定密钥加密，性能测试结果如下（使用ctime自带的clock()函数进行计时）：

Type: AES-128; Length(bytes): 16384; Encrypt time: 0.006000s; Decrypt time: 0.011000s

Type: AES-192; Length(bytes): 16384; Encrypt time: 0.006000s; Decrypt time: 0.012000s

Type: AES-256; Length(bytes): 16384; Encrypt time: 0.008000s; Decrypt time: 0.015000s

Type: AES-128; Length(bytes): 10485760; Encrypt time: 3.115000s; Decrypt time: 8.743000s

Type: AES-192; Length(bytes): 10485760; Encrypt time: 4.775000s; Decrypt time: 7.654000s

Type: AES-256; Length(bytes): 10485760; Encrypt time: 4.230000s; Decrypt time: 8.985000s

1. **SHA算法**

实现了SHA-256算法，并对附录中给定的测试样例（B5）进行了测试。代码见附件。