

Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов

# ТЕОРЕТИКО-ЧИСЛЕННЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Учебное пособие

институт фундаментальной подготовки



СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ  
SIBERIAN FEDERAL UNIVERSITY

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

**Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов**

## **ТЕОРЕТИКО-ЧИСЛЕННЫЕ МЕТОДЫ В КРИПТОГРАФИИ**

Рекомендовано Сибирским региональным учебно-методическим центром высшего профессионального образования для межвузовского использования в качестве учебного пособия для студентов, обучающихся по специальности 090102 «Компьютерная безопасность» и направлениям подготовки 090900 «Информационная безопасность» и 010200 «Математика и компьютерные науки» от 5 июля 2010 г.

Красноярск  
СФУ  
2011

УДК 519.72(075)  
ББК 32.811я73  
К53

*Рецензенты:*

**И. О. Богульский**, ведущий научный сотрудник ИВМ СОРАН,  
д-р физ.-мат. наук, проф.;

**Ю. В. Шорников**, д-р техн. наук, проф. кафедры АСУ новоси-  
бирского государственного технического университета

**Кнауб, Л. В.**  
К53 Теоретико-численные методы в криптографии : учеб. пособие /  
Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов. – Красноярск : Сибирский фе-  
деральный университет, 2011. – 160 с.  
ISBN 978-5-7638-2113-7

Излагаются некоторые элементы теории чисел, отношения сравнимости, мо-  
дулярная арифметика, степенные вычеты, первообразные корни, индексы, алго-  
ритмы дискретного логарифмирования, китайская теорема об остатках, простые  
числа и проверка на простоту, разложение чисел на множители и арифметические  
операции над большими числами. В прил. 1 описаны основы теории групп, колец  
и полей, а в прил. 2 приведены реализации некоторых алгоритмов, даны тексты  
программ на языке Borland C++, снабженные подробными комментариями.

Для студентов, обучающихся по специальности 090102 «Компьютерная  
безопасность» и направлениям подготовки 090900 «Информационная безопас-  
ность» и 010200 «Математика и компьютерные науки».

УДК 519.72(075)  
ББК 32.811я73

Учебное издание

**Кнауб Людмила Владимировна, Новиков Евгений Александрович  
Шитов Юрий Александрович**

## **ТЕОРЕТИКО-ЧИСЛЕННЫЕ МЕТОДЫ В КРИПТОГРАФИИ**

Редактор Т. М. Пыжик  
Компьютерная вёрстка Д. Р. Мифтахутдинова

Подписано в печать 06.06.2011. Печать плоская. Формат 60×84/16  
Бумага офсетная. Усл. печ. л. 9,3. Тираж 100 экз. Заказ № 2481

Редакционно-издательский отдел Библиотечно-издательского комплекса  
Сибирского федерального университета. 660041, г. Красноярск, пр. Свободный, 79

Отпечатано полиграфическим центром Библиотечно-издательского комплекса  
Сибирского федерального университета. 660041, г. Красноярск, пр. Свободный, 82а

ISBN 978-5-7638-2113-7

© Сибирский федеральный университет, 2011

## ВВЕДЕНИЕ

Основой данного пособия является курс лекций по теоретико-численным методам в криптографии (ТЧМК). Этот курс предназначен для студентов ИКИТ кафедры прикладной математики и компьютерной безопасности, которые специализируются по информационной безопасности. Лекции по данному предмету формировались с 1996 года. Надо сказать, что в то время литературы на русском языке по таким направлениям, как защита информации, криптографии и математическим методам в криптографии практически не было (в отличие от зарубежных изданий). Поэтому на первом этапе «скелет» курса формировался на элементах теории чисел, алгоритмах арифметических операций с длинными числами и криптографических алгоритмах с открытыми ключами (RSA, схема Диффи – Хеллмана, схема Эль-Гамала, схема аутентификации Шнора). Постепенно в тексты лекций, начиная с 2000 года, включались численные алгоритмы для решения трудных задач теории чисел. Для этого использовались переводы из зарубежных изданий по соответствующей тематике. В 2003 году Ю. А. Шитов издал методические указания по изучению численных алгоритмов для некоторых задач из теории чисел, которые использовались в курсе лекций по ТЧМК [15].

С 2001 года по направлениям «Криптография и математические методы в криптографии» начинают появляться учебные пособия и монографии на русском языке. В библиографическом списке приведен, по мнению авторов, достаточно полный обзор существующей литературы по этому направлению. В список не включены те учебники, в которых содержатся главы и разделы по арифметическим алгоритмам в теории чисел, так как любое учебное пособие по классическим курсам представляет собой аранжировку давно сформулированных и доказанных результатов, поэтому мы широко используем материалы из учебников, перечисленных в библиографическом списке.

Данное пособие отличается порядком и простотой изложения. Немного больше, чем в других пособиях, уделяется внимание решениям сравнений. Кроме того, при изложении результатов исключаются из рассмотрения доказательства некоторых трудных теорем, поскольку при желании слушатели курса могут ознакомиться с доказательствами в перечисленных источниках. При выборе материала авторы исходили из минимальных требований к начальной подготовке слушателей данного курса. Авторы предлагаемого пособия делают упор на возможность практической реализации изложенных алгоритмов на компьютере. Для некоторых алгоритмов, сформулированных в пособии, в приложении даны тексты программ, реализованных на языке BORLAND C++. Программы реализовал и тестировал М. В. Рыбков – студент группы ВТ 05–04, ИКИТ, СФУ.

Нумерация определений, теорем и соотношений приведены в разделах пособия.

## ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	2
НЕКОТОРЫЕ ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ.....	4
ВЫЧИСЛЕНИЕ НАИБОЛЬШЕГО ОБЩЕГО ДЕЛИТЕЛЯ .....	9
Алгоритм Евклида.....	9
Бинарный алгоритм Евклида .....	9
Расширенный алгоритм Евклида.....	10
Вариант расширенного алгоритма Евклида .....	10
ОТНОШЕНИЕ СРАВНИМОСТИ .....	14
МОДУЛЯРНАЯ АРИФМЕТИКА.....	16
КЛАССЫ.....	17
Полная и приведенная система вычетов.....	18
Функция Эйлера.....	19
СРАВНЕНИЯ ПЕРВОЙ СТЕПЕНИ.....	24
КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ .....	27
Криптосистема RSA.....	28
Формирование системы RSA.....	30
Алгоритм шифрования .....	30
Алгоритм дешифрования .....	30
Цифровая подпись.....	30
СТЕПЕННЫЕ ВЫЧЕТЫ .....	35
ПЕРВООБРАЗНЫЕ КОРНИ .....	46
ИНДЕКСЫ .....	47
АЛГОРИТМ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ .....	53
Задача дискретного логарифмирования в конечном поле .....	53
$p$ -метод Полларда.....	53
Схема Эль – Гамала .....	55
Схема Шнорра .....	56
КИТАЙСКАЯ ТЕОРЕМА ОБ ОСТАТКАХ .....	59
СРАВНЕНИЯ СТЕПЕНЕЙ ВЫШЕ ПЕРВОГО .....	63
СРАВНЕНИЯ ПО СОСТАВНОМУ МОДУЛЮ .....	70
ДВУЧЛЕННЫЕ СРАВНЕНИЯ .....	72
СРАВНЕНИЯ ВТОРОЙ СТЕПЕНИ ПО ПРОСТОМУ МОДУЛЮ И КВАДРАТИЧНЫЕ ВЫЧЕТЫ .....	76
Алгоритм вычисления символа Якоби .....	84
ВЫЧИСЛЕНИЕ КВАДРАТНЫХ КОРНЕЙ ПО МОДУЛЮ .....	88
Случай простого модуля .....	88
Случай составного модуля.....	91
Вычисление квадратных корней по составному модулю .....	96
ЦИФРОВАЯ ПОДПИСЬ ФИАТА – ШАМИРА .....	98
ПРОСТЫЕ ЧИСЛА .....	100
ПРОВЕРКА НА ПРОСТОТУ .....	102
Пробное деление .....	102

Решето Эратосфена .....	102
Тест на основе малой теоремы Ферма .....	103
Схема алгоритма на базе малой теоремы Ферма .....	103
Тест Соловея – Штрассена .....	104
Схема алгоритма на базе малой теоремы Ферма .....	104
Тест Рабина – Миллера .....	104
Схема алгоритма Рабина – Миллера .....	105
Построение больших простых чисел и детерминированные алгоритмы проверки чисел на простоту .....	106
Проверка чисел Мерсенна на простоту .....	107
РАЗЛОЖЕНИЕ ЧИСЕЛ НА МНОЖИТЕЛИ .....	108
Метод пробного деления .....	108
Факторизация Ферма .....	109
$p$ -метод Полларда .....	111
$(p-1)$ -метод Полларда .....	113
АРИФМЕТИЧЕСКИЕ ОПЕРАЦИИ НАД БОЛЬШИМИ ЧИСЛАМИ ....	116
Сложение .....	116
Вычитание .....	117
Умножение .....	117
Деление .....	118
Модифицированное деление столбиком .....	118
Модульное умножение .....	119
Метод Монтгомери .....	119
БИБЛИОГРАФИЧЕСКИЙ СПИСОК .....	122
Приложение 1. ГРУППЫ, КОЛЬЦА, ПОЛЯ .....	123
Группы .....	123
Кольца. Поля. Многочлены над полем .....	127
Приложение 2. РЕАЛИЗАЦИЯ АЛГОРИТМОВ .....	132
Описание .....	132
Решение сравнения .....	132
Алгоритм Евклида .....	136
Бинарный алгоритм Евклида .....	138
Расширенный алгоритм Евклида .....	139
Вычисление символа Якоби .....	141
Вычисление символа Лежандра .....	143
Решето Эратосфена .....	145
Пробное деление .....	146
Тест на основе малой теоремы Ферма .....	147
Тест Соловея – Штрассена .....	149
Тест Рабина – Миллера .....	151
Метод $p-1$ Полларда .....	153
Метод $p$ -Полларда .....	155
Факторизация Ферма (разность квадратов) .....	157