《深入浅出CryptoPP密码学库》

作者：韩露露、杨波

日期：2019年3月1日

说明

本电子文档为《深入浅出CryptoPP密码学库》的目录，它最初被存放于GitHub上。

⇓

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 第1章CryptoPP库简介

2 第2章安装和配置CryptoPP库

3 第3章程序设计基础

3.1 C/C++基础知识

3.1.1 面向对象程序设计的常用概念

3.1.2 类（Class）和对象（Object）

3.1.3 类的数据成员（Data Member）和成员函数（Member Function）

3.1.4 继承（Inheritance）

3.1.5 类成员的访问属性（Access Property）

3.1.6 重载（Overloading）

3.1.7 构造函数（Constructor）和析构函数（Destructor）

3.1.8 类型转换（Type Cast）

3.1.9 多态性（Polymorphism）和虚函数（Virtual Function）

3.1.10 纯虚函数（Pure Virtual Function）和抽象类（Abstract Class）

3.1.11 传引用（By Reference）、传值（By Value）和传指针（By Pointer）

3.1.12 友元函数（Friend Function）和友元类（Friend Class）

3.1.13 内存分配（Allocate）和释放（Free）

3.1.14 模板（Template）

3.1.15 异常处理（Exception Handling）

3.1.16 命名空间（Namespace）

3.2 数据结构和算法

3.2.1 使用SecByteBlock类

3.3 面向对象的程序设计原则和设计模式

3.3.1 创建型模式（Creational Pattern）

3.3.2 结构型模式（Structural Pattern）

3.3.3 行为型模式（Behavioral Pattern）

3.3.4 其他模式（Other Pattern）

3.4 小结

4 第4章初识CryptoPP库

5 第5章随机数发生器（Random Number Generator）

6 第6章Hash函数（Hash Function）

7 第7章流密码（Stream Cipher）

8 第8章分组密码（Block Cipher）

9 第9章消息认证码（Message Authentication Code）

10 第10章密钥派生和基于口令的密码（Key Derivation and Password-based Cryptography）

11 第11章公钥密码数学基础

12 第12章公钥加密（Public Key Encryption）

13 第13章数字签名（Digital Signature）

14 第14章密钥协商（Key Agreement）

15 第15章建立安全信道

16 附录