《第二章 安装和配置CryptoPP库》示例代码

作者：韩露露、杨波

日期：2019年3月1日

说明

本电子文档来源于书籍《深入浅出CryptoPP密码学库》，它最初被存放于GitHub上。任何人都可以复制、传播、使用本示例代码。

⇓

简介

《深入浅出CryptoPP密码学库》内容简介：

本书向读者介绍密码学库CryptoPP（或Crypto++）的使用方法和设计原理。CryptoPP是一个用C++语言编写的、开源的、免费的密码程序库，它最初由Wei Dai开发，现由开源社区维护。CryptoPP库广泛应用于学术界、开源项目、非商业项目以及商业项目，它几乎包括了目前已经公开的所有密码算法，支持当前主流的多种系统平台，并且具有良好的设计结构和较高的执行效率。

全书共15章，主要内容包括随机数发生器、Hash函数、流密码、分组密码、消息认证码、密钥派生和基于口令的密码、公钥加密系统、数字签名、密钥协商等，本书涵盖C++程序设计、设计模式、数论和密码学等知识。

本书最大的特点就是以应用为导向、以解决实际工程问题为目标，理论结合实践，将抽象的密码学变成保障信息安全的实际工具。

本书可以作为密码学、网络安全等专业在校学生的上机实验教材，也可以作为信息安全产品开发者、科研人员、密码算法实现者的参考手册。

⇓

资源

本书更多示例代码：https://github.com/locomotive-crypto
Crypto++网站：https://www.cryptopp.com/
Crypto++库GitHub地址：https://github.com/weidai11/cryptopp
Crypto++库SourceForge地址：https://sourceforge.net/projects/cryptopp/
Crypto++库Google论坛：
⇒公告通知地址：https://groups.google.com/forum/#!forum/cryptopp-announce
⇒用户群组地址：https://groups.google.com/forum/#!forum/cryptopp-users

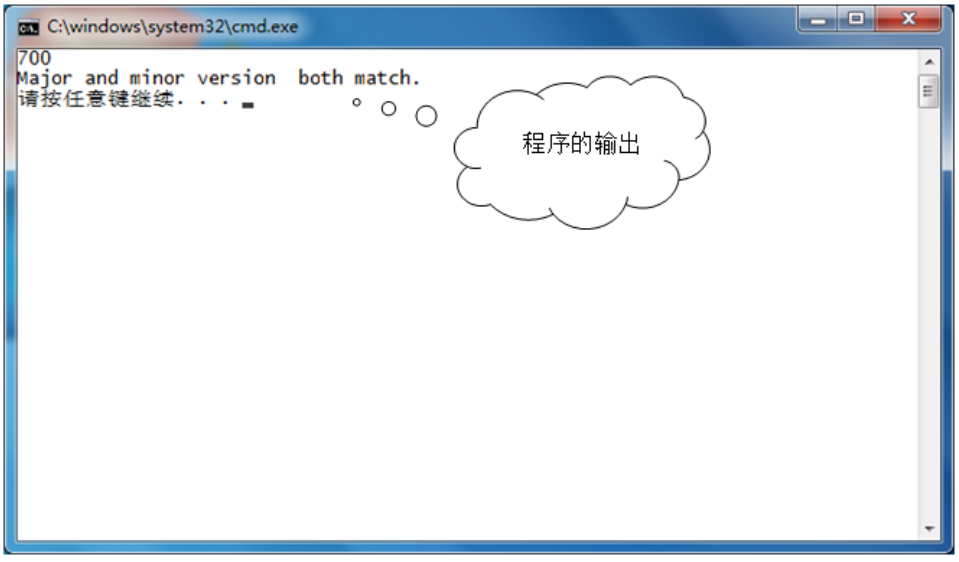
目录

1 测试代码

当按照本章所述的方法完成CryptoPP库的配置后，在Visual Studio 2015集成开发环境中输入如下测试代码：

```
#include<cryptlib.h> //CryptoPP库的头文件
#include<iostream> //使用cout、cin
using namespace std; //C++标准命名空间
using namespace CryptoPP; //CryptoPP库命名空间
int main()
{
    if (LibraryVersion() != HeaderVersion())
    {
        cout << "Potential version mismatch." << endl;
        const int lmaj = (LibraryVersion() / 100U) % 10;
        const int lmin = (LibraryVersion() / 10U) % 10;
        const int hmaj = (HeaderVersion() / 100U) % 10;
        const int hmin = (HeaderVersion() / 10U) % 10;
        if(lmaj != hmaj)
            cout << "Major version mismatch." << endl;
        else if(lmin != hmin)
            cout << "Minor version mismatch." << endl;
    }
    else
    {
        cout << LibraryVersion() << endl;
        cout << "Major and minor version  both match." << endl;
    }
    return 0;
}
```

若程序库配置正确，则本程序的输出结果如下图所示：



2 声明

Cryptography

⇓

⇓

⇓

此为《深入浅出CryptoPP密码学库》随书电子文档，它仅包含书籍中示例程序的源代码。关于示例代码的解释说明，详见书籍相应章节内容。

由于作者水平有限，错误之处在所难免。欢迎通过如下方式反馈相关问题：

⇒ QQ：1220195669

⇒ 微信：cc1220195669

⇓

⇓

⇓

《深入浅出CryptoPP密码学库》