全国信息技术人才培养工程指定培训教材
网络信息安全工程师高级职业教育系列教程

信息产业部电子教育与考试中心 组编
胡振宇 蒋建春 编著

密码学基础与安全应用

MIMAXUE JICHU YU ANQUAN YINGYONG

北京邮电大学出版社
www.buptpress.com

全国信息技术人才培养工程指定培训教材
网络信息安全工程师高级职业教育系列教程

密码学基础与安全应用

信息产业部电子教育与考试中心　组编
胡振宇　蒋建春　编著

北京邮电大学出版社
·北京·

内 容 简 介

本书是“网络信息安全工程师高级职业教育”证书认证考试人员的必备教程。本书参考和借鉴了广大网络信息安全人员的最新研究成果，吸收了网络信息安全最佳实践经验，并以作者自己在网络信息安全领域从事理论研究及技术创新的经历和体会，系统归纳总结了密码学网络安全应用所需知识和技能，同时给出了密码学网络安全应用的典型案例。本书主要内容包括密码学基础知识、对称加密算法、非对称加密算法、散列算法及其应用、数字签名、PKI 技术、SSL 、SSH 、IPSec 、PGP 加密文件系统等。

本书侧重于密码学网络安全技术应用，避免了深奥的理论证明。书中配有练习题。读者通过该书，能够快速地掌握职业所需要的密码学知识和安全技能。本书可以作为从事网络信息安全的广大技术人员和大专院校师生的参考用书，也可作为各类计算机信息技术培训和辅导教材。

图书在版编目(CIP)数据

密码学基础与安全应用/胡振宇，蒋建春编著．—北京：北京邮电大学出版社，2008

ISBN 978-7-5635-1591-2

Ⅰ．密… Ⅱ．①胡…②蒋… Ⅲ．①密码—理论—职业教育—教材②计算机网络—安全技术—职业教育—教材 Ⅳ．TN918.1 TP393.08

中国版本图书馆 CIP 数据核字(2008)第 050263 号

书　　名：密码学基础与安全应用

作　　者：胡振宇　蒋建春

责任编辑：崔　珞

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京忠信诚胶印厂

开　　本：787 mm×1 092 mm　1/16

印　　张：10.75

字　　数：26 千字

印　　数：1—5 000 册

版　　次：2008 年 10 月第 1 版　2008 年 10 月第 1 次印刷

ISBN 978-7-5635-1591-2　　定　价：22.00 元

序　言

当今世界，随着信息技术在经济社会各领域不断深化的应用，信息技术对生产力以至于人类文明发展的巨大作用越来越明显。党的“十七大”提出要“全面认识工业化、信息化、城镇化、市场化、国际化深入发展的新形势新任务”，“发展现代产业体系，大力推进信息化与工业化融合”，明确了信息化的发展趋势，首次鲜明地提出了信息化与工业化融合发展的崭新命题，赋予了我国信息化全新的历史使命。近年来，日新月异的信息技术呈现出新的发展趋势，信息技术与其他技术的结合更加紧密，信息技术应用的深度、广度和专业化程度不断提高。

我国的信息产业作为国民经济的支柱产业正面临着有利的国际、国内形势，电子信息产业的规模总量已进入世界大国行列。但是我们也清楚地认识到，与国际先进水平相比，我们在产业结构、核心技术、管理水平、综合效益、普及程度等方面，还存在较大差距，缺乏创新能力与核心竞争力，“大”而不强。国际国内形势的发展，要求信息产业不仅要做大，而且要做强，要从制造大国向制造强国转变，这是信息产业今后的重点工作。要实现这一转变，人才是基础。机遇难得，人才更难得，要抓住本世纪头二十年的重要战略机遇期，加快信息行业发展，关键在于培养和使用好人才资源。《中共中央、国务院关于进一步加强人才工作的决定》指出，人才问题是关系党和国家事业发展的关键问题，人才资源已成为最重要的战略资源，人才在综合国力竞争中越来越具有决定性意义。

为抓住机遇，迎接挑战，实施人才强业战略，信息产业部启动了“全国信息技术人才培养工程”。该项工程旨在通过政府政策引导，充分发挥全行业和全社会教育培训资源的作用，建立规范的信息技术教育培训体系、科学的培训课程体系、严谨的信息技术人才评测服务体系，培养造就大批行业急需的、结构合理的高素质信息技术应用型人才，以促进信息产业持续快速协调健康发展。

由各方专家依据信息产业对技术人才素质与能力的需求，在充分吸取国内外先进信息技术培训课程优点的基础上，信息产业部电子教育与考试中心精心组织编写了信息技术系列培训教材。这些教材注重提升信息技术人才分析问题和解决问题的能力，对各层次信息技术人才的培养工作具有现实的指导意义。我们谨向参与本系列教材规划、组织、编写同志们致以诚挚的感谢，并希望该系列教材在全国信息技术人才培养工作中发挥有益的作用。

信息产业部电子教育与考试中心

前　言

密码学的历史源远流长，但长期以来它只在很少的范围内（如军事、外交、情报等部门）使用，因而对一般人来说是陌生的。再加上它常常涉及晦涩的数学知识，因而它显得古老而深奥。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。随着互联网发展和信息技术的普及，网络和信息技术已经日渐深入到日常生活和工作当中。密码学及应用技术在一个以信息化为主要特征的时代中将发挥越来越重要的作用。

本书是“网络信息安全工程师高级职业教育（Network Security Advanced Career Education，NSACE）项目的必备教材。通过对本书的学习，读者既可以了解到密码学的基本原理和常用加密方法，又能掌握将常用的密码技术应用到实际中的最佳技巧。本书主要章节内容如下。

第1章，密码学基础知识。这一章向读者介绍密码系统的组成、密码学相关术语、密码系统的分类方法、密码系统的常见攻击类型及破译等级。同时，还介绍密码学的主要应用方向。

第2章，对称加密算法。这一章内容主要是关于DES、IDEA和AES的工作原理、实现方法以及安全性评价。除此之外，这一章还详细讲解了分组密码常用工作模式。

第3章，非对称加密算法。这一章讲解了非对称加密算法与对称加密算法区别特点。帮助读者了解RSA、ElGamal及椭圆曲线密码体制的工作原理。这一章也介绍了RSA算法的主要缺点。

第4章，散列算法及其应用。本章内容是散列算法的安全要求、散列算法的一般构造原理，并着重介绍了MD5算法和SHA-1算法的工作过程。

第5章，数字签名。介绍散列算法在消息认证方面的应用。读者可以了解数字签名的概念及其安全性要求，理解数字签名的一般过程和工作机制。了解用RSA算法、ElGamal算法以及椭圆曲线算法实现数字签名和软件版权保护的原理。

第6章，PKI技术。在这一章主要介绍了PKI技术的服务内容、PKI技术的体系结构以及PKI技术的应用。

第7章，SSL。本章内容包括SSL协议的组成部分、SSL提供的安全服务种

类、SSL 的工作原理和实际应用。

第 8 章，SSH。本章内容介绍了 SSH 协议的组成部分、SSH 提供的安全服务种类、SSH 的工作原理和实际应用。

第 9 章，IPSec。本章内容是关于 IPSec 协议的组成部分、IPSec 提供的安全服务种类、IPSec 的工作原理和实际应用。

第 10 章，PGP。本章内容讲解 PGP 的安全功能及工作机制，也介绍了 PGP 的实例应用。

第 11 章，加密文件系统。主要介绍了 Windows 加密文件系统(EFS)的工作原理、适用条件以及 EFS 的使用操作。

第 12 章，密码系统的安全测试与评价。这一章主要介绍了密码系统的设计原则。读者可以了解加密系统检测的主要方面和对密码系统的评价要素。

最后，本书还包括一个附录，这是本书中涉及的加密算法的源代码。读者可以到 NSACE 网站(http://www.nsace.org.cn)上下载这些源代码，以结合相应内容进行学习。

在本书的写作与出版过程中，首先感谢卿斯汉老师、冯登国老师的指导。作者感谢参考资料作者以及网上安全论坛中的网友所提供的资料，由于篇幅受限，所用到的参考资料不能一一列举，敬请谅解。作者也要感谢网康科技有限公司首席执行官袁沈钢对 NSACE 项目热情支持。作者特别感谢盛晨媛女士和杜志海先生，在本书写作过程中给出许多宝贵指导意见，为本书的顺利出版付出了大量心血。

本书是作者在网络信息安全职业教育领域工作中的尝试，编写过程力求突出职业教育特点。由于作者水平有限，书中如果有不当之处，希望广大读者不吝赐教。

作 者

目　　录

第 1 章　密码学基础知识

1.1　密码系统的组成 …… 1
1.2　密码学相关术语 …… 2
1.3　加密算法的分类 …… 3
1.3.1　对称加密算法 …… 3
1.3.2　公钥加密算法 …… 4
1.4　常见密码分析的攻击类型 …… 5
1.5　密码算法的破译等级 …… 6
1.6　本章小结 …… 6
1.7　本章练习 …… 6

第 2 章　对称加密算法

2.1　DES 算法 …… 8
2.1.1　DES 加密 …… 8
2.1.2　DES 解密 …… 9
2.1.3　DES 实现过程分析 …… 9
2.2　IDEA 算法 …… 16
2.2.1　IDEA 算法简介 …… 16
2.2.2　算法框架 …… 16
2.2.3　评价 …… 18
2.3　AES 算法 …… 18
2.3.1　AES 加密 …… 18
2.3.2　AES 解密 …… 19
2.4　分组密码的工作模式 …… 19
2.4.1　电码本模式 …… 20
2.4.2　密码分组链模式 …… 20
2.4.3　密码反馈模式 …… 20
2.4.4　输出反馈模式 …… 21
2.4.5　计数器模式 …… 21
2.5　对称加密算法的典型应用 …… 21

2.6 本章小结…… 26
2.7 本章练习…… 27

第 3 章 非对称加密算法

3.1 RSA 算法 …… 29
3.1.1 RSA 算法描述 …… 29
3.1.2 RSA 的安全性 …… 31
3.1.3 RSA 的主要缺点 …… 32
3.2 ElGamal 算法…… 32
3.3 椭圆曲线加密算法…… 33
3.3.1 密码学中的椭圆曲线…… 33
3.3.2 椭圆曲线上的加法运算…… 33
3.3.3 椭圆曲线上简单的加/解密 …… 36
3.4 对称和非对称加密算法的综合应用…… 37
3.5 非对称加密算法的典型应用…… 38
3.6 本章小结…… 39
3.7 本章练习…… 39

第 4 章 散列算法及其应用

4.1 散列算法…… 42
4.1.1 散列函数的属性…… 42
4.1.2 散列函数的构造方式…… 42
4.1.3 典型散列算法…… 43
4.2 MD5 算法原理分析 …… 43
4.2.1 基本描述…… 44
4.2.2 MD5 的非线性轮函数 …… 45
4.2.3 MD5 相对 MD4 所作的改进…… 47
4.2.4 关于 MD5 和 SHA-1 安全性的最新进展 …… 47
4.3 散列算法的典型应用…… 48
4.3.1 用 MD5 校验和实现文件完整性保护 …… 48
4.3.2 文件系统完整性保护…… 49
4.3.3 身份鉴别…… 49
4.3.4 网页自动恢复系统…… 49
4.4 本章小结…… 50
4.5 本章练习…… 50

第 5 章 数字签名

5.1 数字签名…… 55
5.1.1 基本概念…… 55

5.1.2 数字签名的工作机制…… 56
5.2 数字签名的实现技术…… 56
5.2.1 利用 RSA 算法实现数字签名 …… 56
5.2.2 利用 ElGamal 算法实现数字签名 …… 57
5.2.3 利用椭圆曲线算法实现数字签名…… 58
5.3 数字签名的应用案例…… 59
5.3.1 椭圆曲线算法在软件保护中的应用…… 59
5.3.2 电子印章…… 60
5.4 本章小结…… 61
5.5 本章练习…… 61

第 6 章 PKI 技术

6.1 PKI 技术概述…… 63
6.2 PKI 技术的安全服务及意义…… 64
6.2.1 PKI 技术的安全服务…… 64
6.2.2 PKI 技术的意义…… 65
6.3 PKI 技术的标准及体系结构…… 66
6.3.1 PKI 技术的标准…… 66
6.3.2 PKI 技术的体系结构…… 67
6.4 PKI 技术的应用与发展…… 69
6.4.1 PKI 技术的应用…… 69
6.4.2 PKI 技术的发展…… 71
6.5 Windows Server 2003 PKI 的证书管理 …… 72
6.5.1 添加证书模板…… 73
6.5.2 委托证书模板管理…… 73
6.5.3 颁发证书…… 74
6.5.4 吊销证书…… 74
6.6 本章小结…… 75
6.7 本章练习…… 75

第 7 章 SSL

7.1 SSL 协议概述 …… 77
7.2 SSL 协议体系结构分析 …… 78
7.2.1 SSL 协议的体系结构 …… 78
7.2.2 SSL 的记录协议 …… 79
7.2.3 SSL 的握手协议 …… 79
7.3 OpenSSL 协议的工作过程 …… 81
7.3.1 OpenSSL 概述 …… 81
7.3.2 OpenSSL 的工作过程 …… 81

7.4 OpenSSL 网站应用 …… 83
7.4.1 网站安全需求分析 …… 83
7.4.2 OpenSSL 的安装 …… 83
7.5 Windows 2000 中 SSL 的配置与应用 …… 86
7.6 SSL VPN …… 89
7.6.1 VPN 概述 …… 89
7.6.2 SSL VPN 的工作原理 …… 89
7.6.3 SSL VPN 的技术特点 …… 90
7.6.4 SSL VPN 的实际应用 …… 91
7.7 本章小结 …… 92
7.8 本章练习 …… 92

第 8 章 SSH

8.1 SSH 概述 …… 94
8.2 SSH 协议的基本框架 …… 95
8.3 SSH 的工作原理 …… 95
8.4 SSH 的身份认证机制 …… 97
8.5 SSH 的应用分析 …… 98
8.6 OpenSSH 应用实例 …… 99
8.6.1 OpenSSH 简述 …… 99
8.6.2 OpenSSH 的安装 …… 99
8.6.3 使用基于传统口令认证的 OpenSSH …… 100
8.6.4 配置并使用基于密钥认证的 OpenSSH …… 100
8.7 Windows 平台下 SSH 的应用实例 …… 102
8.7.1 安装 F-Secure SSH 软件 …… 102
8.7.2 SSH 服务器端的设置 …… 102
8.7.3 客户端的设置与连接 …… 104
8.7.4 应用举例 …… 106
8.8 本章小结 …… 107
8.9 本章练习 …… 107

第 9 章 IPSec

9.1 IPSec 的体系结构 …… 109
9.1.1 AH 协议结构 …… 109
9.1.2 ESP 协议结构 …… 110
9.1.3 ESP 隧道模式和 AH 隧道模式 …… 111
9.1.4 AH 和 ESP 的综合应用 …… 112
9.2 IPSec 的应用分析 …… 113
9.3 Linux 环境下 IPSec 的应用实例 …… 113

9.3.1 手动密钥管理 …… 114
9.3.2 自动密钥管理 …… 117
9.3.3 建立 IPSec 安全隧道 …… 124
9.4 Windows 2000 下基于 IPSec 的 VPN …… 125
9.4.1 Windows 2000 中 IPSec 的配置 …… 125
9.4.2 测试 IPSec 策略 …… 129
9.5 本章小结 …… 130
9.6 本章练习 …… 130

第 10 章 PGP

10.1 电子邮件安全需求 …… 132
10.2 PGP 的工作机制 …… 132
10.2.1 PGP 的安全服务 …… 132
10.2.2 加密密钥和密钥环 …… 134
10.2.3 公钥的管理机制 …… 134
10.3 PGP 的应用实例 …… 135
10.3.1 PGP 的安装 …… 135
10.3.2 生成密钥 …… 136
10.3.3 加密、解密应用 …… 138
10.4 本章小结 …… 139
10.5 本章练习 …… 140

第 11 章 加密文件系统

11.1 Windows 加密文件系统概述 …… 141
11.2 EFS 的工作原理 …… 141
11.3 EFS 的组成 …… 142
11.4 EFS 与 NTFS 对文件保护的关系 …… 142
11.5 EFS 的优势和局限 …… 143
11.6 EFS 的设置 …… 144
11.7 EFS 的恢复代理 …… 144
11.8 EFS 操作实例 …… 144
11.8.1 加密和解密文件与文件夹 …… 144
11.8.2 复制和移动加密文件 …… 145
11.8.3 与其他用户共享加密文件 …… 146
11.8.4 备份证书和私钥 …… 146
11.8.5 指定恢复代理 …… 147
11.8.6 禁止加密功能 …… 148
11.8.7 注意事项 …… 149
11.9 EFS 使用方法小结 …… 150

11.10 本章小结 …… 151
11.11 本章练习 …… 151

第 12 章 密码系统的安全测试与评价

12.1 密码算法的安全性检测 …… 153
12.1.1 数据变换有效性测试 …… 153
12.1.2 算法对明文的扩散性检验 …… 154
12.1.3 密钥更换的有效性检验 …… 155
12.1.4 线性复杂度检验 …… 155
12.2 密码系统的评价 …… 155
12.2.1 保护程序与应用需求相符合 …… 155
12.2.2 对安全性的信心要建立在密码体制所依据的困难问题上 …… 156
12.2.3 实际效率 …… 156
12.2.4 采用实际可用的原型和服务 …… 156
12.2.5 明确性 …… 157
12.2.6 开放性 …… 157
12.3 本章小结 …… 157
12.4 本章练习 …… 157
参考文献 …… 158

第1章　密码学基础知识

学习目标

* 了解密码系统的组成，掌握密码学相关术语的含义。
* 了解密码系统的分类方法、密码系统的常见攻击类型及破译等级。
* 了解密码学的应用方向。

密码学以研究秘密通信为目的，即研究对传输信息采取何种变换以防止第三者对有效信息的窃取。密码学是一门古老而深奥的学科，它对一般人来说是陌生的，因为长期以来，它只在很少的范围(如军事、外交、情报等部门)内使用。计算机密码学是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。随着计算机网络和计算机通信技术的发展，计算机密码学得到前所未有的重视并迅速普及和发展起来。目前，它已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。

密码是隐蔽语言、文字、图像等信息的特种符号。凡是用特种符号按照通信双方约定的方法把通信内容的原形隐蔽起来，不为第三者所识别的通信方式称为密码通信。密码学主要关注的对象是加密和解密方法。加密即按某种方式将要发送的消息转换成看起来毫无意义的符号，而解密是指授权接收者可通过相应的方法将这些看起来毫无意义的符号还原成原来的信息，以获取发送者的消息内容，而非授权者从这些文字中得不到任何有用的信息。在计算机通信中，采用密码技术将信息隐蔽起来，再将隐蔽后的信息传输出去，使信息在传输过程中即使被窃取或截获，窃取者也不能了解信息的内容，从而保证信息传输的安全。

1.1　密码系统的组成

任何一个加密系统至少包括下面4个组成部分：

(1) 未加密的消息，也称明文。

(2) 加密后的消息，也称密文。

(3) 加密解密设备或算法。

(4) 加密解密的密钥。

根据加密、解密时使用的密钥是否相同，可将加密算法分为两种：对称加密算法和非对称加密算法。

1.2 密码学相关术语

1. 发送者和接收者

发送者即为消息的最初构造者，是传送消息的起始点。假设发送者想发送消息给接收者，且想安全地发送信息，亦即他想确信偷听者不能阅读发送的消息，通常要在消息被发送之前采用某种方法对消息进行加密变换，然后将加密后的密文发送出去。接收者是指一条被发送的消息的目的地。通常是授权的可以正确处理加密消息的人或设备。

2. 消息、加密和密文

消息被称为明文。用某种方法伪装消息以隐藏它的内容的过程称为加密，加了密的消息称为密文，而把密文转变为明文的过程称为解密。

在密码学领域中，明文通常用 M(Message)或 P(Plaintext)来表示。由于涉及计算机，它可能是简单的二进制数据，或是比特流(文本文件、位图、数字化的语音流或数字化的视频图像)。明文可被传送或存储，无论是哪种情况，M 指待加密的消息。

密文用 C(Ciphertext)表示，它也是二进制数据，有时和 M 一样大，有时稍大(通过压缩和加密的结合，C 有可能比 P 小些。然而，单单加密通常不能使 C 比 P 小)。加密函数 E(Encrypt)作用于 M 得到密文 C，用数学公式表示为

$$E(M)=C$$

相反地，解密函数 D(Decrypt)作用于 C 产生 M，用数学公式表示为

$$D(C)=M$$

先加密后再解密消息，原始的明文将恢复出来，等式

$$D[E(M)]=M$$

必须成立。

3. 算法和密钥

密码算法是指用于加密和解密的数学函数(通常情况下，有两个相关的函数中一个用作加密，另一个用作解密)。

如果算法的保密性是基于保持算法的秘密，这种算法称为受限制的算法。受限制的算法具有历史意义，但按现在的标准，它们的保密性已远远不够。大的或经常变换的用户组织不能使用它们，因为每有一个用户离开这个组织，其他的用户就必须改换另外不同的算法。如果有人无意暴露了这个秘密，所有人都必须改变他们的算法。

更糟的是，受限制的密码算法不可能进行质量控制或标准化。每个用户组织必须有他们自己的唯一算法。这样的组织不可能采用流行的硬件或软件产品。但窃听者却可以买到这些流行产品并学习算法，于是用户不得不自己编写算法并予以实现，如果这个组织中没有好的密码学家，那么他们就无法知道他们是否拥有安全的算法。

尽管有这些主要缺陷，受限制的算法对低密级的应用来说还是很流行的，用户或者没有认识到或者不在乎他们系统中内在的问题。

现代密码学用密钥解决了这个问题，密钥用 K(Key)表示。K 可以是很多数值里的任意值。密钥 K 的可能值的范围叫做密钥空间。加密和解密运算都使用这个密钥(即运算都依赖于密钥，并用 K 作为下标表示)，这样，加/解密函数现在变成

$$E_K(M)=C$$

$$D_K(C)=M$$

这些函数具有下面的特性：

$$D_K[E_K(M)]=M$$

有些算法使用不同的加密密钥和解密密钥，也就是说加密密钥 PK(Public Key，通常是公开的密钥)与相应的解密密钥 SK(Secret Key，通常是保密的密钥)不同，在这种情况下：

$$E_{PK}(M)=C$$

$$D_{SK}(C)=M$$

$$D_{SK}[E_{PK}(M)]=M$$

所有这些算法的安全性都基于密钥的安全性；而不是基于算法的细节的安全性。这就意味着算法可以公开，也可以被分析，可以大量生产使用算法的产品，即使偷听者知道用户的加密算法也没有关系；只要窃听者不知道用户使用的具体密钥，他就不可能获得用户消息的有效内容。

4. 协议

如果一个加密算法必须由多个(多于两个)实体共同参与才能完成，则称之为一个密码协议。协议是一组适当定义的、在多个实体间执行的一组规则。这里的必要前提是多个实体共同参与执行。如果一组规则仅由一个实体执行，则它只是一种程序，而不能称之为协议。

除了提供机密性外，密码学通常还有以下的作用：

(1) 鉴别。消息的接收者应该能够确认消息的来源；入侵者不可能伪装成他人。

(2) 完整性检验。消息的接收者应该能够验证在传送过程中消息没有被修改；入侵者不可能用假消息代替合法消息。

(3) 抗抵赖。发送者一旦发送出一个消息，事后不可能虚假地否认他曾经发送的消息。

1.3 加密算法的分类

根据加密和解密所用的密钥是否相同，可将密码算法分为对称加密算法和非对称加密算法(也称公钥加密算法)两类。

1.3.1 对称加密算法

对称加密算法有时又叫传统加密算法，就是加密密钥能够从解密密钥中推算出来，反过来也成立。在大多数对称加密算法中，加/解密密钥是相同的。这些算法也叫私钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称加密算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加/解密。只要通信需要保密，密钥就必须保密。

对称加密算法的加密和解密表示为

$$E_K(M)=C$$

$$D_K(C)=M$$

对称加密算法可分为两类。一次只对明文中的单个比特(有时对单个字节)运算的算法称为序列算法或序列密码,也称为流密码。另一类算法是对明文的一组比特并行运算,这些比特组称为分组,相应的算法称为分组算法或分组密码。现代计算机密码算法的典型分组长度为 64 bit,这个长度大到足以防止分析破译,但又小到足以方便使用的程度(在计算机出现前,密码算法通常每次只对明文的一个字符运算,可认为是序列密码对字符序列的运算)。

对于使用对称加密算法进行安全通信的双方来说,他们必须拥有相同的密钥而且不能让其他人知道。如果他们处在不同的物理位置,必须使用信使、加密电话或者其他的安全通信介质,防止密钥在传输过程中泄露。在消息的传输过程中,偷听或截获到密钥的任何人,就能够阅读、修改和伪造用这个密钥加密或认证的所有信息。无论采用何种算法,对称加密算法的永恒问题就是密钥的发布,也就是怎样才能使接收者得到密钥而不被其他人截获。

1.3.2 公钥加密算法

公钥加密算法可以解决密钥发布的问题,公钥的概念由 Whitfield Diffie 和 Martin Hellman 在 1975 年提出(现在有证据表明英国情报机关先于 Diffie 和 Hellman 几年发明了这种方法,但是却作为军事秘密,而且在用公钥加密算法解决密钥发布的问题没有进行实质性的工作)。

公钥加密算法是这样设计的:用作加密的密钥不同于用作解密的密钥,而且解密密钥不能根据加密密钥计算出来(至少在合理假定的长时间内)。之所以叫做公钥加密算法,是因为加密密钥能够公开,陌生者也能用加密密钥加密信息,但只有用相应的解密密钥才能解密信息。

在公钥加密算法中,用于加密的密钥称为是公钥(Public Key),是公开的。用于解密的密钥称为是私钥(Secret Key 或 Private Key),是用户保密的。想从公钥推导出私钥在计算上是不可行的。拥有公钥的人可以加密信息却不能将其解密,只有拥有对应私钥的人才能解密信息。

用公钥 PK 加密表示为

$$E_{PK}(M)=C$$

用相应的私钥 SK 解密可表示为

$$D_{SK}(C)=M$$

有时人们将消息用私钥 SK 加密而用公钥 PK 解密,以表示消息发送方对该消息的数字签名。此时,这些运算可分别表示为

$$E_{SK}(M)=C$$

$$D_{PK}(C)=M$$

一般来说,公钥密码算法的速度比对称密码算法要慢得多,这使得公钥密码算法在大数据量的加密应用中受到限制。公钥加密算法的主要优势在于可以让事先没有安全通道的通

信双方可以安全地交换信息。收、发双方通过安全通道共享密钥的前提条件不存在了。所有的通信中只包含了公钥，私钥是不会传输或共享的。

由于对称加密算法曾经是传送秘密信息的唯一手段，保持安全通道和发布密钥的高昂费用将其应用范围限制在如政府或者大银行这样少数的用户中。公钥加密算法是加密技术的革命，它可以为普通人提供强加密手段。

1.4　常见密码分析的攻击类型

对密码进行分析的尝试称为攻击(Attack)，其目的是恢复出消息明文、密钥或其他有价值的信息。密码分析也可以发现密码体制的弱点，最终得到上述结果。假定分析者知道所用的加密算法的全部知识，常见的密码分析攻击有 4 类。

1. 唯密文攻击(Ciphertext-only Attack)

密码分析者有一些消息的密文，这些消息都用同一加密算法和密钥加密。密码分析者的任务是尽可能多地恢复明文或推算出密钥。其形式化描述为：已知 $C_1=E_K(P_1)$，$C_2=E_K(P_2)$，…，$C_i=E_K(P_i)$，推导出 P_1，P_2，…，P_i 以及 K 或找出一个算法从 $C_{i+1}=E_K(P_{i+1})$ 推导出 P_{i+1}。

2. 已知明文攻击(Known-plaintext Attack)

密码分析者不仅可以得到一些消息的密文，而且也知道这些密文对应的明文本身。其任务是用加密信息推导出用来加密的密钥或导出一个算法，以便对用同一密钥加密的任何新密文进行解密。其形式化描述为：已知 P_1，$C_1=E_K(P_1)$，P_2，$C_2=E_K(P_2)$，…，P_i，$C_i=E_K(P_i)$，推导出密钥 K 或找出一个算法从 $C_{i+1}=E_K(P_{i+1})$ 推导出 P_{i+1}。

显然，已知明文攻击比唯密文攻击的能力更强，敌手掌握的有关该密码的信息也更多。

3. 选择明文攻击(Chosen-plaintext Attack)

密码分析者不仅可以获得若干密文及其相应的明文，而且还可以选择被加密的明文。因为明文是经过选择的，必然提供了更多的可被利用的信息，其攻击力更强。其形式化描述为：已知 P_1，$C_1=E_K(P_1)$，P_2，$C_2=E_K(P_2)$，…，P_i，$C_i=E_K(P_i)$，其中 P_i 可由密码分析者自行选择，推导出密钥 K 或找出一个算法从 $C_{i+1}=E_K(P_{i+1})$ 推导出 P_{i+1}。

4. 选择密文攻击(Chosen-ciphertext Attack)

密码分析者能自行选择不同的被加密的密文，并可得到相应的解密明文，其形式化描述为：已知 C_1，$P_1=D_K(C_1)$，C_2，$P_2=D_K(C_2)$，…，C_i，$P_i=D_K(C_i)$，其中 C_i 可由密码分析者自行选择，推导出密钥 K 或找出一个算法从 $C_{i+1}=E_K(P_{i+1})$ 推导出 P_{i+1}。

对于以上的选择明文攻击和选择密文攻击，还有相应的自适应性攻击。在选择明文攻击时，密码分析者还可根据前面的结果，调整自己对要加密的明文消息的选择，称为自适应性选择明文攻击(Adaptive-chosen-plantext Attack)。对于选择密文攻击，密码分析者则可根据前面的结果，调整自己对要解密的密文的选择，称为自适应性选择密文攻击(Adaptive-chosen-ciphertext Attack)。在以上的各种攻击方法中，自适应性选择密文攻击的能力最强。通常所说的选择明文攻击及选择密文攻击均指自适应性选择明文攻击及自适应性选择密文攻击。