Оглавление

Предисловие 7

Глава 1. **Факторизация целых чисел с помощью эллиптических кривых** 10
§ 1.1. Криптосистема RSA 12
§ 1.2. Общие сведения об эллиптических кривых . . 22
§ 1.3. Эллиптические кривые над полем рациональных чисел 32
§ 1.4. Эллиптические кривые над конечными полями $\mathbb{F}_p$ 36
§ 1.5. Факторизационный алгоритм Ленстры 39

Глава 2. **Дискретное логарифмирование и гиперэллиптические кривые** 48
§ 2.1. Первообразные корни. Индексы 50
§ 2.2. Дискретное логарифмирование в мультипликативных группах конечных полей 55
§ 2.3. Дискретный логарифм на эллиптических кривых 60
§ 2.4. Гиперэллиптические кривые 63
§ 2.5. Функции на гиперэллиптической кривой 66
§ 2.6. Дивизоры и якобианы 77
§ 2.7. Сложение приведенных дивизоров 82
§ 2.8. Дзета-функция гиперэллиптической кривой . . 87
§ 2.9. Дискретный логарифм на якобианах гиперэллиптических кривых 92
§ 2.10. Случай большого простого поля 95

ГЛАВА 3. **Проверка целых чисел на простоту** 99
§ 3.1. Проверка на составленность. Алгоритм Миллера 100
§ 3.2. Алгоритм Поклингтона – Лемера 102
§ 3.3. Проверка на простоту с помощью эллиптических кривых 105
§ 3.4. Групповые кольца круговых полей, суммы Гаусса и Якоби 111
§ 3.5. Критерий простоты 117
§ 3.6. Применение сумм Якоби 123
§ 3.7. Описание алгоритма Адлемана – Ленстры 131

ГЛАВА 4. **Эллиптические интегралы и итерационные алгоритмы** 138
§ 4.1. Арифметико-геометрическое среднее 139
§ 4.2. Эллиптические интегралы 144
§ 4.3. Основные свойства полных эллиптических интегралов 151
§ 4.4. Соотношение Лежандра 159
§ 4.5. Тэта-функции и арифметико-геометрическое среднее 163
§ 4.6. Алгоритм для вычисления π 172
§ 4.7. Итерационные алгоритмы высших порядков . . 179

Литература 184