Содержание

Введение 3

ГЛАВА 1. Элементы абстрактной алгебры 4
§1.1. Алгоритм Евклида 4
§1.2. Группы: примеры и простейшие свойства 5
§1.3. Кольца и поля: примеры и простейшие свойства . . . 12
§1.4. Основные понятия теории групп 17
§1.5. Структура кольца $\mathbb{Z}_m$ и его мультипликативной группы 24

ГЛАВА 2. Элементы компьютерной алгебры 31
§2.1. Эффективность алгоритмов. Понятие сложности алгоритма 31
§2.2. Расширенный алгоритм Евклида 35
§2.3. Модулярная арифметика 41
§2.4. Разложение натурального числа на простые множители 54
§2.5. Вычисление значения многочлена 62
§2.6. Умножение многочленов 69

ГЛАВА 3. Элементы криптографии 79
§3.1. Историческая справка. Основные понятия 79
§3.2. Классификация шифров 81
§3.3. Примеры шифров 86
§3.4. Криптосистема RSA 93

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА 99