**中科大计算机学院**

**实 验 报 告**

**实验课程名称：网络安全**

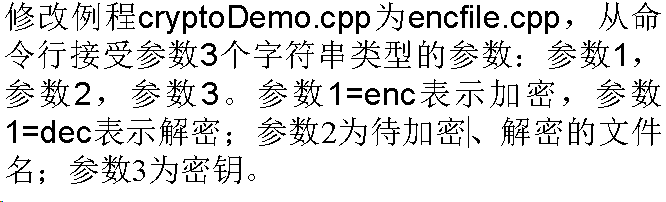
**姓名：陈坦访**

**学号：SA15011010**

**实 验 报 告**

**一、实验室名称： 网络安全实验**

**二、实验内容：**



**三、实验原理：**

对称密码体制的发展趋势将以分组密码为重点。分组密码算法通常由[密钥](http://baike.baidu.com/view/934.htm" \t "_blank)扩展算法和加密（解密）算法两部分组成。密钥扩展算法将b字节用户主密钥扩展成r个子密钥。加密算法由一个密码学上的弱函数f与r个子密钥迭代r次组成。混乱和密钥扩散是分组密码算法设计的基本原则。抵御已知明文的差分和线性攻击，可变长密钥和分组是该体制的设计要点。

AES是美国国家标准技术研究所NIST旨在取代[DES](http://baike.baidu.com/view/7510.htm" \t "_blank)的21世纪的加密标准。

AES的基本要求是，采用对称分组密码体制，密钥长度的最少支持为128、192、256，分组长度128位，算法应易于各种硬件和软件实现。1998年NIST开始AES第一轮分析、测试和征集，共产生了15个候选算法。1999年3月完成了第二轮AES2的分析、测试。2000年10月2日美国政府正式宣布选中[比利时](http://baike.baidu.com/view/21905.htm" \t "_blank)密码学家Joan Daemen 和 Vincent Rijmen 提出的一种密码算法RIJNDAEL 作为 AES.

在应用方面，尽管DES在安全上是脆弱的，但由于快速DES芯片的大量生产，使得DES仍能暂时继续使用，为提高安全强度，通常使用独立密钥的三级DES。但是DES迟早要被AES代替。流密码体制较之分组密码在理论上成熟且安全，但未被列入下一代加密标准。

AES加密数据块分组长度必须为128比特，密钥长度可以是128比特、192比特、256比特中的任意一个（如果数据块及密钥长度不足时，会补齐）。AES加密有很多轮的重复和变换。大致步骤如下：1、密钥扩展（KeyExpansion），2、初始轮（Initial Round），3、重复轮（Rounds），每一轮又包括：SubBytes、ShiftRows、MixColumns、AddRoundKey，4、最终轮（Final Round），最终轮没有MixColumns。AES加密过程是在一个4×4的[字节](http://baike.baidu.com/view/60408.htm" \t "_blank)矩阵上运作，这个矩阵又称为“状态（state）”，其初值就是一个明文区块（矩阵中一个元素大小就是明文区块中的一个Byte）。（Rijndael加密法因支持更大的区块，其矩阵行数可视情况增加）加密时，各轮AES加密循环（除最后一轮外）均包含4个步骤：

1. AddRoundKey — 矩阵中的每一个字节都与该次轮秘钥（round key）做XOR运算；每个子密钥由密钥生成方案产生。
2. SubBytes — 通过个非线性的替换函数，用[查找表](http://baike.baidu.com/view/1627735.htm" \t "_blank)的方式把每个字节替换成对应的字节。
3. ShiftRows — 将矩阵中的每个横列进行循环式移位。
4. MixColumns — 为了充分混合矩阵中各个直行的操作。这个步骤使用线性转换来混合每列的四个字节。

最后一个加密循环中省略MixColumns步骤，而以另一个AddRoundKey取代。

**四、实验目的：**

了解AES的加解密过程，会运用openssl对文件进行加解密

**五、实验内容：**

使用AES对文件进行加解密

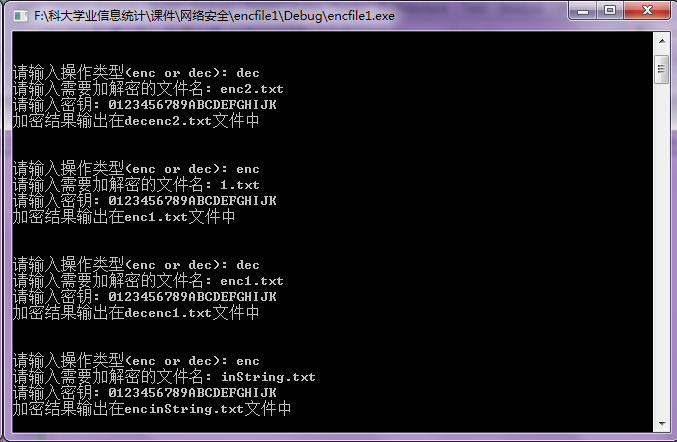
**六、实验环境（硬件设备、软件）：**

硬件：计算机

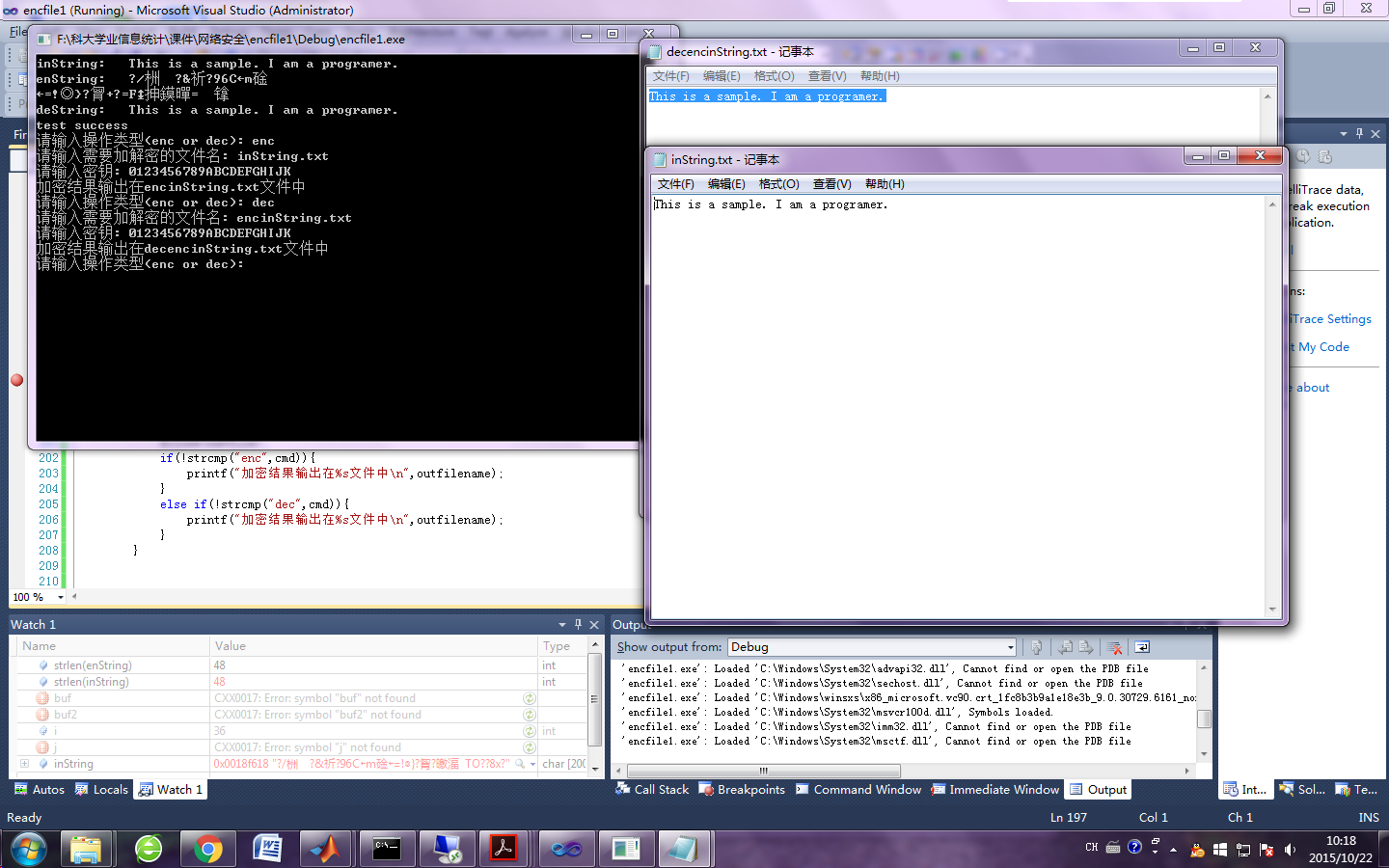
软件：windows 7,openssl

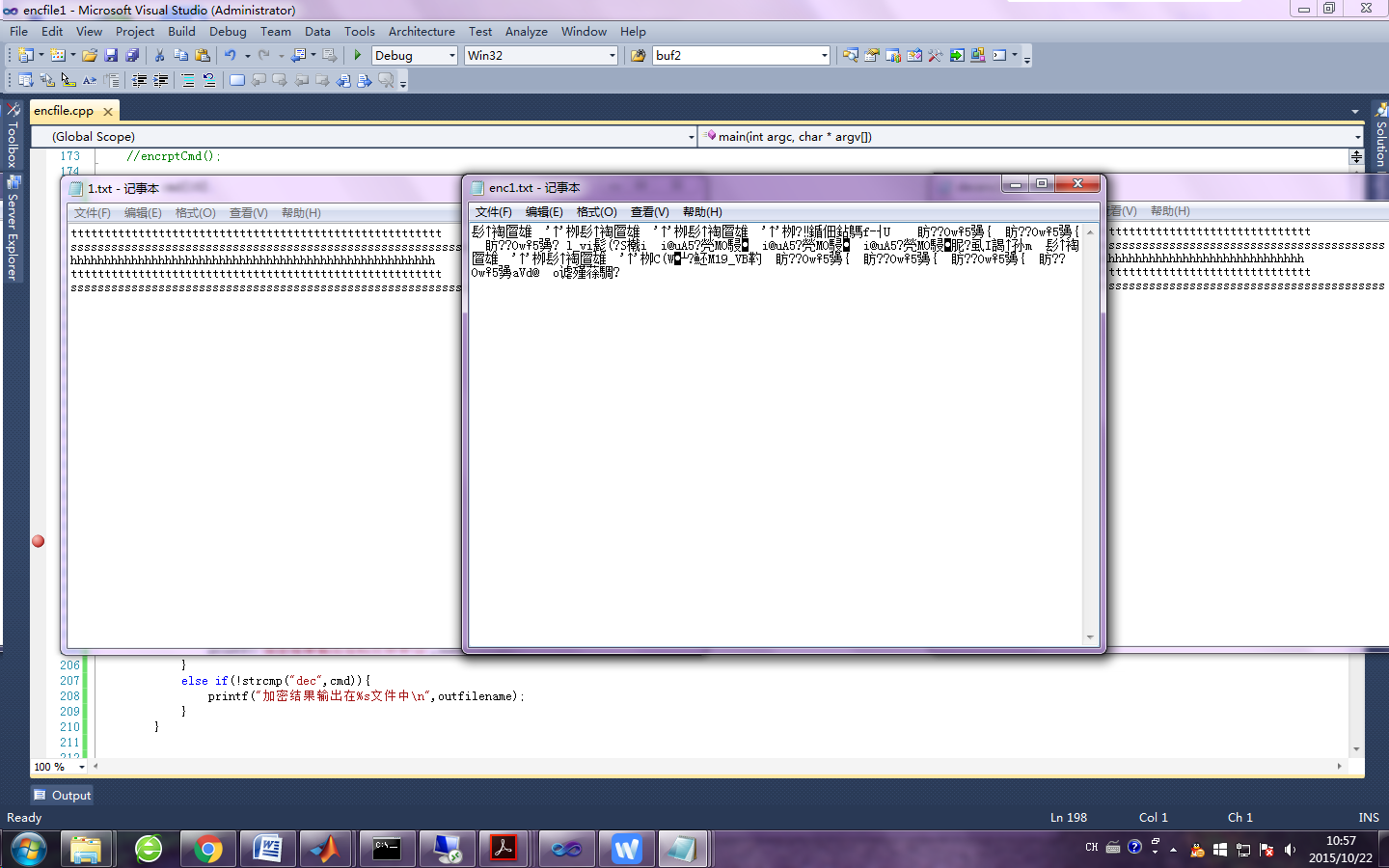
**七、实验结果：**

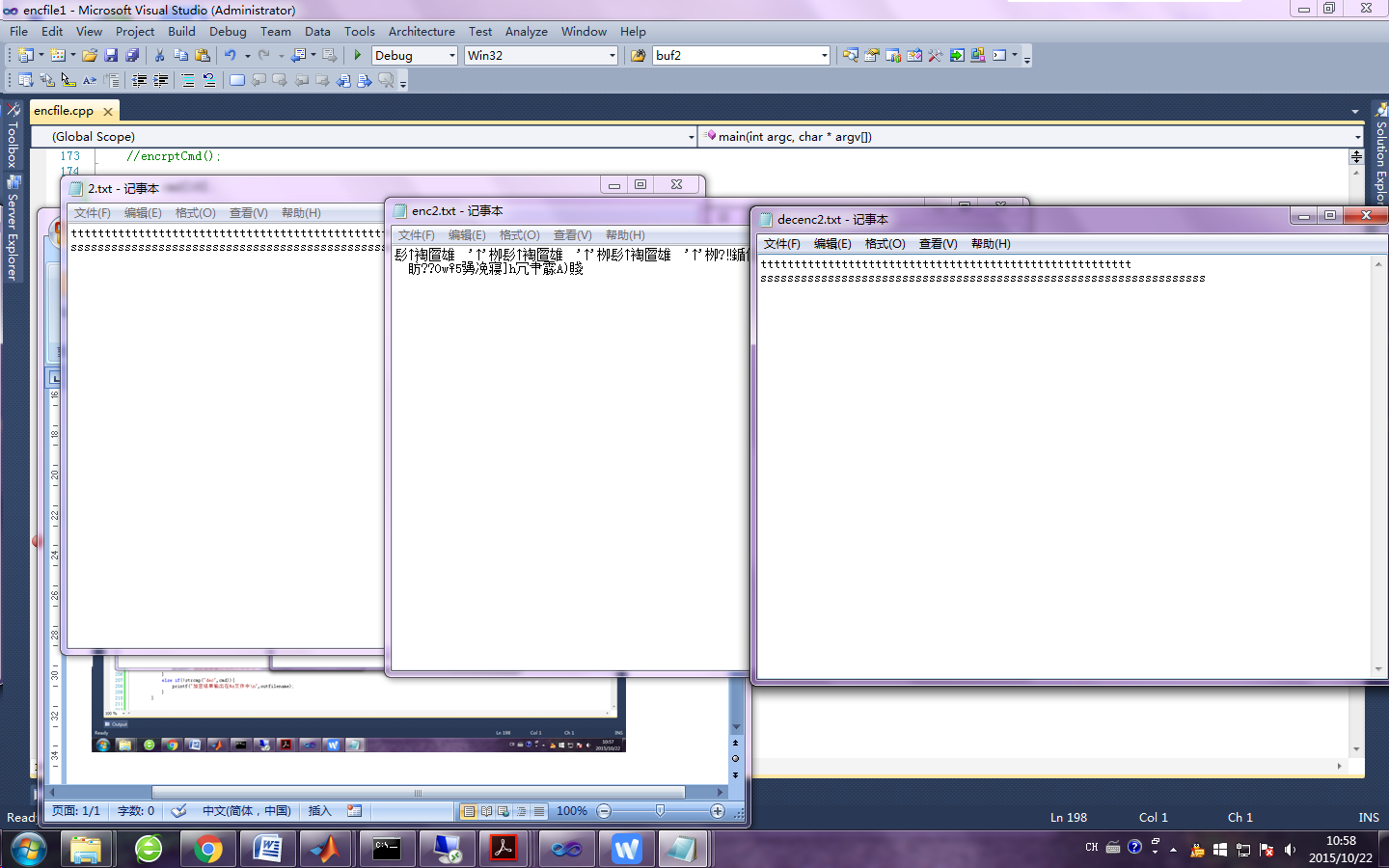
输入指令：



文件加解密结果：







**八、实验结论：**

使用AES库函数接口对文件加解密成功，实验顺利。