<<密码学基础>>

图书基本信息

书名：<<密码学基础>>

13位ISBN编号：9787030212641

10位ISBN编号：7030212649

出版时间：2008-5

出版时间：科学出版社

作者：陈少真

页数：303

字数：371000

<<密码学基础>>

内容概要

本书全面讲解密码学的基本知识，在阐述密码理论的同时，还介绍了大量的算法和标准，特别在序列密码体制、分组密码体制和公开密钥密码体制的章节中，不仅介绍了经典的密码体制和算法，而且阐述了部分算法的安全性分析以及相关领域的最新研究成果，为使读者更好地掌握密码学知识，本书讲授必要的数学背景，并在附录中提供相关参考资料，以便读者进行相关研究，本书表达清晰、论证严谨、习题丰富。

本书可作为高等院校应用数学、通信和计算机等专业密码学、通信安全和网络安全等课程的教材或参考书，也可供信息安全系统设计开发人员、密码学和信息安全爱好者参考。

<<密码学基础>>

书籍目录

<<密码学基础>>

章节摘录

第1章　引论　　本章主要对密码学中的基本概念进行简要介绍，并对密码学中常用的一些符号和密码分析的类型加以说明，同时对密码学相关的信息论和计算复杂性基础知识加以阐述。

1.1密码学与信息安全概述　　研究信息的保密和复原保密信息以获取其真实内容的学科称为密码学（cryp—tology）。

它包括：　　密码编码学（cryptography）：研究对信息进行编码，实现隐蔽信息的一门学科。

密码分析学（cryptanalytics）：研究复原保密信息或求解加密算法与密钥的学科。

在邮政系统和信息的电气化传输发展以前，通信主要由秘密信使来完成。

然而信使有被抓获和叛变的可能，所以人们希望他们的通信不能为那些没有获得他们所提供的特殊的解密信息的人们所理解。

完成这一目的的技术就构成了密码编码学。

因此，密码编码学是一门使传递的信息只为预定的接收者所理解而不向他人泄漏的学科。

这里所说的信息包括文字、语音、图像和数据等一切可用于人们进行思想交流的工具。

密码的出现迫使人们使用这样或那样的方法去揭示使用了密码技术的保密通信的秘密。

当然，这一过程是在缺乏隐蔽此消息的密码技术的任何细节知识的情况下进行的。

完成这一目的的过程就构成了密码分析学，有时也称为破译或攻击。

因此，密码分析学是研究如何获得使用了密码技术的保密通信的真实内容的一门学科。

密码方法的使用和研究起源颇早。

四千多年以前，人类创造的象形文字就是原始的密码方法。

我国周朝姜太公为军队制定的阴符（阴书）就是最初的密码通信方式。

19世纪末，无线电的发明使密码学进入一个开始发展的时期。

这一时期密码的主要标志是以手工操作或机械操作实现的，通常称之为初等密码。

这类密码的编码思想是：要么错乱明文的顺序，要么用一个字母去替换另一个明文字母，要么用一组字母去替换另一组明文字母，要么对明文信息进行多次代替和置换，以达到文字加密的目的。

这一阶段始于20世纪之初，一直延续到20。

版权说明