

# 《漫画密码》

## 图书基本信息

书名：《漫画密码》

13位ISBN编号：9787030253200

10位ISBN编号：7030253205

出版时间：2009-8

出版社：科学

作者：[日] 三谷政昭

页数：226

译者：李光东,李纯,刘敏亮

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《漫画密码》

## 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。

# 《漫画密码》

## 内容概要

《欧姆社学习漫画:漫画密码》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。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！

有趣故事情节、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。《欧姆社学习漫画:漫画密码》也可以作为广大青少年的密码学基础知识读本。

# 《漫画密码》

## 作者简介

三谷政昭，出生于日本广岛县尾道市濑户田町。1974年毕业于东京工业大学工学部电子工程专业，曾任东京工业大学工学部助教，现任东京电机大学工学部情报通信工程学教授，工学博士。研究专业为电子信号处理工程学、通信工程学、教育工程学。

著作有《电子信号处理入门》(欧姆社)、《用Scilab学电子信号处理》(CQ出版社)、《简易电子电路基础( )二极管、三级管篇》(Micro Net)、《重新学习信号数学》(CQ出版社)、《即学即用的傅里叶变换》(讲谈社)等。

佐藤伸一，出生于日本福岛县伊达市。1990年毕业于东京电机大学研究生院电气工程学专业。曾在民间企业中从事影像相关设备的设计工作，并担任过私立大学医学部的助手，进行生物工程学方面的研究。现任东京电机大学工学部情报通信工程科助理一职。研究专业为电子信号处理工程学、教育工程学。

## 书籍目录

- 序章
- 第1章 密码学基础
  - 1-1 密码学的相关词汇
    - 密码学的基本词汇
    - 加密密钥Ek与解密密钥Dk的关系
  - 1-2 古典密码技术
    - 凯撒密码序章
    - 第1章 密码学基础
      - 1-1 密码学的相关词汇
      - 密码学的基本词汇
      - 加密密钥Ek与解密密钥Dk的关系
      - 1-2 古典密码技术
    - 凯撒密码
    - 换字式密码
    - 多表替代密码
    - 转制式密码
    - 1-3 密码的安全强度
    - 换字式密码的密钥数量
    - 多表替代密码的密钥数量
    - 转置式密码的密钥数量
    - 解密需要的条件
    - 第一安全的密码
    - 安全的密码
  - 第2章 通用密钥加密技术
    - 2-1 二进制运算和不可兼析取
    - 2-2 通用密钥密码的定义
    - 通用密钥密码的特征
    - 2-3 流密码的构成
    - 2-4 分组密码的构成
    - CBC模式
    - 2-5 DES密码的构成
    - Feistel类型密码的基本结构
    - Involution
    - DES密码密钥的生成
    - DES线性函数f的构成
    - DES加密和解密的基本构成
    - 2-6 3-DES密码和AES密码
    - AES密码的概要
    - 简易版DES加密和解密详解
    - 二进制数据的变换
    - DES密文的生成
    - DES密文的解密
    - DES加密密钥的生成
    - DES解密密钥的生成
  - 第3章 公开密钥加密技术
    - 3-1 公开密钥密码的基础知识
    - 公开密钥加密方式的主要种类

- 单向函数
- RSA密码的诞生
- 3-2 素数和素因数分解
  - 素数的判定
- 3-3 取模运算
  - 取模运算的加法运算和减法运算
  - 取模运算的乘法运算和除法运算
- 3-4 费尔马小定理和欧拉定理
  - 数论之父费尔马
  - 费尔马方法和拟素数
  - 欧拉定理
  - 数学家欧拉
  - 2个素数乘积的欧拉函数
- 3-5 RSA密码的构成
  - RSA密码的加密和解密
  - RSA密码密钥的生成法
  - 公开密钥和私密密钥的制作方法
  - RSA密文的生成
  - RSA密文的解密
- 3-6 公开密钥密码和离散对数问题
  - 离散对数问题
  - ElGamal密码的加密和解密
  - 专栏 扩展的欧几里得辗转相除法
- 第4章 密码的实际应用
  - 4-1 Hybrid密码
  - 4-2 Hybrid函数和消息认证代码
    - 篡改
    - 篡改的对策
    - Hastl函数
    - 冒名诈骗
    - 冒名诈骗的对策
    - 消息认证代码的构成
    - 否认的定义
    - 消息认证代码的两个缺点
  - 4-3 电子签名
    - 否认的对策
    - 电子签名的构成
    - 中间者攻击
    - 中间者攻击的对策
    - 证书和认证中心
  - 4-4 公开密钥密码基础设施 (PKI)
    - 专栏 零知识对话证明
    - 补充说明
    - 参考文献

# 《漫画密码》

## 媒体关注与评论

用漫画这种形式讲数学、物理和统计学，十分有利于在广大青少年中普及科学知识。——周恩来、邓颖超秘书，周恩来邓颖超纪念馆顾问 中日友好协会理事，《数理天地》顾问，全国政协原副秘书长

用漫画和说故事的形式讲数学，使面貌冷峻的数学变得亲切、生动、有趣，使学习数学变得容易，这对于提高全民的数学水平无疑是功德无量的事。——《数理天地》杂志社社长总编 “希望杯”全国数学邀请赛组委会命题委员会主任 周国镇

用漫画的形式，讲解日常生活中的数学、物理知识，更能让大家感受到数学殿堂的奥妙与乐趣。——《光明日报》原副总编辑 中华炎黄文化研究会常务副会长 鲁諝

科学漫画是帮助学习文科的人们用形象思维的方式掌握自然科学的金钥匙。——中国人民大学外语学院日语专业主任 大学日语教学研究会会长 成同社

在日本留学的时候，我在电车上几乎每次都能看到很多年轻的白领看这套图书，经济实惠、图文并茂、浅显易懂，相信这套图书的中文版也一定会成为白领们的手中爱物。——大连理工大学能源与动力学院博士副教授 宁亚东

我非常希望能够在书店里看到这样的书：有人物形象、有卡通图、有故事情节，当然最重要的还有深厚的理工科底蕴。我想这样的书一定可以大大提升孩子们的学习兴趣，降低他们对于高深的理工科知识的恐惧感。——北京启明星培训学校校长

书中的数学知识浅显实用，漫画故事的形式使知识贴近生活，概念更容易理解。——北京大学数学科学学院博士 张磊

## 《漫画密码》

### 精彩短评

- 1、算是很不错的东西了，我都看着很费劲
- 2、内容很好，漫画的形式生动又有趣。
- 3、后面不懂了。。
- 4、内容还不错，只是略微有些小的错误。

虽然是翻译的书，但总希望出版社能够有个纠错的机制。

- 5、孩子明白了很多密码知识，通过此书学会了2进制，自己会编写简单的密码，对聪明的孩子来说，可以启发益智。有些内容稍深，但反复看，随着年龄的增长，会明白很多。
- 6、借之扫扫盲，仅此而已。
- 7、知道了很多以前不知道的
- 8、密码书可以 不过要投入
- 9、这本还不错
- 10、个人认为这本书非常适合学生阅读，有一部分内容是读完高中才能看懂的！但非常适合高中生作为课外读物！
- 11、能把这么抽象的数学知识融入漫画里，相信很多人会对数学更感兴趣
- 12、读起来诙谐轻松，但是对于零基础的我来说，都后面的一些地方，还是不太明白。
- 13、数学无力...慢慢补吧。
- 14、能把神秘的密码学讲的这么浅显,这本身就是需要极高的智慧,只能说声作者,译者,出版者你们都辛苦了!
- 15、没看完，以后估计也不会再看了
- 16、这本书曾经一度让我想过长大研究密码...
- 17、非常好的书，学习起来有乐趣
- 18、只是读了前面一部分，后面的就没读了，总体来说应该不错，将密码学用漫画的形式表现出来，通俗易懂
- 19、漫画密码
- 20、很好！快递员态度很好，辛苦了！
- 21、两个星期才拿到书，物流太不给力了。
- 22、其中DES和RSA的部分没有一定基础估计是看不下去的。个人觉得是一本好书，密码学又从另一个角度复习了一次。
- 23、书的内容忘光了
- 24、欧姆社的漫画很不错
- 25、这套科普书非常好看，图文并茂。
- 26、很多比较费解的问题被漫画冰释了。
- 27、密码原来还有很多种类的呱，看漫画也易懂
- 28、书店质量很好。
- 29、一套很好的图书，值得推荐。
- 30、很好，适合用来加密技术入门。
- 31、后面的密码加密算法还是解释的不清楚。
- 32、关于数学的内容就没心思看--
- 33、没看懂。。。
- 34、对这个系列的书都非常喜欢，厕上精品
- 35、挺好的一本书，入门书籍。
- 36、老实说，不是很好看
- 37、没有基础+不感兴趣+没有细看+没有推敲=什么也没学会。。。。。。囧o( )o
- 38、好玩。易懂。
- 39、书是写得不错，对于没有数学功底的人来说太难了。不是作者没写好，而是密码学本身就是很难的。



## 《漫画密码》

- 40、不错的漫画书 对了漫画密码那本不是学电脑技术和数学方面的千万不要买会看不懂的
- 41、好书，孩子很喜欢，
- 42、适合小朋友观看，呵呵，开玩笑了。  
主要是让大家有个简单的了解，很适合第一次讲课用
- 43、这种类型的书很好，看着不累，对知识吸收也快
- 44、此系列里相当有深度的一本
- 45、密码 密码
- 46、漫画XX系列里面比较好的，终于知道DES，RSA的具体加密过程了，数学也讲的挺清楚
- 47、哦，其实细节我都跳过了，因为看不懂。。。
- 48、这个系列没有什么可以说的
- 49、这一系列的书陆续买了五本，打算给孩子扩宽知识面的，也很吸引孩子动脑，漫画学起来有意思多了！
- 50、书中的内容非常好。让大人孩子都有收获。

# 《漫画密码》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:[www.tushu000.com](http://www.tushu000.com)