

欧姆社学习漫画

漫画密码

〔日〕三谷政昭 佐藤伸一/著

〔日〕Hinoki Iderou/漫画绘制

〔日〕VERTE/漫画制作

李光东 李 纯 刘敏亮/译



科学出版社

www.sciencep.com

欧姆社学习漫画

漫画密码

〔日〕三谷政昭 佐藤伸一 著

〔日〕Hinoki Iderou 漫画绘制

〔日〕VERTE 漫画制作

李光东 李 纯 刘敏亮 译



科学出版社

北 京

图字: 01-2009-2820号

内 容 简 介

这是一本很好看的书,你一定能看懂!书中有扣人心弦的故事,让人可以轻松、愉快地动脑筋思考的精彩内容。加密、破译、疯狂升级、天才、叛徒……聪明人制造了密码,等待更聪明的人去毁灭它,这是人类知识和智慧的较量!本书用漫画的形式讲解了密码的实质、来源、用处、设置方法……为大家展现了一个生动的密码世界。

有趣的故事情节、时尚的漫画人物造型、细致的内容讲解定能让你留下深刻的印象,让你看过忘不了。通过这种轻松的阅读学习,读者可以掌握密码科学的常识。本书也可以作为广大青少年的密码学基础知识读本。

图书在版编目(CIP)数据

漫画密码/(日)三谷政昭,佐藤伸一著;(日)Hinoki Iderou漫画绘制;
VERTE漫画制作;李光东,李纯,刘敏亮译—北京:科学出版社,2009
(欧姆社学习漫画)

ISBN 978-7-03-025320-0

I.漫… II.①三…②佐…③H…④V…⑤李…⑥李…⑦刘… III.密码—普
及读物 IV.TN918.2-49

中国版本图书馆CIP数据核字(2009)第147201号

责任编辑:唐璐 赵丽艳/责任制作:董立颖 魏谨
责任印制:赵德静/封面制作:铭轩堂

北京东方科龙图文有限公司 制作
<http://www.okbook.com.cn>

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

<http://www.sciencep.com>

北京天时彩色印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2009年8月第 一 版 开本:787×1092 1/16

2009年8月第一次印刷 印张:15

印数:1—5 000 字数:228 000

定价:29.80元

(如有印装质量问题,我社负责调换)

❀ 前 言 ❀

当今是以因特网为核心的网络化信息社会。活用网页发布信息，使用电子邮件进行交流，以及网上购物与电子银行的普及，都极大地方便了我们的日常生活。

但是，在享受网络时代给我们带来的便利的同时，“网络安全”、“信息安全”、“个人信息保护”、“密码”这些我们听起来有些厌烦的词汇，不断冲击着我们的生活。那么，到底为什么会出现这种情况呢？

我们使用网络的时候，会进行各种各样的信息交流。在这些信息当中，就包含着不能被人所知的私密信息。比如，信用卡账号、银行账号、病例、贷款的金额、电子邮箱地址等，这些都是不能轻易泄露给他人、必须要进行“信息保护”的私密信息。由于私密信息被恶意利用而产生不良后果的事件时有发生，所以，如何保护信息的安全，就毫无疑问地成为网络信息时代最重要的研究课题。在这充斥着不安因素的网络信息社会，为了识别信息的真伪，防止冒名诈骗，信息的伪造、篡改、窃密等犯罪的发生，安心、安全地使用各种网络化信息服务，“密码”成为了保障信息安全的基本技术。

近年来，密码技术得到了突飞猛进的发展。它不仅仅只局限于信息情报安全专家们所研究的领域，对于使用网络服务的大众来说，密码技术也理所当然地成为了不可缺少的知识。

那么，密码技术是如何构成的呢？如何才能实现信息化，保护个人信息不被窃取呢？

本书以漫画故事为基础，详细讲解了密码技术的构成和作用。同时，为了理解密码技术而必须掌握的不可缺少的高等数学知识，我们也将进行简明扼要的讲解。亲爱的读者朋友，不管你是谁，都可以一边开心地看故事，一边轻松地学习密码知识。当然，在故事中会出现一些密码谜题，大家可以一边踏踏实实地学习，一边享受破解这些谜题的乐趣。

在读完本书的同时，希望大家都能迅速掌握基本的密码技术与信息情报安全的基础知识。

最后，向出版本书的欧姆社开发局的诸位，以及担任绘画的 Hinoki Iderou 先生，

表示衷心的感谢。

著 者

❀ 目 录 ❀

序 章	1
第 1 章 密码学基础	15
1-1 密码学的相关词汇	16
❀ 密码学的基本词汇	20
❀ 加密密钥 E_k 与解密密钥 D_k 的关系	21
1-2 古典密码技术	24
❀ 凯撒密码	24
❀ 换字式密码	25
❀ 多表替代密码	26
❀ 转制式密码	27
1-3 密码的安全强度	28
❀ 换字式密码的密钥数量	31
❀ 多表替代密码的密钥数量	32
❀ 转置式密码的密钥数量	32
❀ 解密需要的条件	35
❀ 绝对安全的密码	35
❀ 安全的密码	37
第 2 章 通用密钥加密技术	45
2-1 二进制运算和不可兼析取	46
2-2 通用密钥密码的定义	57
❀ 通用密钥密码的特征	62
2-3 流密码的构成	63
2-4 分组密码的构成	66
❀ CBC模式	69
2-5 DES 密码的构成	70

✿ Feistel类型密码的基本结构	71
✿ Involution	72
✿ DES密码密钥的生成	75
✿ DES非线性函数 f 的构成	76
✿ DES加密和解密的基本构成	77
2-6 3-DES 密码和 AES 密码	78
✿ AES密码的概要	83
简易版 DES 加密和解密详解	87
✿ 二进制数据的变换	87
✿ DES密文的生成	87
✿ DES密文的解密	95
✿ DES加密密钥的生成	100
✿ DES解密密钥的生成	104

第 3 章 公开密钥加密技术 107

3-1 公开密钥密码的基础知识	108
✿ 公开密钥加密方式的主要种类	117
✿ 单向函数	118
✿ RSA密码的诞生	121
3-2 素数和素因数分解	122
✿ 素数的判定	131
3-3 取模运算	136
✿ 取模运算的加法运算和减法运算	139
✿ 取模运算的乘法运算和除法运算	148
3-4 费尔马小定理和欧拉定理	154
✿ 数论之父费尔马	155
✿ 费尔马方法和拟素数	157
✿ 欧拉定理	158
✿ 数学家欧拉	159

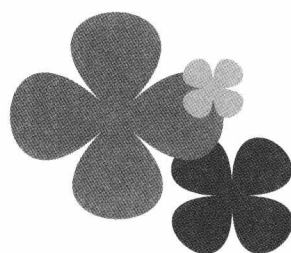
✿ 2个素数乘积的欧拉函数	160
3-5 RSA 密码的构成	163
✿ RSA密码的加密和解密	165
✿ RSA密码密钥的生成法	167
✿ 公开密钥和私密密钥的制作方法	169
✿ RSA密文的生成	171
✿ RSA密文的解密	173
3-6 公开密钥密码和离散对数问题	175
✿ 离散对数问题	176
✿ ElGamal密码的加密和解密	178
专栏 扩展的欧几里得辗转相除法	183

第4章 密码的实际应用 187

4-1 Hybird 密码	188
4-2 Hash 函数和消息认证代码	192
✿ 篡改	192
✿ 篡改的对策	194
✿ Hash函数	195
✿ 冒名诈骗	196
✿ 冒名诈骗的对策	197
✿ 消息认证代码的构成	198
✿ 否认的定义	199
✿ 消息认证代码的两个缺点	201
4-3 电子签名	202
✿ 否认的对策	202
✿ 电子签名的构成	203
✿ 中间者攻击	205
✿ 中间者攻击的对策	206

✱ 证书和认证中心	206
4-4 公开密钥密码基础设施 (PKI)	208
专栏 零知识对话证明	219
补充说明	225
参考文献	227

序 章



某省某市 78 分局

事科

咨询处

目黑留香

哥哥，给我买嘛！

目黑顺警官

不行，不行，电脑对高中生来说太奢侈了！

嘶嘶

但是对学习数学很有帮助啊！

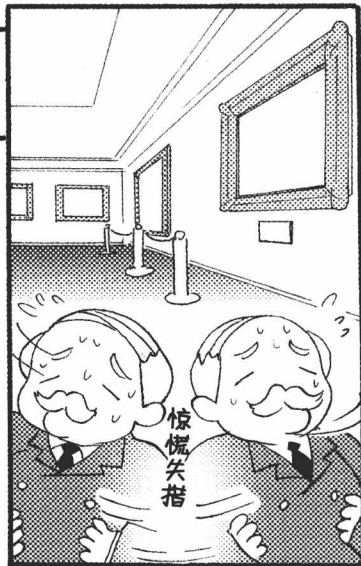
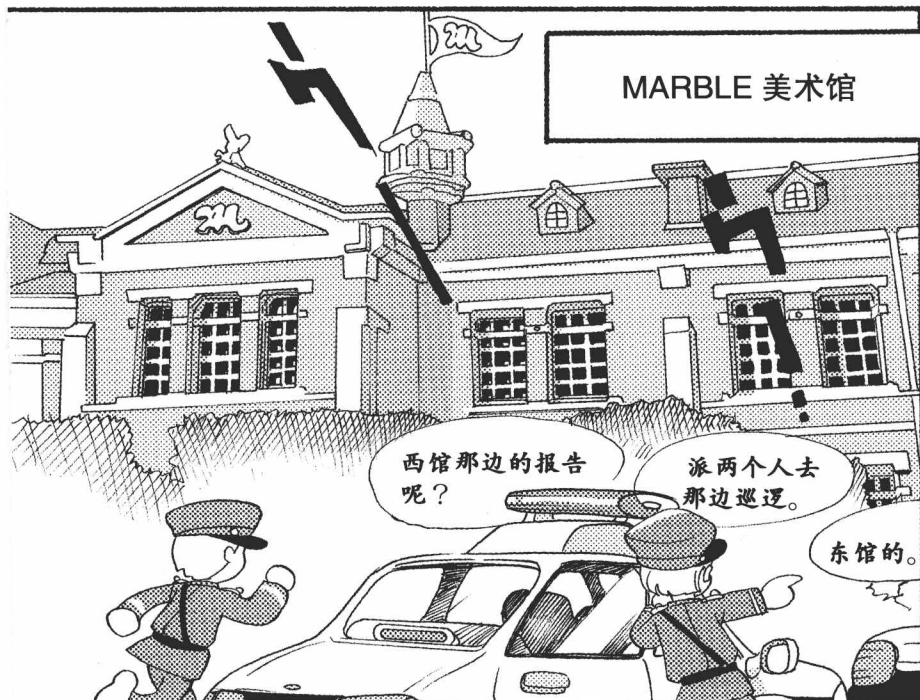
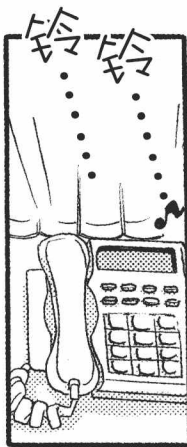
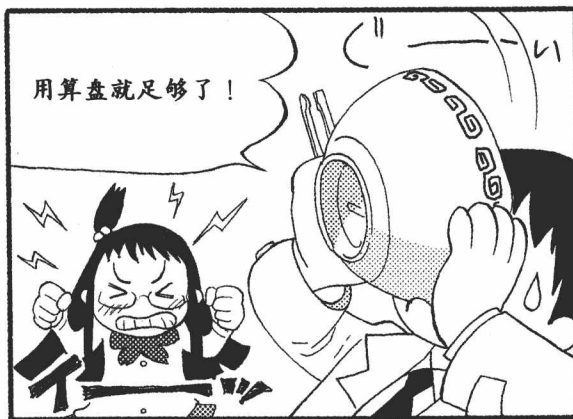
$$ax + by = \gcd(a, b)$$

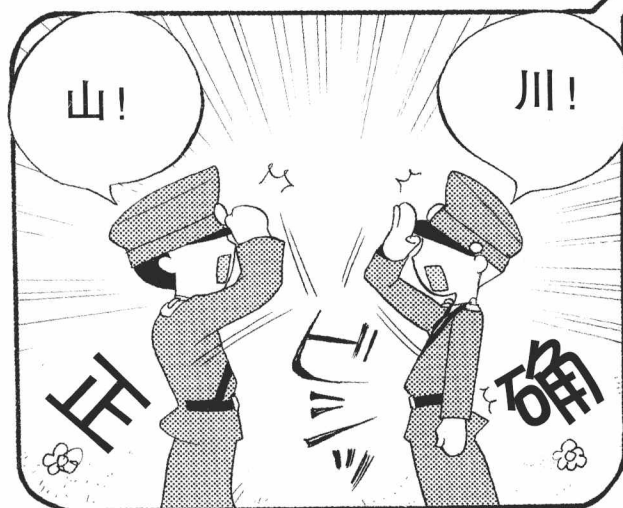
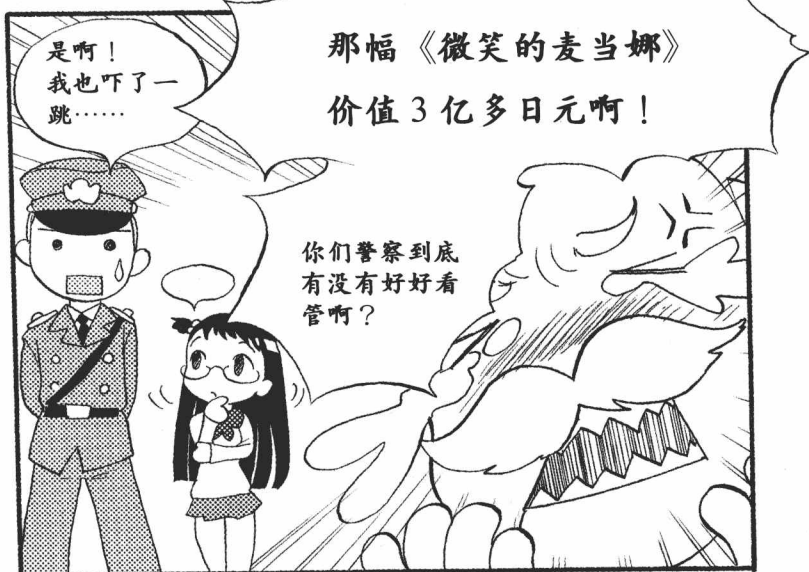
$$a^{p-1} = 1 \pmod{p}$$

$$\varphi(p) = p - 1$$

我很想

要嘛！





画的保管地点都是用密码写的，其他人应该不会知道的。



baomiguanchangmisuoshi
midiwumicangku

好啊！
太完美啦！

太过分了……

那样的防范，根本起不到任何作用的！

你是谁啊？

我是每晚报社的
记者米田理绪！



