ВЫСШЕЕ ОБРАЗОВАНИЕ

ВВЕДЕНИЕ В ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

М. М. Глухов
И. А. Круглов
А. Б. Пичкур
А. В. Черемушкин

ЛАНЬ

E.LANBOOK.COM

М. М. ГЛУХОВ, И. А. КРУГЛОВ,
А. Б. ПИЧКУР, А. В. ЧЕРЕМУШКИН

ВВЕДЕНИЕ В ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ

УЧЕБНОЕ ПОСОБИЕ
Издание второе, стереотипное

РЕКОМЕНДОВАНО
УМО по образованию в области технологии сырья и продуктов животного происхождения в качестве учебного пособия для студентов высших учебных заведений, обучающихся по специальности «Пищевая биотехнология».

ЛАНЬ
САНКТ-ПЕТЕРБУРГ · МОСКВА · КРАСНОДАР
2024

УДК 003.26
ББК 22.131я73

В 24 Введение в теоретико-числовые методы криптографии : учебное пособие для вузов / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — 2-е изд., стер. — Санкт-Петербург : Лань, 2024. — 396 с. — Текст : непосредственный.

ISBN 978-5-507-47610-7

Учебное пособие содержит полное изложение материала учебной дисциплины «Теоретико-числовые методы в криптографии» Государственного образовательного стандарта высшего профессионального образования по направлению подготовки «Компьютерная безопасность».

Основу учебного пособия составляют результаты элементарной теории чисел (главы 1–4). В последующих главах рассматривается материал, имеющий многочисленные приложения в современной криптографии: проверка простоты целых чисел, разложение целых чисел на множители, эллиптические кривые, дискретное логарифмирование, теория целочисленных решеток. Особое внимание в пособии уделено алгоритмическим аспектам теории чисел.

Предназначено для студентов вузов, обучающихся по направлениям подготовки в области информационной безопасности, а также для аспирантов.

УДК 003.26
ББК 22.131я73

Рецензенты:
В. П. ЗЯЗИН, профессор кафедры «Информационная безопасность» МИРЭА, кандидат физико-математических наук;
Э. А. ПРИМЕНКО, доцент кафедры математической кибернетики факультета ВМК МГУ им. М. В. Ломоносова.

Обложка
П. И. ПОЛЯКОВА

ОГЛАВЛЕНИЕ