数据加密解密技术

杨　静　张天长　主编

WUHAN UNIVERSITY PRESS
武汉大学出版社

数据加密解密技术

杨　静　张天长　主编

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

数据加密解密技术/杨静,张天长主编.—武汉:武汉大学出版社,2017.5

ISBN 978-7-307-19281-2

Ⅰ.数… Ⅱ.①杨… ②张… Ⅲ.①密码—加密技术 ②密码—解密译码 Ⅳ.TN918.4

中国版本图书馆 CIP 数据核字(2017)第 090495 号

责任编辑:叶玲利 责任校对:李孟潇 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:湖北恒泰印务有限公司

开本:787×1092 1/16 印张:14.5 字数:342 千字 插页:1

版次:2017 年 5 月第 1 版 2017 年 5 月第 1 次印刷

ISBN 978-7-307-19281-2 定价:42.00 元

版权所有,不得翻印;凡购我社的图书,如有质量问题,请与当地图书销售部门联系调换。

前　言

在当今社会，信息主导并改变着社会活动的方方面面，因此，信息安全问题显得尤为重要。信息安全问题涉及国家安全、社会公共安全，直接关系到世界各国重大国家利益；信息安全问题是互联网经济的制高点，也是推动互联网、电子政务和电子商务发展的关键。因此，研究和发展信息安全技术是当前社会的迫切要求。信息安全涉及很多技术和知识，密码技术是其中一个重要的组成部分。由密码学发展起来的密码技术，不仅大量应用于军事、政治、经济领域，同时也构成了整个信息安全技术体系的理论基础。由于计算机及网络使用的日益深入和广泛，密码技术的重要性也越来越突出。为了培养高素质的网络安全与执法人才，切实加强网络安全与执法专业建设，在湖北警官学院教材编写委员会的大力支持下，信息技术系组织专门力量编写了《数据加密解密技术》一书。本书从信息安全技术体系出发，对密码学、密码技术、加密解密技术等理论知识进行了详细的阐述，重点介绍了数据加密解密技术的实战应用，包括各种加密解密方法和相关软件的使用，以及加密解密技术在网络中的应用。本书适用于网络安全与执法专业的学生，也可以作为从事该方面工作人员的参考书。

本书由杨静、张天长主编，杨静负责全书的架构设计和内容统编，全部书稿由张天长审定。其中第一章由张天长编写，第二章由罗世奇编写，第三章由黄凤林编写，第四章由龚德忠编写，第五、六、七、八、九章由杨静编写。该书的编写得到了湖北省教育厅人文社会科学研究项目“信息化时代社会治安管理研究”（项目编号：16Y144）、湖北省教育厅科研重点项目“‘互联网+’环境下网络虚拟社会秩序管控体系研究”（项目编号：D20164202）和2017年湖北省自然科学基金项目“深度学习的Android恶意代码检测与分析”（项目编号：2017CFB745）的大力支持。

数据的加密与解密技术涉及范围广泛，发展快速，我们在编写过程中参考了许多作者的研究资料，并在附录的参考文献中一一列出，在此表示深深的感谢。由于编者水平有限，书中存在着或多或少的不足之处，希望读者不吝赐教。

编　者

2017年3月

目　录

1　信息安全技术体系中的密码学 …… 1
1.1　信息安全技术基础理论 …… 1
1.1.1　信息 …… 1
1.1.2　信息论 …… 1
1.1.3　信息安全保障 …… 2
1.1.4　信息安全发展 …… 2
1.2　信息安全数学基础 …… 2
1.2.1　代数结构 …… 2
1.2.2　域中的多项式 …… 4
1.2.3　整除性和除法 …… 4
1.2.4　素数、素数与 RSA …… 4
1.2.5　有限域 $GF(p)$、有限域 $GF(2n)$、$GF(2n)$ 与 ECC …… 5
1.2.6　离散对数、离散对数与 ELGamal …… 6
1.3　密码学简介 …… 7

2　密码技术 …… 9
2.1　密码技术概述 …… 9
2.1.1　为什么要进行加密 …… 9
2.1.2　信息是怎么进行加密的 …… 10
2.2　数据加密 …… 13
2.2.1　基本概念 …… 13
2.2.2　数据加密方法 …… 13
2.2.3　数据加密与网络安全 …… 15
2.3　对称加密技术 …… 15
2.3.1　对称加密技术简介 …… 15
2.3.2　对称密码的密钥交换 …… 17
2.4　非对称加密技术 …… 17
2.4.1　非对称加密技术简介 …… 17
2.4.2　公开密钥密码的密钥交换 …… 20
2.5　文件加密和数字签名 …… 20

试读结束：需要全本请在线购买：　www.ertongbook.com

2.5.1　文件加密 …… 20
2.5.2　数字签名 …… 21
2.5.3　使用数字签字的密钥交换 …… 22
2.6　混合密码系统 …… 23

3　加密与解密技术 …… 26
3.1　常见加密类型 …… 26
3.1.1　BIOS 加密 …… 26
3.1.2　登录口令 …… 26
3.1.3　文件加密 …… 27
3.1.4　其他类型加密 …… 27
3.2　解密原理与方法 …… 27
3.3　解密技术 …… 27
3.3.1　暴力破解密码技术 …… 27
3.3.2　空间换时间技术(Time-Memory Trade-OFF) …… 30
3.3.3　GPU 加速技术 …… 30
3.3.4　字典攻击 …… 32
3.3.5　程序嗅探、监控 …… 32
3.3.6　社会工程学 …… 32

4　解密实战 …… 33
4.1　本地破解 …… 33
4.1.1　BIOS 密码 …… 33
4.1.2　操作系统密码 …… 36
4.1.3　office 系列密码破解 …… 39
4.2　远程破解 …… 43
4.2.1　ADSL 密码用户密码破解与防护 …… 43
4.2.2　E-mail 密码剖解与防范 …… 48
4.2.3　破解远程 FTP 密码 …… 54
4.2.4　论坛和网络社区密码防范 …… 56

5　加密解密常用工具 …… 60
5.1　密码恢复工具 Cain & Abel …… 60
5.1.1　读取缓存密码 …… 61
5.1.2　查看网络状况 …… 61
5.1.3　ARP 欺骗与嗅探(1) …… 62
5.1.4　ARP 欺骗与嗅探(2) …… 65
5.2　易用的加密解密工具——X-SCAN …… 66

5.2.1 X-SCAN 功能简介 …… 67
5.2.2 X-SCAN 使用指南 …… 67
5.3 兼具数据修复的加密工具——WinHex …… 74
5.4 用 WinHex 检查安全性 …… 75
5.5 字典生成器 …… 79
5.5.1 黑客字典剖析 …… 79
5.5.2 超级字典生成器——Superdic …… 83
5.6 其他常用加密工具 …… 86
5.6.1 EncryptTool …… 86
5.6.2 Rsa-Tool 2 …… 89
5.6.3 Hash calculation …… 92
5.6.4 CrypTool 1.4.31 beta …… 94

6 数据包加解密分析工具 …… 96
6.1 TCP/IP 体系结构 …… 96
6.2 数据包 …… 96
6.3 常见的 sniff …… 97
6.3.1 Sniffer …… 97
6.3.2 Wireshark …… 104

7 加密解密技术应用于应用层 …… 115
7.1 电子邮件 …… 115
7.1.1 电子邮件的构造 …… 115
7.1.2 电子邮件的安全性 …… 116
7.2 PGP …… 117
7.2.1 情景 …… 117
7.2.2 密钥环 …… 119
7.2.3 PGP 证书 …… 122
7.2.4 密钥撤回 …… 129
7.2.5 从环中提取消息 …… 129
7.2.6 PGP 包 …… 131
7.2.7 PGP 信息 …… 136
7.2.8 PGP 的应用 …… 137
7.3 S/MIME …… 138
7.3.1 MIME …… 138
7.3.2 S/MIME …… 144
7.4 概要 …… 147

8　加密解密技术应用于传输层 …… 149
8.1　SSL 结构 …… 149
8.1.1　服务 …… 150
8.1.2　密钥交换算法 …… 150
8.1.3　加密/解密算法 …… 152
8.1.4　散列算法 …… 153
8.1.5　密码套件 …… 154
8.1.6　压缩算法 …… 155
8.1.7　加密参数的生成 …… 155
8.1.8　会话和连接 …… 155
8.2　4 个协议 …… 159
8.2.1　握手协议 …… 159
8.2.2　改变密码规格协议 …… 165
8.2.3　告警协议 …… 166
8.2.4　记录协议 …… 167
8.3　SSL 信息构成 …… 169
8.3.1　改变密码规格协议 …… 170
8.3.2　告警协议 …… 170
8.3.3　握手协议 …… 170
8.3.4　应用数据 …… 177
8.4　传输层安全 …… 178
8.4.1　版本 …… 178
8.4.2　密码套件 …… 178
8.4.3　加密秘密的生成 …… 179
8.4.4　告警协议 …… 180
8.4.5　握手协议 …… 182
8.4.6　记录协议 …… 183

9　加密解密技术应用于网络层 …… 184
9.1　两种模式 …… 184
9.2　两个安全协议 …… 186
9.2.1　验证文件头(AH) …… 187
9.2.2　封装安全载荷(ESP) …… 188
9.2.3　IPv4 和 IPv6 …… 189
9.2.4　AH 和 ESP …… 189
9.2.5　IPSec 提供的服务 …… 189
9.3　安全关联 …… 191
9.3.1　安全关联的概念 …… 191

9.3.2　安全关联数据库(SAD) …… 191
9.4　安全策略 …… 193
9.5　互联网密钥交换(IKE) …… 195
9.5.1　改进的 Diffle-Hellman 密钥交换 …… 196
9.5.2　IKE 阶段 …… 198
9.5.3　阶段和模式 …… 199
9.5.4　阶段Ⅰ：主模式 …… 199
9.5.5　阶段Ⅱ：野蛮模式 …… 204
9.5.6　阶段Ⅲ：快速模式 …… 206
9.5.7　SA 算法 …… 208
9.6　ISAKMP …… 209
9.6.1　一般文件头 …… 209
9.6.2　有效载荷 …… 210

参考文献 …… 220

1 信息安全技术体系中的密码学

1.1 信息安全技术基础理论

1.1.1 信息

美国数学家、控制论的奠基人诺伯特·维纳对信息的定义是，信息是人们在适用外部世界和控制外部世界的过程中，同外部世界进行交换的内容名称。我国信息论专家钟义信认为，信息是事物运动的状态与方式，是物质的一种属性。在这里，“事物”泛指一切可能的研究对象，包括外部世界的物质客体，也包括主观世界的精神现象；“运动”泛指一切意义上的变化，包括机械运动、化学运动、思维运动和社会运动；“运动方式”是指事物运动在时间上所呈现的过程和规律；“运动状态”则是事物运动在空间上所展示的形状与态势。钟义信还指出，信息不同于消息，消息只是信息的外壳，信息则是消息的内核；信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容；信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述。信息还不同于情报和知识。总之，“信息即事物运动的状态与方式”这个定义具有最大的普遍性，不仅能涵盖所有其他的信息定义，还可以通过引入约束条件转换为所有其他的信息定义。

信息的基本特征：

1. 未知性或不确定性；
2. 由不知到知等效为不确定性集合元素减少；
3. 可以度量；
4. 可以产生、消失，可以被携带、存储、处理；
5. 可以产生动作。

1.1.2 信息论

从信息的特征可以看出，信息理论要回答的问题很多。作为基础理论，信息论强调用数学语言来描述信息科学中的共性问题及解决方案。信息论分为狭义信息论、广义信息论、一般信息论。

狭义的信息论：主要总结了香农的研究成果，它在信息的度量的基础之上，研究了如何有效、可靠地传输信息。

广义信息论：不仅包括前两项的研究内容，而且包括所有与信息有关的领域。

一般信息论：主要研究通信问题，但还包括噪声理论，信号滤波与预测、调制、信息处理等问题。

信息论的产生与发展，使得信息更高效地传输，便捷了人们的生活。但是在信息传输的过程中，一些不法分子利用信息系统自身的漏洞进行违法犯罪活动，如信息的窃取、信息诈骗、信息攻击与破坏，信息安全问题日益突出。为凸显出信息安全学科的重要性，2015 年 6 月，国务院学位委员会和教育部正式增设网络空间安全一级学科。如何保障信息有效的传输，满足 CIA(confidentiality、integrity、availability)即机密性、完整性、可用性成为信息安全的首要问题，于是信息安全保障技术日益发展，就是为了满足社会和国家的需要。

1.1.3 信息安全保障

信息安全保障是指在信息系统的整个生命周期中，通过分析信息系统的风险，制定并执行相应的安全保障策略，从技术、管理、工程和人员等方面提取的安全保障要求，确保信息系统的机密性、完整性、可用性，降低安全风险到可接受的程度，保障信息系统能够实现组织机构的使命。

1.1.4 信息安全发展

信息安全发展主要经历以下三个阶段：通信保密阶段、计算机安全阶段、信息安全保障阶段。

通信保密阶段：当代信息安全学起源于 20 世纪 40 年代的通信保密；

计算机安全阶段：20 世纪 60 年代和 70 年代，计算机安全的概念开始逐步得到推行；

信息安全保障阶段：20 世纪 90 年代以后，开始倡导信息保障。

1.2 信息安全数学基础

1.2.1 代数结构

由集合以及集合上的运算组成的数学结构称为代数结构(也称为代数系统)。代数结构是抽象代数的一个主要内容，它研究的中心问题是集合上的抽象运算及运算的性质和结构。研究抽象代数结构的基本特征和基本结构，不仅能深化代数结构的理论研究，也能扩展其应用领域。

定义 1：S 为非空集合，映射 f：$S^n \to S$ 称为 S 上的 n 元运算。

由集合 S 及 S 上的封闭运算 f_1，f_2，…，f_k 所组成的系统就称为一个代数系统，记作 $<S, f_1, f_2, \cdots, f_k>$，或 $(S, f_1, f_2, \cdots, f_k)$。

一个代数系统需要满足以下三个条件：

- 有一个非空集合 S；
- 有一些建立在集合 S 上的运算；
- 这些运算在 S 上是封闭的。

试读结束：需要全本请在线购买： www.ertongbook.com

定义 2：设 S 为集合，函数 f：$S\to S$ 称为 S 上的一元运算。

定义 3：设 o 为 S 上的二元运算，对于任意 x，$y\in S$，都有 $xoy=yox$，则称运算 o 是可交换的，或者运算 o 在 S 上满足交换律。

定义 4：设 o 为 S 上的二元运算，对于任意 x，y，$z\in S$，都有 $(xoy)oz=xo(yoz)$，则称运算 o 是可结合的，或者运算 o 在 S 上满足结合律。

定义 5：设 o 为 S 上的二元运算，对于任意 $x\in S$，都有 $xox=x$，则称该运算 o 适合幂等律。

定义 6：设 o 和 $*$ 为 S 上的二元运算，对于任意 x，y，$z\in S$，有 $xo(y*z)=(x*y)o(x*z)$，称运算 o 对 $*$ 是可分配的，或者运算 o 对 $*$ 在 S 上满足分配律。

定义 7：设 o 和 $*$ 为 S 上的二元运算，对于任意 x，$y\in S$，都有 $x*(xoy)=x$，$xo(x*y)=x$，则称运算 o 和 $*$ 满足分配律。

定义 8：一个代数系统 $(S,\ *)$，若存在一个元素 $e\in U$，使得对 $x\in S$，有 $e*x=x*e=x$，则称 e 为对于运算“$*$”的单位元，也称幺元。

定义 9：一个代数系统 $(S,\ o)$，若存在一个元素 $e_l\in S$，使得对任意 $x\in S$，有 $e_lox=x$，则称 e_l 为对于运算“o”的左幺元。

若存在一个元素 $e_r\in S$，使得对任意 $x\in S$，有：$xoe_r=x$，则称 e_r 为对于运算“o”的右幺元。若 $\theta\in S$，对于运算 o 既是左幺元又是右幺元，则称 θ 为 S 上关于 o 运算的零元。

定义 10：设 o 为 S 上的二元运算，e 为 o 运算的单位元，对于 $x\in S$，如果存在 $y_l\in S$，或者 $y_r\in S$，使得 $y_lox=e$，或者 $xoy_r=e$，那么 y_l 称为 x 的左逆元，y_r 称为 x 的右逆元。若 $y\in S$ 既是 x 的左逆元，又是 x 的右逆元，则称 y 是 x 的逆元。如果 x 的逆元存在，则称 x 是可逆的。

定义 11：设 o 为 S 上的二元运算，对于任意 x，y，$z\in S$，满足

(1)若 $xoy=xoz$ 且 $x\neq 0$，则 $y=z$；

(2)若 $yox=zox$ 且 $x\neq 0$，则 $y=z$；那么称 o 运算满足消去律，其中(1)称作左消去律，(2)称作右消去律。

定义 12：代数系统的定义：X 是非空集合，X 上的 m 个运算，f_1，f_2，…，f_m 构成代数系统 U，记作 $U=<X,\ f_1,\ f_2,\ \cdots,\ f_m>(m\geqslant 1)$

定义 13：有限代数系统：$U=<X,\ f_1,\ f_2,\ \cdots,\ f_m>$ 是个代数系统，如果 X 是个有限集合，则称 U 是个有限代数系统。

定义 14：同类型代数系统：给定两个代数系统 $U=<X,\ f_1,\ f_2,\ \cdots,\ f_m>$，$V=<Y,\ g_1,\ g_2,\ \cdots,\ g_m>$ 如对应的运算 f_i 和 g_i 的元数相同($i=1,\ 2,\ 3,\ \cdots,\ m$)，则称 U 与 V 是同类型代数系统。

定义 15：设 $V=<X,\ f_1,\ f_2,\ \cdots,\ f_k>$ 是代数系统，B 是 S 的非空子集，如果 B 对 f_1，f_2，…，f_k，都是封闭的，且 B 和 S 含有相同的代数常数，则称 $<B,\ f_1,\ f_2,\ \cdots,\ f_k>$ 是 V 的子代数系统，简称子代数。

V 的最大的子代数就是 V 本身，如果 V 中所有代数常数构成集合 B，且 B 对 V 中所有运算封闭，则 B 就构成了 V 的最小的子代数。最大和最小子代数称为 V 的平凡的子代数。若 B 是 S 的真子集，则 B 构成的子代数称为 V 的真子代数。

定义 16：设 $V_1=<S_1, o>$和 $V_2=<S_2, *>$是代数系统，其中 o 和 $*$ 是二元运算，V_1与 V_2的积代数是 $V=<S_1\times S_2, \cdot>$。

定义 17：设 $V_1=<S_1, o>$和 $V_2=<S_2, *>$是代数系统，其中 o 和 $*$ 是二元运算，$f: S_1\to S_2$，且对任意 $x, y\in S_1$，$f(xoy)=f(x)*f(y)$，则称 f 为 V_1到 V_2的同态映射，简称同态。

1.2.2 域中的多项式

定义 18：如果群$<G, *>$中的二元运算 $*$ 是可交换的，则称该群为阿贝尔群，也叫交换群。即 $G=<S_1, S_2, \cdots, S_m>$，$S_i*S_k=S_k*S_i$。

域的定义：若代数系统$<F, +, \cdot>$具有(1) $|F|>1$，(2)$<F, +>$，$<F-\{0\}, \cdot>$均是阿贝尔群，(3)乘法对加法可分配，则称它是域。

普通多项式：一个 $n(n\geqslant 0)$次多项式的表述如下：$f(x)=a_nx^n+a_{n-1}x^{n-1}\cdots a_kx^k+\cdots+a_1x^1+a_0x^0=\sum_{i=0}^{n}a_ix^i$

系数在 Z_p 中的多项式运算：在 Z_5 中元素个数为 5 个$\{0, 1, 2, 3, 4\}$，S 中 $3^{-1}=2$，$4/3=(4*3^{-1})\bmod 5=3$ 并不是 $4/3=1+1/3$，因为在 Z_5 中 $1/3=2$。那么域中的多项式：给定 n 次多项式 $f(x)$和 m 次多项式 $g(x)$，$m\leqslant n$，$g(x)$除以 $f(x)$商为 $q(x)$，余数 $r(x)$，各多项式的次数为 $d(f(x))=n$，$d(g(x))=m$，$d(q(x))=n-m$，$d(r(x))\leqslant m-1$

多项式的模运算：$GF(2^8)$中，即约多项式为 $m(x)$

$m(x)=x^8+x^4+x^3+x+1\quad f(x)=x^6+x^4+x^2+x+1\quad g(x)=x^7+x+1$

$f(x)*g(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1$

$f(x)*g(x)\bmod m(x)=x^7+x^6+1$

1.2.3 整除性和除法

设 a、b 是两个整数，其中 $b\neq 0$，如果存在一个整数 q 使得等式 $a=bq$ 成立，就称 b 整除 a 或者 a 被 b 整除，记作 $b\mid a$，并把 b 叫做 a 的因数，把 a 叫做 b 的倍数。这时，q 也是 a 的因数，我们常常将 q 写成 $a\mid b$ 或$\frac{b}{a}$。

定理 1 设 a，$b\neq 0$，$c\neq 0$ 是三个整数，若 $c\mid b$，$b\mid a$，则 $c\mid a$。

定理 2 设 a，b，$c\neq 0$ 是三个整数，若 $c\mid a$，$c\mid b$，则 $c\mid a\pm b$。

定理 3 设 a，b，c 是三个整数，若 $c\mid a$，$c\mid b$ 则对任意整数 s，t，有 $c\mid sa+tb$。

定理 4 若整数 a_1，$\cdots$，a_n 都是整数 $c\neq 0$ 的倍数，则对任意 n 个整数 s_1，$\cdots$，s_n，整数 $s_1a_1+\cdots+s_na_n$ 是 c 的倍数。

定理 5 设 a，b 都是非零整数．若 $a\mid b$，$b\mid a$，则 $a=\pm b$。

欧几里得除法：设 a，b 是两个整数，其中 $b>0$，则存在唯一的整数 q，r 使得 $a=bq+r$，$0\leqslant r<b$。

1.2.4 素数、素数与 RSA

数论主要关心的是素数，实际上数论也主要是围绕这一主题来展开的。

何为素数？整数 $p>1$ 是素数当且仅当它只有因子 1，-1，$-p$，p。任意一个素数 $a>1$ 都可以唯一地分解为 $a=p_1^{a_1}\times p_2^{a_2}\times p_3^{a_3}\times p_4^{a_4}\times\cdots\times p_i^{a_i}\cdots\times p_t^{a_t}$，其中 $p_i(1\leqslant i\leqslant t)$ 均是素数。$p_1<p_2<\cdots<p_i<p_t$，且所有 a_i 都是正整数。

RSA 加密算中的数学原理就是**大素数分解问题**。

RSA 加密算法简史：RSA 是 1977 年由罗纳德·李维斯特(Ron Rivest)、阿迪·萨莫尔(Adi Shamir)和伦纳德·阿德曼(Leonard Adleman)一起提出的。当时他们三人都在麻省理工学院工作。RSA 就是他们三人姓氏开头字母拼在一起组成的。

公钥与密钥的产生：

假设 Alice 想要通过一个不可靠的媒体接收 Bob 的一条私人信息。她可以用以下的方式来产生一个公钥和一个私钥：

1. 随意选择两个大的质数 p 和 q，p 不等于 q，计算 $N=pq$。

2. 根据欧拉函数，求得 $r=(p-1)(q-1)$。

3. 选择一个小于 r 的整数 e，求得 e 关于模 r 的模反元素，命名为 d。(模反元素存在，当且仅当 e 与 r 互质)

4. 将 p 和 q 的记录销毁。

(N, e)是公钥，(N, d)是私钥。Alice 将她的公钥(N, e)传给 Bob，而将她的私钥(N, d)藏起来。

加密消息：

假设 Bob 想给 Alice 送一个消息 m，他知道 Alice 产生的 N 和 e。他使用起先与 Alice 约好的格式将 m 转换为一个小于 N 的整数 n，比如他可以将每一个字转换为这个字的 Unicode 码，然后将这些数字连在一起组成一个数字。假如他的信息非常长的话，他可以将这个信息分为几段，然后将每一段转换为 n。用下面这个公式他可以将 n 加密为 c：$n^e\equiv c\pmod N$，计算 c 并不复杂。Bob 算出 c 后就可以将它传递给 Alice。

解密消息：

Alice 得到 Bob 的消息 c 后就可以利用她的密钥 d 来解码。她可以用以下这个公式来将 c 转换为 n：$c^d\equiv n\pmod N$，得到 n 后，她可以将原来的信息 m 重新复原。

解码的原理是：

$c^d\equiv n^{e\cdot d}\pmod N$以及 $ed\equiv 1\pmod{p-1}$和 $ed\equiv 1\pmod{q-1}$。

由费马小定理可证明，因为 p 和 q 是质数。

$n^{e\cdot d}\equiv n\pmod p$和 $n^{e\cdot d}\equiv n\pmod q$

这说明：因为 p 和 q 是不同的质数，所以 p 和 q 互质。

$n^{e\cdot d}\equiv n\pmod{p*q}$

1.2.5 有限域 $GF(p)$、有限域 $GF(2n)$、$GF(2n)$与 ECC

有限域：非空集合 F，若 F 中定义了加和乘两种运算，且满足：

1. F 关于加法构成阿贝尔群，加法恒等元记为 0；

2. F 中所有非零元素对乘法构成阿贝尔群，乘法恒等元记为 1；

3. 加法和乘法之间满足分配律。

则 F 与这两种运算构成域，当域元素个数有限时，称为有限域或伽罗瓦(Galois)域，记为 GF，并把元素的个数 n 称为 F 的阶，记为 $GF(n)$，否则称为无限域。

椭圆曲线并不是椭圆，之所以称为椭圆曲线是因为它们与计算椭圆周长的方程相似。椭圆曲线可以定义在不同的有限域上，对我们最有用的是定义在 $GF(p)$ 上的椭圆曲线和定义在 $GF(2^n)$ 上的椭圆曲线。

1. $GF(p)$ 上的椭圆曲线

定义 19：设 p 是大于 3 的素数，且 $4a^3+27b^2\neq 0$，则称曲线 $y^2=x^3+ax+b$，a，$b\in GF(p)$ 为 $GF(p)$ 上的椭圆曲线。

2. $GF(2^n)$ 上的椭圆曲线

定义 20：设 p 是大于 3 的素数，且 $4a^3+27b^2\neq 0$，则称曲线 $y^2+xy=x^3+ax+b$，a，$b\in GF(2^m)$ 为 $GF(2^m)$ 上的椭圆曲线。

1.2.6 离散对数、离散对数与 ELGamal

(1)模 n 的整数幂

欧拉函数：现在有一个素数 p，$\varphi(n)$ 表示小于 n 并且与 n 互素的正整数的个数，对于素数 p，$\varphi(p)=p-1$。

对于任意互素的 a 和 n，$a^{\varphi(n)}\equiv 1(\bmod n)$。

则至少有一个整数 m 满足，$a^m\equiv 1(\bmod n)$，即 $M=\varphi(n)$，$a^m\equiv 1(\bmod n)$ 中成立的最小正幂 m 为下列之一。

- a(模 n)的阶
- a 所属的模 n 的指数
- a 所产生的周期长

(2)模算术对数

$y=x^{\log_x(y)}$，其中 $\log_x(1)=0$，$\log_x(x)=1$，$\log_x(yz)=\log_x(y)+\log_x(z)$

$$\log_x(y^r)=r\log_x(y)。$$

对于某素数 p(对于非素数也可以)的本原根 a，a 的 1 到 $p-1$ 的各次幂恰可产生 1 到 $p-1$ 的每个整数一次仅一次。而对任何整数 b，根据模运算的定义，b 满足 $b\equiv r(\bmod p)$，$0\leqslant r\leqslant p-1$。

因此对于任何整数 b 和素数 p 的本原根 a，有唯一的幂 i 使得 $b\equiv a^i(\bmod p)$，$0\leqslant i\leqslant p-1$。该指数 i 称为以 a 为底(模 p)b 的对数，$i=\log_{a(\bmod p)}(b)$

离散对数的计算，考虑 $y=g^x(\bmod p)$ 对给定 g，x，p 可以直接计算出 y。

(3)ElGamal 提出的一种基于离散对数的公开密码体制，系统用户选择一个素数 q，α 是 q 的素根。

用户 A 生成的密钥对如下：

(1)随机生成整数 X_A，使得 $1<X_A<q-1$；

(2)计算 Y_A，$Y_A=a^{X_A}\bmod q$；

(3)A 的私钥 X_A，公钥 $\{q, \alpha, Y_A\}$。其他任意用户 B 通过 A 的公钥可以加密信息：

①将信息表示为一个整数 M，$1 \leqslant M \leqslant q-1$，以分组密码序列的方式来发送信息，其中每个分块的长度不小于整数 q；

②选择任意整数 k，$1 \leqslant k \leqslant q-1$，计算一次密钥 $K=(Y_A)^k \bmod q$。

(4)将 M 加密成明文对 (C_1, C_2)：$C_1=\alpha^k \bmod q$　$C_2=KM \bmod q$ 用户 A 恢复明文：

①通过计算 $K=(C_1)^{X_A} \bmod q$；

②计算 $M=C_2K^{-1} \bmod q$。

1.3 密码学简介

学习密码学，我们首先需了解一下加密和解密。加密是按照特定的公式，对各种明文信息进行变换，以隐藏其真正的意义和内容；而解密可以说是加密的逆过程，只有通过解密将密文还原，我们才能知道那些看似无序的密文中隐藏着什么含义。密码学是一门研究编制密码和破译密码的科学。它实际上是指两个部分，其中研究密码变化的客观规律，应用于编制密码以保守通信秘密的称为编码学；应用于破译密码以获取通信情报的称为破译学，总称密码学。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，将明文变换为密文，称为加密变换；将密文变换为明文，称为解密变换。密码学在早期仅研究针对文字或数字进行的加、解密变换，然而随着通信技术的发展，针对语音、图像、数据等各种数据加、解密进行的研究越来越深入。

密码学是在编码与破译的实践中逐步发展起来的，并随着先进科学技术的应用，发展成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府采用的密码编制及破译手段都具有高度的机密性。

中国古代的某些秘密通信手段，已经比较近似于密码的维形。宋曾公亮、丁度等编撰的《武经总要》中有记载，北宋前期，在作战中曾用一首五言律诗的 40 个汉字，分别代表 40 种情况或要求，这种方式已具有了密码本的特点。

1871 年，上海大北水线电报公司选用 6899 个汉字，代以四码数字，制成了中国最初的商用明码本，同时也设计了由明码本改编为密本及进行加乱的方法，并在此基础上逐步发展出各种比较复杂的密码。

在欧洲，公元前 405 年，斯巴达的将领曾经使用了原始的错乱密码；公元前 1 世纪，古罗马皇帝恺撒曾使用有序的单表代替密码，后人在此基础上逐步发展出了密码本、多表代替等各种密码体制。

20 世纪初，产生了最初可以使用的机械式和电动式密码机，同时也出现了一些商业密码机公司。20 世纪 60 年代后，电子密码机得到较快发展和广泛应用，密码学的发展进入了一个新的阶段。

密码破译是随着密码的使用而逐步产生和发展的。1412 年，波斯人卡勒卡尚迪所编著的《百科全书》中载有破译简单代替密码的方法。到 16 世纪末期，欧洲一些国家设有专

职的破译人员，以破译截获的密信，密码破译技术有了相当的发展。1863 年普鲁士人卡西斯基所著《密码和破译技术》，以及 1883 年法国人克尔克霍夫所著《军事密码学》等著作，都对密码学的理论和方法做了一些论述和探讨。1949 年美国人香农发表了《秘密体制的通信理论》一文，运用信息论的原理系统地分析了密码学中的一些基本问题。

自 19 世纪以来，由于电报特别是无线电报的广泛使用，为密码通信和第三者的截获都提供了极为有利的条件，通信保密和破译之间形成了一场十分激烈的暗战。

1917 年，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战。1942 年，美国从破译日本海军密报中，获悉日军对中途岛地区的作战意图和兵力部署，从而以劣势兵力击破了日本海军的主力，扭转了太平洋地区的战局。在保卫英伦三岛和其他许多著名的历史事件中，密码破译的成功都起到了极其重要的作用，这些事例也从反面说明了密码保密的重要性和意义。

世界上各个国家的政府都十分重视密码保护工作，有些国家甚至设立了庞大的机构，拨出巨额经费，集中数以万计的专家和科技人员，投入大量的高速计算机和其他先进设备进行研究。与此同时，民间企业和学术界也对密码学日益重视，不少数学家、计算机专家等也都纷纷投身于密码学的研究行列，更加速了密码学的发展。

密码学是信息安全的核心，在信息安全技术体系中的起着极其重要的作用。

①用加密来保护信息

利用密码变换将明文变换成只有合法者才能恢复的密文，这是密码最基本的功能。信息的加密保护包括传输信息和存储信息两方面，相比较而言，后者解决起来难度更大。

②采用密码技术对发送信息进行验证

为防止传输和存储的消息被有意或无意地篡改，采用密码技术对消息进行运算生成消息验证码(MAC)，附在消息之后发出或与信息一起存储，对信息进行认证。它在票据防伪中具有重要应用，如税务的金税系统和银行的支付密码器。

③采用数字证书来进行身份鉴别

数字证书就是网络通信中标志通信各方身份信息的一系列数据，是网络正常运行所必需的。过去常采用通行字，但安全性差，现在一般采用交互式询问回答，在询问和回答过程中采用密码加密。特别是采用密码技术的带 CPU 的智能卡，安全性好。在电子商务系统中，所有参与活动的实体都需要用数字证书来表明自己的身份，数字证书从某种角度上说就是“电子身份证”。

④数字指纹

在数字签名中有重要作用的“报文摘要”算法，即生成报文“数字指纹”的方法，近年来备受关注，构成了现代密码学的一个重要侧面。

⑤利用数字签名来完成最终协议

在信息时代，电子数据的收发使我们过去所依赖的个人特征都将被数字代替，数字签名的作用有两点：一是因为自己的签名难以否认，从而确认了文件已签署这一事实；二是因为签名不易仿冒，从而确定了文件是真的这一事实。

试读结束：需要全本请在线购买： www.ertongbook.com