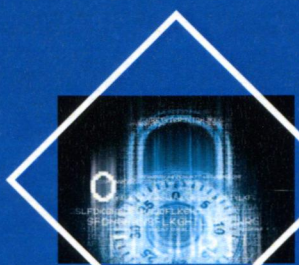
РФФИ

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
Р697

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.

Р697 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

ОГЛАВЛЕНИЕ