<<密码学与网络安全>>

图书基本信息

书名：<<密码学与网络安全>>

13位ISBN编号：9787302197270

10位ISBN编号：730219727X

出版时间：2009-4

出版时间：清华大学出版社

作者：福罗赞

页数：592

前言

互联网作为一个世界范围的通信网络，已经在许多方面改变了我们的日常生活。
一个最新的商业上的例子就是每个人都可以在线购物。
万维网（www）还可以让我们分享信息。
电子邮件的技术把世界各个角落的人联系在了一起。
这种必然的发展也形成了对互联网的依赖。
互联网作为一个开放的论坛，已经产生了一些安全方面的问题。
互联网需要有机密性、完整性和可信性。
人们需要确保网络通信是机密的。
当我们在线购物时，我们需要确保出售方是真实的。
当我们把交易请求发送给银行时，我们还要保证信息的完整性不被破坏。
网络安全其实就是可以让我们放心使用互联网的一系列协议——没有安全攻击。
最普通的可以为互联网提供安全的工具就是密码学，这是一门古老的技术，现在已经应用于网络安全了。
本书首先向读者介绍密码学的基本原理，然后应用这些基本原理来说明网络安全协议。
本书的特点本书的特点就是让读者更容易地理解密码学与网络安全。
结构本书增加了一些讲授密码学与网络安全的方法。
这些方法都是假定读者没有数论和抽象代数的知识。
如果没有这些领域的知识背景，我们就没法讨论密码学与网络安全，所以我们在第2章、第4章和第9章讨论了这几方面的内容。
如果读者对这几方面的内容熟悉的话，可以跳过这几章。
从第1～15章讨论密码学。
第16～18章讨论互联网的安全性。

<<密码学与网络安全>>

内容概要

本书作者Behrouz A. Forouzan运用一种易于理解的写作风格和直观的表述方法，为我们全面介绍了密码学与网络安全方面的概念。
他把难于理解的数学概念穿插在了中间的章节中，这样既为后面章节的学>-3打下必要的数学基础，又紧密结合密码学，使枯燥的数学概念变得妙趣横生。
本书以因特网为框架，详细地介绍了密码学、数据通信和网络领域的基础知识、基本概念、基本原理和实践方法，包含大量实践性强的程序，涵盖最新的网络安全技术，堪称密码学与网络安全方面的经典著作。
本书（包括其中文版）可作为大学本科信息安全类和通信类专业学生的教科书，也可作为有兴趣研究密码学与网络安全的读者的自学用书。

<<密码学与网络安全>>

书籍目录

章节摘录

插图：Improvement Let us improve on our first thought to get closer to the Feistel cipher.We know that we need to use the same input to the noninvertible element （the function）,but we don't want to use only the key. We want the input to the function to also be partof the plaintext in the encryption and part of the ciphertext in the decryption. The keycan be used as the second input to the function. In this way, our function can be a com-plex element with some keyless elements and some keyed elements. To achieve thisgoal, divide the plaintext and the ciphertext into two equal-length blocks, left and fight.We call the left block L and the right block R. Let the right block be the input to thefunction, and let the left block be exclusive-ored with the function output. We need toremember one important point: the inputs to the function must be exactly the same inencryption and decryption.This means that the fight section of plaintext in the encryp-tion and the fight section of the ciphertext in the decryption must be the same. In otherwords, the fight section must go into and come out of the encryption and decryptionprocesses unchanged. Figure 5.16 shows the idea.

编辑推荐

《密码学与网络安全(中文导读英文版)》为大学计算机教育国外著名教材系列之一。

<<密码学与网络安全>>

版权说明