第一图书网, tushu007.com

# <<计算数论与现代密码学>>

## 图书基本信息

书名：<<计算数论与现代密码学>>

13位ISBN编号：9787040344714

10位ISBN编号：7040344718

出版时间：2013-1

出版时间：高等教育出版社

作者：颜松远

页数：418

字数：590000

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：http://www.tushu007.com

第一图书网, tushu007.com

# <<计算数论与现代密码学>>

## 前言

The book is about number theory and modem cryptography. More specically, it is about computational number theory and modem public-key cryptography based on number theory. It consists of four parts. The first part, consisting of two chapters, provides some preliminaries. Chapter 1 provides some basic concepts of number theory, computation theory, computational number theory, and modem public-key cryptography based on number theory. In chapter 2, a complete introduction to some basic concepts and results in abstract algebra and elementary number theory is given. The second part is on computational number theory. There are three chapters in this part.Chapter 3 deals with algorithms for primality testing, with an emphasis on the Miller-Rabin test, the elliptic curve test, and the AKS test. Chapter 4 treats with algorithms for integer factorization, including the currently fastest factoring algorithm NFS (Number Field Sieve), and the elliptic curve factoring algorithm ECM (Elliptic Curve Method). Chapter 5 discusses various modem algorithms for discrete logarithms and for elliptic curve discrete logarithms.It is well-known now that primality testing can be done in polynomial-time on a digital computer, however, integer factorization and discrete logarithms still cannot be performed in polynomial-time. From a computational complexity point of view, primality testing is feasible (tractable, easy) on a digital computer, whereas integer factorization and discrete logarithms are infeasible (intractable, hard, difficult). Of course, no-one has yet been able to prove that the integer factorization and the discrete logarithm problems must be infeasible on a digital computer. Building on the results in the first two parts, the third part of the book studies the modem cryptographic schemes and protocols whose security relies exactly on the infeasibility of the integer factorization and discrete logarithm problems. There are four chapters in this part.Chapter 6 presents some basic concepts and ideas of secret-key cryptography. Chapter 7 studies the integer factoring based public-key cryptography, including, among others, the most famous and widely used RSA cryptography, the Rabin cryptosystem, the probabilistic encryption and the zero-knowledge proof protocols. Chapter 8 studies the discrete logarithm based cryptography, including the DHM key-exchange protocol (the world's first public-key system), the E1Gamal cryptosystem, and the US Government's Digital Signature Standard (DSS), Chapter 9 discusses various cryptographic systems and digital signature schemes based on the infeasibility of the elliptic curve discrete logarithm problem, some of them are just the elliptic curve analogues of the ordinary public-key cryptography such as elliptic curve DHM, elliptic curve E1Gamal, elliptic curve RSA, and elliptic curve DSA/DSS.

第一图书网, tushu007.com

# <<计算数论与现代密码学>>

## 内容概要

数论和密码学是两个不同的学科，且分属于不同的研究领域，而现代公钥密码体制的创立和应用则将这两个不同的学科紧密地联系在一起。
这是因为这些密码体制的安全性几乎完全基于某些数论问题的难解性。
比如极负盛誉的rsa密码体制之所以难以破译，就是因为整数分解问题难以快速解决。
《计算数论与现代密码学》首先从计算理论的观点介绍数论中一些难解性问题，如整数分解问题和离散对数问题(包括椭圆曲线离散对数问题)，然后讨论基于这些难解性问题的现代公钥密码体制，最后讨论这些难解性问题的量子计算方法以及这些密码体制的量子攻击方法；由于量子计算仅适合于快速解决某些难解性数论问题(并非所有难解性的数论及数学问题)，因此还讨论了某些量子计算鞭长莫及的数学问题以及基于这些问题的抗量子密码体制。
此外，书中还配有大量实例和练习，便于读者学习和掌握。

《计算数论与现代密码学》可作为高等学校计算机、信息安全、电子与通信工程、数学等专业高年级本科生和研究生的教材，也可作为相关领域研究人员的参考书。

第一图书网, tushu007.com


## 作者简介

Song Y. Yan（颜松远），江西吉安人。
获中国科学院研究生院理学硕士学位，并获英国约克大学数学博士学位。
长期在国外大学从事计算数论、计算理论和密码学等方面的科研与教学工作，在Springer出版专著4部：1.《Number Theory for Computing》第1版（2000年）、第2版（2002年）、波兰文版（2006年，华沙国家科技出版社）、中文版（2007年，清华大学出版社）；2.《Primality Testing and Integer Factorization in Public-Key Cryptography》第1版（2004年）、第2版（2009年）；3.《Cryptanalytic Attacks on RSA》第1版（2007年）、俄文版（2010年，莫斯科国家科技出版中心）；4.《Quantum Attacks on Public-Key Cryptosystems》第1版（2012年）。

第一图书网, tushu007.com


## 书籍目录

part i preliminaries
1 introduction
1.1 what is number theory?
1.2 what is computation theory?
1.3 what is computational number theory?
1.4 what is modern cryptography?
1.5 bibliographic notes and further reading
references
2 fundamentals
2.1 basic algebraic structures
2.2 divisibility theory
2.3 arithmetic functions
2.4 congruence theory
2.5 primitive roots
2.6 elliptic curves
2.7 bibliographic notes and further reading
references
part ii computational number theory
3 primality testing
3.1 basic tests
3.2 miller-rabin test
3.3 elliptic curve tests
3.4 aks test
3.5 bibliographic notes and further reading
references
4 integer factorization
4.1 basic concepts
4.2 trial divisions factoring
4.3 p and p - 1 methods
4.4 elliptic curve method
4.5 continued fraction method
4.6 quadratic sieve
4.7 number field sieve
4.8 bibliographic notes and further reading
references
5 discrete logarithms
5.1 basic concepts
5.2 baby-step giant-step method
5.3 pohlig-hellman method
5.4 index calculus
5.5 elliptic curve discrete logarithms
5.6 bibliographic notes and further reading
references
part iii modern cryptography
6secret-key cryptography

第一图书网, tushu007.com


6.1 cryptography and cryptanalysis
6.2 classic secret-key cryptography
6.3 modern secret-key cryptography
6.4 bibliographic notes and further reading
references
7 integer factorization based cryptography
7.1 rsa cryptography
7.2 cryptanalysis of rsa
7.3 rabin cryptography
7.4 residuosity based cryptography
7.5 zero-knowledge proof
7.6 bibliographic notes and further reading
references
8 discrete logarithm based cryptography
8.1 diffie-heuman-merkle key-exchange protocol
8.2 e1gamal cryptography
8.3 massey-omura cryptography
8.4 dlp-based digital signatures
8.5 bibliographic notes and further reading
references
9 elliptic curve discrete logarithm based cryptography
9.1 basic ideas
9.2 elliptic curve diffie-hellman-merkle key exchange scheme
9.3 elliptic curve massey-omura cryptography
9.4 elliptic curve eigamal cryptography
9.5 elliptic curve rsa cryptosystem
9.6 menezes-vanstone elliptic curve cryptography
9.7 elliptic curve dsa
9.8 bibliographic notes and further reading
references
part iv quantum resistant cryptography
10 quantum computational number theory
10.1 quantum algorithms for order finding
10.2 quantum algorithms for integer factorization
10.3 quantum algorithms for discrete logarithms
10.4 quantum algorithms for elliptic curve discrete
logarithms
10.5 bibliographic notes and further reading
references
11 quantum resistant cryptography
11.1 coding-based cryptography
11.2 lattice-based cryptography
11.3 quantum cryptography
11.4 dna biological cryptography
11.5 bibliographic notes and further reading
references
index

第一图书网, tushu007.com

第一图书网, tushu007.com

# <<计算数论与现代密码学>>

## 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:http://www.tushu007.com