《密码编码学与网络安全》

图书基本信息

书名：《密码编码学与网络安全》

13位ISBN编号：9787121033414

10位ISBN编号：7121033410

出版时间：2006-11

出版社：电子工业出版社

作者：斯托林斯

页数：486

《密码编码学与网络安全》

内容概要

William Stallings为读者提供了一本关千密码编码学与网络安全的最优秀书籍。

更新的第四版反映了该领域的最新发展趋势与进展，详尽讲述了密码编码学与网络安全的原理、技术与实践。首先，本书系统地解释了加密的概念与标准、密码、对称与公钥加密、数字签名等内容；接着探讨了网络安全的实践，为鉴别、电子邮件安全、IP安全以及Web安全引入了最新的应用；最后，本书回顾了系统安全的挑战，涉及到了主要的攻击与当今的最佳防范措施。像往常一样，本书提供了非常卓越的支持，包括大量的补充材料以及联机资源。

对学生、教师以及工程技术人员而言，本书仍是该领域的最佳资源。

本书系统地介绍了密码编码学与网络安全的基本原理和应用技术。全书主要包括下列四个部分：对称密码部分讨论了对称密码的算法和设计原理；公钥加密和散列函数部分讨论了公钥密码的算法和设计原理、报文认证码和散列函数的应用等；网络安全应用部分讨论了系统层的安全问题，包括电子邮件安全、IP安全以及Web安全等；系统安全部分讨论了入侵者和病毒造成的威胁及相应的对策、防火墙和可信系统的应用等。第四版与第三版相比，新增了Whirlpool，CMAC，DDoS以及CCITSE等内容，并对简化的AES，PKI等内容做了扩充。此外，对于基本内容的讲述方法也有许多变化和更新，并新增加了100多道习题。

本书可作为信息类专业高年级本科生与低年级研究生的教材，也可供从事信息安全、计算机、通信、电子工程等领域的科技人员参考。

《密码编码学与网络安全》

作者简介

斯托林斯（William Stallings）：计算机网络与体系结构方面成就卓著。他六次荣获由“教材与大学作者协会”颁发的“年度最佳计算机科学与工程教材”奖，作品包括《操作系统——精髓与设计原理》、《计算机组成与体系结构》、《数据与计算机通信》等。他是致力于密码学各个方面的学术期刊Cryptologia的编委会成员之一。目前他作为独立顾问为计算机硬件制造商、软件开发商和政府研究机构提供咨询服务。

《密码编码学与网络安全》

书籍目录

《密码编码学与网络安全》

精彩短评

1、习题很有趣，编码学入门一本不错的书
2、想看这本书的初衷是被一个Vendor的代码气笑了，不过想想自己关于安全的知识也并不成体系，于是复习了一遍。
3、。。。有很多东西看不懂><
4、教材
5、跟大家的感受一样 译的太烂
原版我给五星。
6、对网络安全领域有了了解
7、翟老
8、这个也讲了不少东西，但是某些密码学的东西还是感觉太难。什么椭圆曲线密码，不知道讲什么东西。
9、书一般，课不错。
10、算是不错的教材了 可以看的
11、虽然有错误，教材
12、翻译减一星……
13、作为入门还是不错的
14、其实我也是有很认真读过这本书的。虽然考的不好么...至少内容大多我还记得..
15、好书，入门就这一本足够！
16、密码学理论与应用，经典必读
17、.....
18、考试。。。竟然考的最简单的移位密码解密。。。崩溃。。。

19、有点问题
20、读了跟没读一样
21、对于初学者很有用
22、怀念我的本科毕业知道老师 就是他教的这门课
23、大学教材
24、全E文PPT与解说..
25、课本哎
26、景涛同好组都爱这本书！
27、对密码学的介绍很详细！
28、大学的一门课学的 很深入 专业

《密码编码学与网络安全》

章节试读

1、《密码编码学与网络安全》的笔记-第1页

已经买了书，还在路上。mark一下。

2、《密码编码学与网络安全》的笔记-第47页

两个概念：
扩散：明文的统计特征消散在密文中。
混淆：使密文和加密密钥间的统计关系更加复杂，阻止发现密钥。
Feistel具体实现的参数、特征：
分组长度：DES是64位，AES是128位。
密钥长度：越长，安全性越高，但加解密速度降低。
迭代轮数：典型值16
子密钥产生算法：越复杂，搞攻击越好。
两个考虑：
1.快速软件加解密
2.简化分析难度
加密公式：（笔记中如何输入角标？）还是先不输入了。

3、《密码编码学与网络安全》的笔记-第101页

密码学在于把规律地、明显地内容变幻为混淆、扩散的、非线性的内容，让大家不知道那到底是什么？
复杂系统科学，在于把世界的非线性的元素通过数学模型的方式来重新还原，做的是密码学的逆运算，相当于解密。
世界的变量是无量的，而科学家的模型再厉害，其也是有量的。以有量境界去猜度、计算无量世界，无异于孩童天真的想法，到头来一无是处。

这个世界还真是奇妙，有无数个学科，并且每个科学家们都在自己的学科里埋头苦干一辈子。到头来，世界该怎么发展还是怎么发展，科学再厉害，也左右不了世界其本身发展的命运历程。科学这东西，说白了无非是一个大系统里的一个小分支罢了。始终搞不明白真相的，只是科学家们找不到真相是不会善罢甘休的，因为找到真相是他们生命的意义。这个和哲学家是一样的。

还是佛说的究竟，“一切法从心想生”，人们头脑中的妄念不息，真相永远无法显现。

其实实相就在那里，只需息念。

4、《密码编码学与网络安全》的笔记-第55页

每组的外面两位实际上决定了.....这一段，看了半天才明白。主要是两个名词得明白，在前边可以找到。
代换：字母内容换成别的字母。例如：ABC 代换后为国 DED。
置换：内容内部变换位置。例如：左边32位，换成右边。 ABCD 置换后 CDAB

本页中表3.4(d)的作用也是思考了一会才明白：
迭代轮数和移位次数的作用实际上置换，就是把内容打乱的意思。

例如：ABCDEFG　第一轮移位后为：BCDEFGA　第二轮：CDEFGAB

雪崩效应：明文或密钥的微小改变将对密文产生很大的影响。我怎么感觉像是蝴蝶效应。

DES争论：密钥长度和算法安全性

1998年7月，造价不到25万美元的“ DES ”破译机破译了DES，花了不到三天的时间。并且，EFF引进了可以从明文堆里辨认明文的自动化方法。

计时攻击：给定的多种密文解密所需时间的观察，来获得关于密钥或明文的信息。

5、《密码编码学与网络安全》的笔记-第292页

感觉第三部分《网络安全应用》，第四部分《系统安全》，作者写的有些了了，没有密码学部分精彩，很多东西只是概念性的描述出来，没有象前面写的那些详细，所以读起来很是无趣，都没有动力再看下去了。

6、《密码编码学与网络安全》的笔记-第183页

公钥算法是基于数学函数而不是替换和转换公钥仅限于密钥管理和签名原因是公钥算法非常耗时，在现实中只能对少部分数据加密才是可行的。私钥是通信方在本地产生的，可保证通信的安全，相当于数学签名，用于认证源及数据完事性。
采用两次公钥，四次复杂的公钥算法，可满足保证性和认证的双重需要。

7、《密码编码学与网络安全》的笔记-第5页

就

8、《密码编码学与网络安全》的笔记-第134页

密码学看到这里才有了些眉目，算步入正轨了，虽然有些细节的算法自己仍然不是很明白，但大体的机制还是清晰的，能到达这一层的，我的学习目的也算达到了。
分组密码的工作模式
电码本：惟一密文，数据较少，有于密钥加密。
密文分组链接模式，一个初始向量IV，用于分组长度大于64位。
密文反馈模式：流密码无需明文长度是分组长度的整数位，可实时操作。
输出反馈模式：一个弱点可被攻击者利用，即密文中某位取反，明文也相应地取反。
计数器模式：硬件上，可并行处理多块加解密，增加吞吐量。软件，可利用处理品的流水线、时钟周期的多指令分派、大数量寄存器、SIMD指令等并行特征。预处理，加密盒子的输出，提高吞吐量。

9、《密码编码学与网络安全》的笔记-第34页

在二次大战中，德国(Enigma）密码机和日本（Purple)密码机都使用了基于转轮原理的密码机。盟军破译了这两种密码，对二战的结局产生了重要的影响　密码学的作用可见一斑。其实，肯定会有这一段故事电影，大家不妨去看看。

其实，对于课后的习题也挺感兴趣的，编写一个解决程序实现广义Caesar密码。通过编程，知识肯定能够得到巩固。
真的很佩服西方的教育，可惜被国人误解，成了填鸭式教育，悲催呀。

10、《密码编码学与网络安全》的笔记-第78页

看到有限域GF（p)这里，真的想了解那些数学家是怎样求解一个公式的，真的很有意思。如果有这方面的书籍就好了，详细介绍一些经典的数学公理是如何被发现的。
有限域就好比一个世界，数学家是规则的制定者（RULE)，有了规则，世界也就诞生了，就会衍生出许多现象，就象佛所说的“ 随缘妙用 ”，大道是相通的。

11、《密码编码学与网络安全》的笔记-第183页

- 非对称密码是一种密码体制, 其加密算法和解密算法使用不同的密钥: 一个是公钥, 一个是私钥. 非对称密码也称为公钥密码.

- 非对称密码用两个密钥中的一个以及加密算法将明文转换成密文. 用另一个密钥和解密算法从密文恢复出明文.

- 非对称密码可以用来保密, 认证或者上述两者的功能.

- 应用最广泛的公钥密码体制是RSA. 其攻击RSA的困难, 是基于寻找大因数的素因子的困难性.

公钥密码学的发展是整个密码学发展历史上最伟大的一次革命, 也许可以说是唯一的一次革命. 从密码学产生至今, 几乎所有的密码体制都是基于替换和置换这些初等方法.

任何加密方法的安全性依赖密钥的长度和破译密文所需要的计算量.

很多公钥密码体制的理论都基于数论.

公钥密码体制的6个组成部分:

- 明文
- 加密算法
- 公钥和私钥
- 密文
- 解密算法

通信各方均可访问公钥, 而私钥是各通信方在本地产生的, 所以不必要进行分配. 只要用户的私钥受到保护, 保持私密性, 那么通信就是安全的.

p188 公钥密码体制的应用可分为三类:
- 加密/解密: 发送方使用接收方的公钥对消息加密.
- 数字签名: 发送方用其私钥对消息"签名". 签名可以通过对整条消息加密或者对消息的一个小的数据块加密来产生, 其中该小数据块是整条消息的函数,

- 密钥交换: 通信双方交换会话密钥. 有几种不同的方法可用于密钥交换, 这些方法都使用了通信一方或者双方的私钥.

《密码编码学与网络安全》

版权说明