Оглавление

Введение 3
ГЛАВА 1. Элементы абстрактной алгебры 5
§1. Алгоритм Евклида 5
§2. Группы и кольца 6
§3. Примеры групп и колец 8
§4. Основные понятия теории групп 15
§5. Структура кольца $\mathbb{Z}_m$ и его мультипликативной группы 19
ГЛАВА 2. Элементы компьютерной алгебры 28
§1. Эффективность алгоритмов. Понятие сложности алгоритма 28
§2. Расширенный алгоритм Евклида 32
§3. Модулярная арифметика 37
§4. Разложение натурального числа на простые множители 47
§5. Вычисление многочлена 55
§6. Умножение многочленов 59
ГЛАВА 3. Элементы криптографии 69
§1. Историческая справка. Основные понятия 69
§2. Примеры шифров. 70
§3. Криптосистема RSA 78
§4. Криптосистема без передачи ключей 81
РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА 86