第3章 对称密码算法

3.1 AES

【实验目的】

通过对 AES 算法的 C 源程序代码进行修改，了解和掌握分组密码体制的运行原理和编程思想。

【原理简介】

AES 是 1997 年 1 月由美国国家标准和技术研究所（NIST）发布公告征集的新一代数据加密标准，以替代 DES 加密算法。其为对称分组密码，分组长度为 128b，密钥长度支持 128b、192b、256b。在最终的评估中，凭借各种平台实现性能的高效性，Vincent Rijnmen 和 Joan Daemen 提出的 Rijndael 算法胜出，最终被国际标准化组织确定为新一代数据加密标准 AES。

有关算法的详细介绍请参阅相关参考书。

【实验环境】

安装 Windows、Linux 操作系统的 PC 一台，且其上安装有一种 C 语言编译环境。

【实验步骤】

本实验使用的是 Rijndael 的作者在《高级加密标准（AES）算法——Rijndael 的设计》（中文版已由清华大学出版社出版）附录中给出的参考代码。该代码演示了在明文和密钥均为全 0 时，不同分组、不同密钥长度下进行 AES 加解密的结果。本实验也可从 https://github.com/libtom/libtomcrypt/blob/master/src/ciphers/aes/aes.c 下载 AES 的实现源码。

请读者分析代码，找出各个部分是由哪个函数实现的，并了解函数实现的具体过程。

选取密钥长度和分组长度均为 128b，试修改上述代码，完成以下实验。

（1）全 0 密钥扩展验证：对于 128b 全零密钥，请利用 KeyExpansion 函数将密钥扩展的结果填入表 3-1 中。

表 3-1　各轮的扩展密钥

第 0 轮	00000000000000000000000000000000	第 4 轮	
第 1 轮	62636363626363636263636362636363	第 9 轮	
第 2 轮		第 10 轮	
第 3 轮			

（2）修改程序，在表 3-2 中填写第 1 轮、第 2 轮的中间步骤测试向量。

```
LEGEND –round r = 0 to 10
Input:  cipher input
Start:  state at the start of round[r]
S_box:  state after s_box substitution
S_row:  state after shift row transformation
M_col:  state after mix column transformation
K_sch:  key schedule value for round[r]
Output: cipher output
PLAINTEXT: 3243F6A8885A308D313198A2E0370734
KEY:       2B7E151628AED2A6ABF7158809CF4F3C
ENCRYPT: 16 byte block, 16 byte key
```

表 3-2　第 1 轮、第 2 轮的中间步骤测试向量

R[00].input	3243F6A8885A308D313198A2E0370734
R[00].k_sch	2B7E151628AED2A6ABF7158809CF4F3C
R[01].start	193DE3BEA0F4E22B9AC68D2AE9F84808
R[01].s_box	
R[01].s_row	
R[01].m_col	
R[01].k_sch	
R[02].start	
R[02].s_box	
R[02].s_row	
R[02].m_col	
R[02].k_sch	

（3）修改该程序，使其可在（128，128）模式下进行文件的加解密，并对某文档进行加解密，观察解密后与原文是否相同。如有不同，试考虑如何解决。再用该程序加密流媒体文件，观察解密后是否能够正确完整播放。

（4）计算加解密的效率，并进行一定的优化使加密效率提高。

【实验报告】

（1）简述 AES 算法每个输入分组的长度及格式。

（2）简述 AES 算法每轮加密过程的 4 个步骤。

（3）填写上面的表格。

【思考题】

计算加解密的效率，并进行一定的优化使加密效率提高。

3.2 DES

【实验目的】

通过对 DES 算法的代码编写，了解分组密码算法的设计思想和分组密码算法的工作模式。

【原理简介】

DES 是 Data Encryption Standard（数据加密标准）的缩写。它是由 IBM 公司研制的一种加密算法，美国国家标准局于 1977 年公布把它作为非机要部门使用的数据加密标准，四十多年来，它一直活跃在国际保密通信的舞台上，扮演了十分重要的角色。DES 是一个分组加密算法，分组长度为 64b，密钥长度也为 64b，但因为含有 8 个奇偶校验比特，所以实际密钥长度为 56b。DES 算法是迄今为止使用最为广泛的加密算法，由于计算能力的发展，DES 算法的密钥长度已经显得不够安全了，所以目前 DES 的常见应用方式是 DES_EDE2，即三重 DES，采用加密—解密—加密三重操作完成加密，其中，加密操作采用同一密钥，解密操作采用另一密钥，有效密钥长度为 112b。

有关算法的详细介绍请参阅相关参考书。

【实验环境】

安装 Windows 操作系统的 PC 一台，其上安装 Visual C++ 6.0 以上版本的编译器。

【实验步骤】

（1）请读者从 http://cryptopp.sourceforge.net/docs/ref521/des_8cpp-source.html 下载 DES 实现的源代码，并以 112b 全 0 密钥加密数据 ff ff ff ff ff ff ff ff，验证加密结果是否为 35 55 50 b2 15 0e 24 51。

（2）测试加密速度和程序代码长度。

（3）使用 CBC 方式加密一段 64b 自选数据，改变初始向量值，比较加密结果。

【实验报告】

（1）DES_EDE2 算法程序实现框图、使用说明和源程序清单。

（2）算法加密速度测试结果。

（3）CBC 方式加密运行结果，并说明 CBC 加密方式的特点。

【思考题】

（1）从加密速度和代码长度比较 DES_EDE2 和 AES 的算法效率。

（2）为什么要使用 DES_EDE2 而不使用密钥不同的两重 DES？

3.3 SMS4

【实验目的】

通过对 SMS4 算法的代码编写，了解分组密码算法的设计思想和工作原理。

【原理简介】

SMS4 是一种由国家商用密码管理办公室发布应用于无线局域网产品中的加密算法。该算法是一个分组算法。该算法的分组长度为 128b，密钥长度为 128b。加密算法与密钥扩展算法都采用 32 轮非线性迭代结构。解密算法与加密算法的结构相同，只是轮密钥的使用顺序相反，解密轮密钥是加密轮密钥的逆序。

【实验环境】

安装 Windows 操作系统的 PC 一台，其上安装 Visual C++ 6.0 以上版本的编译器。

【实验步骤】

（1）从 http://read.pudn.com/downloads76/sourcecode/crypt/287055/sms4/sms4.cpp__.htm 参考编写 SMS4 算法，并以密钥 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10 加密数据 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10，验证加密结果是否为 68 1e df 34 d2 06 96 5e 86 b3 e9 4f 53 6e 42 46。

（2）利用相同加密密钥对一组明文反复加密 1 000 000 次，密钥为 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10，加密数据为 01 23 45 67 89 ab cd ef fe dc ba 98 76 54 32 10，验证测试结果是否为 59 52 98 c7 c6 fd 27 1f 04 02 f8 04 c3 3d 3f 66。

（3）计算加解密的效率，并进行一定的优化使加密效率提高。

【实验报告】

（1）简述 SMS4 加密算法密钥生成的步骤及加解密过程。

（2）SMS4 加密算法实现框图和源程序清单。

【思考题】

（1）分析 SMS4 在密码结构上与 DES、AES 有何异同。

（2）根据 SMS4 算法，编程研究 SMS4 的 S 盒的以下特性。

① 明文输入改变一位，密文输出平均改变多少位？

② S 盒输入改变一位，S 盒输出平均改变多少位？

③ L 输入改变一位，L 输出平均改变多少位？

④ 对于一个输入，连续施加 S 盒变换，变换多少次时出现输出等于输入？

（3）我国公布商用密码算法有何意义？