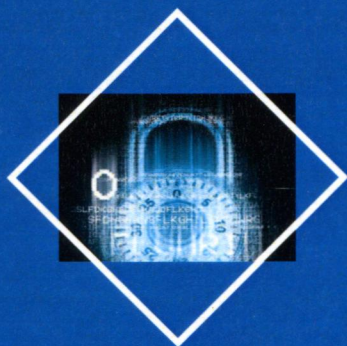


В. А. Романьков

**АЛГЕБРАИЧЕСКАЯ
КРИПТОЛОГИЯ**



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
им. Ф.М. ДОСТОЕВСКОГО

В. А. Романьков

АЛГЕБРАИЧЕСКАЯ КРИПТОЛОГИЯ

Монография

Омск



2020

УДК 512.624.95

ББК 22.176

P697

*Издание осуществлено при финансовой поддержке
Российского фонда фундаментальных исследований
по проекту № 20-11-00007, не подлежит продаже*



Рецензенты:

д-р физ.-мат. наук, проф. А. Г. Мясников;

д-р физ.-мат. наук, проф. В. Н. Ремесленников;

д-р физ.-мат. наук, проф. Е. И. Тимошенко

Романьков, В. А.

P697 Алгебраическая криптология : монография / В. А. Романьков. –
Омск : Изд-во Ом. гос. ун-та, 2020. – 262 с.

ISBN 978-5-7779-2491-9

Содержит теоретические основы и описания известных теоретико-числовых и алгебраических конструкций в криптологии. Приводятся схемы, системы и протоколы, описываются методы их анализа, даются примеры такого анализа. Кроме того, монография содержит описания новых криптографических схем и алгоритмов, разработанных автором как в теоретико-числовой, так и в алгебраической криптологии. В основном излагаются достижения последних пяти лет. Упор делается на алгебраические аспекты, что объясняет ее название.

Адресована специалистам в алгебре и криптологии. Может быть полезной для студентов и аспирантов, изучающих эти предметы, а также для преподавателей соответствующих курсов и разработчиков практических алгоритмов криптографии. Кроме того, может стать основой для дальнейших теоретических исследований.

The monograph is addressed to specialists in algebra and cryptology. It may be useful for students and post-graduate students studying these subjects, as well as for teachers of relevant courses. It can also be useful for developers of practical algorithms for cryptology and the basis for further theoretical research. The monograph contains the theoretical foundations and descriptions of well-known number-theoretic and algebraic constructions in cryptology. Schemes, systems and protocols are presented, methods for their analysis are described, and examples of such analysis are given. In addition, the monograph contains descriptions of new cryptographic schemes and algorithms developed by the author in both number-theoretic and algebraic cryptology. Mostly the monograph outlines the achievements of the past five years. The emphasis is on algebraic aspects, which explains the name of the monograph.

УДК 512.624.95

ББК 22.176

ISBN 978-5-7779-2491-9

© Романьков В. А., 2020

© ФГБОУ ВО «ОмГУ

им. Ф. М. Достоевского», 2020

ОГЛАВЛЕНИЕ

Предисловие	7
Введение	13
1. Базовые сведения о теоретико-числовой криптографии ...	16
1.1. Основные понятия	16
1.1.1. Системы шифрования	16
1.1.2. Идея шифрования с открытым ключом	18
1.2. Основные схемы теоретико-числовой криптографии на кольцах вычетов	19
1.2.1. Система Ривеста–Шамира–Адлемана (RSA)	19
1.2.2. Система Гольдвассер–Микали	22
1.2.3. Система Рабина	24
1.2.4. Система Пэйн	26
1.3. Основные схемы теоретико-числовой криптографии на конечных полях	28
1.3.1. Протокол Диффи–Хеллмана	29
1.3.2. Протокол Масси–Омуры	30
1.3.3. Протокол Эль-Гамала	31
1.4. Электронная (цифровая) подпись	32
1.4.1. Подпись на базе RSA	32
1.4.2. Схема базовой электронной подписи Эль-Гамала	35
1.5. Аутентификация	37
1.6. Диофантова криптография	38
1.6.1. 10-я проблема Гильберта	38
1.6.2. Универсальность диофантова языка	39
2. Базовые сведения об алгебраической криптографии	44
2.1. Платформы и алгоритмические проблемы	44
2.1.1. Постановка алгоритмических проблем	46
2.1.2. Неразрешимые и трудноразрешимые алгоритмические проблемы как основа для построения криптографических схем	51
2.1.3. О сложности алгоритмических проблем и соответствующих им проблем поиска	52
2.1.4. Асимптотическая плотность	56
2.2. Основные схемы алгебраической криптографии	59
2.2.1. Схемы, основанные на трудноразрешимости проблемы поиска сопрягающего элемента	59
2.2.2. Протокол Ко и др.	60

2.2.3. Протокол Аншель – Аншеля – Голдфельда	61
2.2.4. Схемы, основанные на трудноразрешимости проблем, связанных с домножениями: общие сведения	62
2.2.5. Протокол распределения ключа Сидельникова – Черепнева – Яценко	64
2.2.6. Протокол распределения ключа Стикеля	64
2.2.7. Общая схема, использующая двусторонние домножения	65
2.2.8. Схемы, основанные на трудноразрешимости проблем, связанных с действиями автоморфизмами и эндоморфизмами: общие сведения	67
2.2.9. Протокол Росошека	68
2.2.10. Протокол Махалонобиса	69
2.2.11. Общая криптографическая схема, использующая автоморфизмы группы	70
3. Методы алгебраического криптографического анализа	71
3.1. Базовые сведения	71
3.2. Метод линейного разложения	76
3.3. Ключевая идея	78
3.3.1. Построение базиса	78
3.3.2. Базовая идея атаки методом линейного разложения	80
3.3.3. Линейная группа, действующая сопряжением	81
3.3.4. Линейная группа, действующая левыми/правыми домножениями	83
3.3.5. Группы, действующие автоморфизмами	84
3.3.6. Сложность предложенных алгоритмов	86
3.4. Протоколы, использующие домножения и сопряжения	87
3.4.1. Криптографический анализ общей схемы, использующей двусторонние домножения	87
3.4.2. Криптографический анализ протокола распределения ключа Ванга и др.	91
3.4.3. Криптографический анализ протокола распределения ключа Ко и др.	93
3.4.4. Криптографический анализ протокола Б. и Т. Харли ...	93
3.5. Протоколы, использующие автоморфизмы группы	95
3.5.1. Криптографический анализ общей схемы, использующей автоморфизмы группы методом линейного разложения	95
3.5.2. Криптографический анализ протокола Росошека	99
3.5.3. Криптографический анализ общей схемы, использующей автоморфизмы методом нелинейного разложения ...	100

3.5.4. Криптографический анализ протокола Махаланобиса ...	103
3.5.5. Криптографический анализ протокола Мазе и др.	104
3.5.6. Криптографический анализ протокола Шпильрайна и др. 106	
3.5.7. Криптографический анализ протокола Росошека рас- пределения ключа ММС	108
3.5.8. Криптографический анализ протокола выработки обще- го ключа Маркова и др.	117
3.5.9. Криптографический анализ протокола выработки обще- го ключа Грибова и др.	120
3.5.10. Криптографический анализ протокола выработки об- щего ключа Михалева и др.	124
3.6. Метод линейного анализа Тсабана.	126
3.6.1. Криптографический анализ протокола ААG	130
3.6.2. Криптографический анализ системы Пекер	133
3.6.3. Криптографический анализ протокола Ко и др.	137
4. Новые схемы теоретико-числовой криптографии	138
4.1. Базовые сведения	138
4.2. Некоторые проблемы для мультипликативных групп конечных полей и колец вычетов	140
4.3. Скрытые множители в конечных полях и кольцах вычетов ...	143
4.3.1. Базовая схема вероятностного подгруппового зашифро- вания, основанного на трудноразрешимости проблемы порядка элемента	143
4.3.2. Новая версия системы, подобной RSA, использующая скрытые множители	145
4.3.3. Криптоанализ предлагаемой системы	149
4.3.4. Вероятностное шифрование на базе протокола Диффи – Хеллмана	150
4.4. Вероятностное шифрование на базе протокола Эль-Гамала ...	151
4.5. Улучшенная версия криптографической системы Рабина	152
4.5.1. Простой способ сделать систему Рабина полностью опре- деленной	152
4.5.2. Версия системы, использующей скрытые множители, аналогичной системе Рабина	153
5. Новые схемы алгебраической криптографии	154
5.1. Новый метод усиления схем алгебраической криптографии ...	154
5.1.1. Маргинальные подмножества	155
5.1.2. Усиленная версия протокола Аншеля и др.	156
5.1.3. Усиленная версия протокола Ко и др.	159

6. Разное	167
6.1. Система Файна–Модденауэр–Розенбергера	167
6.1.1. Описание системы.....	168
6.1.2. Криптоанализ системы.....	171
6.2. Полилинейные системы на нильпотентных группах.....	183
6.2.1. Дискретный логарифм в нильпотентной группе	183
6.2.2. Криптоанализ полилинейных систем.....	188
6.3. Односторонние функции	192
6.4. 10-я проблема Гильберта и проблема эндоморфной сводимости	197
6.5. Общая схема построения односторонних функций	203
6.6. Протокол аутентификации Григорьева–Шпильрайна	205
6.7. Двукратная проблема эндоморфной сводимости	207
6.8. Свободные метабелевы группы	207
6.8.1. Интерпретация диофантовых уравнений в метабелевых группах.....	214
6.8.2. Кодирование текстов в свободных метабелевых группах .	232
6.9. Цифровая подпись.....	235
6.9.1. Группа кос и E -умножение.....	236
6.9.2. Генерация ключей.....	238
6.9.3. Генерация подписи и ее проверка	239
Литература	240
Summary	259