<<密码学原理与实践>>

图书基本信息

书名：<<密码学原理与实践>>

13位ISBN编号：9787121090288

10位ISBN编号：7121090287

出版时间：2009年

出版时间：电子工业出版社

作者：[加]Douglas R.Stinson

页数：452

译者：冯登国

前言

2002年我组织相关专家翻译了Douglas R.Stinson所著的《密码学原理与实践》一书的第二版，本书翻译出版后在国内密码学界产生了很大的影响，反应很好。
凭我自己的学习经验，要掌握好一门课程，必须精读一两本好书，我认为本书是值得精读的一本。
2008年年初，电子工业出版社委托我翻译Douglas R.Stinson所著的《密码学原理与实践》一书的第三版，我通读了一遍本书，发现本书的前7章与第二版的几乎一样，只有细微差异，但新增加了7章内容，这些内容都很基础也很新颖，我受益匪浅，于是我花了大量时间翻译了本书，以供密码学爱好者参考。

本书是一本很有特色的教科书，具体表现在以下6个方面：　　1.表述清楚。
书中所描述的问题浅显易懂，如分组密码的差分分析和线性分析本是很难描述的问题，本书中以代替置换网络（SPN）作为数学模型表述得很清楚。

2.论证严谨。
书中对很多密码问题如唯一解距离、Hash函数的延拓准则等进行了严格的数学证明，有一种美感。

3.内容新颖。
书中从可证明安全的角度对很多密码问题特别是公钥密码问题进行了清楚的论述，使用了谕示器（Oracle）这一术语，通过阅读本书可使读者能够掌握这一术语的灵魂。
书中对一些最新领域，如组播安全、数字版权保护等也做了相应的介绍。

4.选材精良。
书中选择一些典型的、相对成熟的素材进行重点介绍，对一些正在发展的方向或需要大量篇幅介绍的内容以综述或解释的方式进行处理，特别适合于各种层次的教学使用。

5.覆盖面广。
几乎覆盖了密码学的所有核心领域以及部分前沿内容，通过阅读本书可以了解密码学的全貌。

6.习题丰富。
书中布置了大量的习题，通过演练这些习题可以熟练掌握密码学的基本技巧。

本书在翻译过程中，得到了很多老师的协助，张斌副研究员协助翻译了第8章、徐静副教授协助翻译了第9章、张振峰副研究员协助翻译了第10章、陈华副研究员协助翻译了第1l章、张立武副研究员协助翻译了第12章、林东岱研究员协助翻译了第13章、赵险峰副研究员协助翻译了第14章，全书由我统一统稿。
没有他们的鼎力相助，本书决不会这么快问世，在此对他们表示衷心的感谢。

本书的出版得到了国家973项目（编号：2007CB311202）和国家自然科学基金（编号：60673083）的支持，在此表示感谢。

<<密码学原理与实践>>

内容概要

本书是密码学领域的经典著作，被世界上的多所大学用做指定教科书。
本书在第二版的基础上增加了7章内容，不仅包括一些典型的密码算法，而且还包括一些典型的密码协议和密码应用。
全书共分14章，从古典密码学开始，继而介绍了Shannon信息论在密码学中的应用，然后进入现代密码学部分，先后介绍了分组密码的一般原理、数据加密标准（DES）和高级加密标准（AES）、Hash函数和MAC算法、公钥密码算法和数字签名、伪随机数生成器、身份识别方案、密钥分配和密钥协商协议、秘密共享方案，同时也关注了密码应用与实践方面的一些进展，包括公开密钥基础设施、组播安全和版权保护等。
在内容的选择上，全书既突出了广泛性，又注重对要点的深入探讨。
书中每一章后都附有大量的习题，这既利于读者对书中内容的总结和应用，又是对兴趣、思维和智力的挑战。
　本书适合于作为计算机科学、数学等相关学科的密码学课程的教材或教学参考书，同时也是密码学研究的必备参考书。

作者简介

Douglus R．Stinson博士：加拿大安大略省滑铁卢(Waterloo)大学计算机学院首席研究员。
目前的研究兴趣包括认证码、秘密共享、通用Hash函数、弹性函数、广播加密、密钥分配协议、组合设计理论等。

<<密码学原理与实践>>

书籍目录

章节摘录

在DES被作为一个标准提出时，曾出现许多批评，其中之一就是针对S盒。
DES中的所有计算，除了S盒，全是线性的，也就是说计算两个输出的异或与先将两个对应输入异或再计算其输出相同。
作为非线性部件，s盒对密码体制的安全性至关重要（在第1章中我们都看到了线性密码体制，如希尔密码是如何被一个已知明文攻击简单攻破的）。
在DES刚提出时，就有人怀疑S盒中隐藏了“陷门”，而美国国家安全局能够轻易地解密消息，同时还虚假地宣称DES是“安全”的。
当然无法否定这样一个猜测，然而到目前为止，并没有任何证据能证明DES中的确存在陷门。
事实上，后来表明DES中的S盒被设计成能够防止某些类型的攻击。
在20世纪90年代初，Biham与Shamir发现差分密码分析（在3.4节已经讨论过）时，美国国家安全局就已承认某些未公布的s盒设计准则正是为了使得差分密码分析变得不可行。
事实上，差分密码分析在DES最初被研发时就已为IBM的研究者所知，但这种方法却被保密了将近20年，直到Biham与Shamir又独立地发现了这种攻击。

<<密码学原理与实践>>

编辑推荐

《密码学原理与实践（第3版）》对那些保障海量信息在全球传递所需的方法和协议进行了全面深人的论述，在需要时提供了数学背景知识，密码体制的描述由更精确的伪代码给出并用示例来说明密码体制的工作过程。

Douglas R.Stinson博士：加拿大安大略省滑铁卢（waterloo）大学计算机学院首席研究员。

目前的研究兴趣包括认证码、秘密共享、通用Hash函数、弹性函数、广播加密、密钥分配协议、组合设计理论等。

冯登国博士：中国科学院软件所研究员、博士生导师，信息安全国家重点实验室主任，国家计算机网络入侵防范中心主任，国家信息化专家咨询委员会委员。

目前主要从事信息与网络安全方面的研究与开发工作。

《密码学原理与实践》自1995年第一次面世以来赢得了巨大的赞誉和广泛的欢迎，很快成为世界上多所大学的密码学课程指定教科书。

该书第二版也受到了同样的推崇，两个版本部成为了长盛不衰的畅销书。

现在这一权威的教科书推出了第三版，它将继续为未来密码学领域的新突破提供坚实的基础。

密码学科学与技术的演进已经经历了几千年。

如今。

史无前例的大量信息在全球传递，我们必须做好准备不断面对新的威胁并使用新的加密方案。

第三版根据密码学研究的最新进展更新了相关章节，分别涵盖以下内容： 密码学中的伪随机比特生成器 实体认证，包括从密码学本原建立的方案和特定意图的“ 雩知识 ”证明方案 密钥建立，包括密钥分配和密钥协商协议，这二者都大力强调了安全模型和证明 公钥基础设施，包括基于身份的密码学 秘密共享方案 多播安全，包括广播加密和版权保护

版权说明