

<b>Предисловие</b> . . . . .	<b>7</b>
<b>Глава 1. Введение</b> . . . . .	<b>9</b>
1.1. Криптография с открытым ключом . . . . .	9
1.2. Группы, кольца, поля . . . . .	15
1.2.1. Группы . . . . .	15
1.2.2. Кольца. Поля. Многочлены над полем . . . . .	23
1.2.3. Алгоритм Евклида и его варианты . . . . .	26
<b>Глава 2. Конечные поля и эллиптические кривые</b> . . . . .	<b>38</b>
2.1. Поля Галуа . . . . .	38
2.1.1. Характеристика поля . . . . .	39
2.1.2. Мультипликативная группа конечного поля . . . . .	40
2.1.3. Конечное расширение поля . . . . .	42
2.1.4. Поле разложения многочлена . . . . .	46
2.1.5. Минимальные многочлены. Существование неприводимых многочленов . . . . .	48
2.1.6. След и норма элемента конечного поля . . . . .	55
2.1.7. Алгоритмическое представление конечного поля . . . . .	56
2.1.8. Поле Галуа как векторное пространство . . . . .	58
2.1.9. Проверка, является ли нормальная система базисом. Переход от нормального базиса к стандартному . . . . .	62
2.1.10. Переход от стандартного базиса к нормальному . . . . .	64
2.1.11. О быстрой линейной алгебре . . . . .	65
2.1.12. Быстрый алгоритм для решения систем линейных уравнений над конечным полем . . . . .	69
2.1.13. Оптимальные и гауссовы нормальные базисы . . . . .	70
2.1.14. Алгебраическое замыкание конечного поля . . . . .	73
2.1.15. Квадратичные вычеты и извлечение квадратных корней в конечных полях . . . . .	74
2.2. Эллиптические кривые . . . . .	82
2.2.1. Алгебраические кривые и эллиптические кривые . . . . .	82
2.2.2. Группа точек эллиптической кривой . . . . .	89
2.2.3. Эллиптические кривые над полями действительных и рациональных чисел . . . . .	99
2.3. Эллиптические кривые над конечными полями . . . . .	104
2.3.1. Порядок эллиптической кривой . . . . .	104
2.3.2. Легко ли вычислить порядок группы точек эллиптической кривой . . . . .	104

2.3.3. Применения теоремы Хассе	105
2.3.4. О структуре групп эллиптических кривых	109
<b>Глава 3. Неприводимые многочлены</b>	<b>111</b>
3.1. Тестирование и поиск неприводимых многочленов	111
3.1.1. Чем интересны неприводимые многочлены	111
3.1.2. Тест на неприводимость. Алгоритм Берлекемпа	112
3.1.3. Оценка сложности алгоритма Евклида	113
3.1.4. Тестирование неприводимости многочленов	114
3.1.5. О тестировании неприводимости многочленов малого веса	116
3.1.6. Асимптотически быстрый алгоритм тестирования неприводимости многочленов	122
3.1.7. Вероятностные алгоритмы тестирования неприводимости многочленов	129
3.1.8. Генерация неприводимых многочленов	131
3.2. Тестирование примитивных многочленов	132
3.2.1. Тестирование примитивности неприводимого многочлена	132
3.2.2. Генерация примитивных многочленов	134
3.2.3. Генерация примитивных элементов в поле $GF(p^n)$	135
3.3. Алгоритмы вычисления минимального многочлена	137
3.3.1. О сложности вычисления минимальных многочленов	137
3.3.2. Быстрый алгоритм вычисления минимального многочлена	138
3.4. Генерация нормальных базисов	140
3.4.1. Критерии базисности нормальной системы	140
3.4.2. Быстрое тестирование базисности нормальных систем	142
3.4.3. О нормальных базисах, порождаемых многочленами малого веса	144
<b>Глава 4. Арифметика <math>GF(2^n)</math> в полиномиальном базисе</b>	<b>146</b>
4.1. Особенности реализации операций	146
4.1.1. Выбор поля и способов реализации	146
4.2. Классический алгоритм умножения в $GF(2)[X]$	150
4.2.1. Элементарные многочлены. Таблица умножения	150
4.2.2. Умножение многочленов с использованием таблицы умножения	152
4.2.3. Модификация классического алгоритма и гибридный алгоритм умножения	154
4.2.4. Еще две модификации классического алгоритма умножения	156
4.3. Алгоритм Карацубы и его реализация	162
4.3.1. О методе Карацубы	162
4.3.2. Умножение многочленов по методу Карацубы	162
4.3.3. Декомпозиционная схема умножения многочленов над $GF(2)$	163
4.3.4. Умножение многочленов	164
4.4. Приведение по модулю неприводимого многочлена	168
4.4.1. Классический алгоритм деления многочленов	168

4.4.2.	Приведение многочлена по модулю многочлена малого веса . . .	170
4.4.3.	Обобщение алгоритма . . . . .	175
4.4.4.	Приведение по модулю многочлена высокого веса . . . . .	180
4.5.	Возведение в степень и инвертирование . . . . .	182
4.5.1.	Возведение в степень $2^m$ в стандартном базисе . . . . .	182
4.5.2.	Инвертирование в полиномиальном или нормальном базисах . .	182
4.5.3.	Быстрый алгоритм возведения в степень в стандартном базисе . . . . .	185
4.5.4.	Быстрое инвертирование в стандартном базисе поля $GF(p^n)$ . . .	189
4.5.5.	Быстрое программное инвертирование на основе алгоритма Евклида . . . . .	189
4.5.6.	Деление с помощью алгоритма Евклида . . . . .	192
4.6.	Асимптотически быстрые алгоритмы . . . . .	192
4.6.1.	Быстрое умножение чисел и многочленов . . . . .	192
4.6.2.	Аддитивные цепочки . . . . .	196
4.6.3.	Приложения аддитивных цепочек . . . . .	204
4.6.4.	Аддитивные цепочки с вычитаниями . . . . .	206
4.6.5.	Алгоритмы возведения в степень с фиксированной базой . . . . .	209
4.6.6.	Ускорение проверки электронной подписи . . . . .	213
4.6.7.	Метод Монтгомери быстрого возведения в степень . . . . .	214
4.6.8.	Пример реализации метода Монтгомери логическими схемами . . . . .	216
4.6.9.	Быстрое возведения в степень через модулярную композицию . .	219
4.6.10.	Быстрое инвертирование в стандартном базисе через модулярную композицию . . . . .	222
4.6.11.	Некоторые уточнения в случае $q = 2$ . . . . .	223
<b>Глава 5.</b>	<b>Арифметика в нормальных базисах . . . . .</b>	<b>226</b>
5.1.	Оптимальные нормальные базисы . . . . .	226
5.1.1.	Три типа оптимальных нормальных базисов . . . . .	226
5.1.2.	Некоторые примеры примитивных элементов по модулю $p$ . . .	227
5.1.3.	Алгоритм генерации оптимальных нормальных базисов первого типа и доказательство их оптимальности . . . . .	228
5.1.4.	Алгоритм генерации оптимальных нормальных базисов второго типа и доказательство их оптимальности . . . . .	232
5.1.5.	Алгоритм генерации оптимальных нормальных базисов третьего типа и доказательство их оптимальности . . . . .	237
5.2.	Оптимизация преобразований базисов . . . . .	242
5.2.1.	О комбинированном использовании полиномиального и нормального базисов . . . . .	242
5.2.2.	Пример выполнения алгоритма перехода от оптимального базиса первого типа к стандартному и обратно . . . . .	245
5.2.3.	Примеры построения логических схем для умножения в стандартном и оптимальном нормальном базисе первого типа . . . . .	246

5.2.4.	Оценка сложности перехода от оптимальных нормальных базисов второго и третьего типа к стандартным и обратно . . . .	250
5.2.5.	О явном вычислении формул перехода и минимальных многочленов для оптимальных нормальных базисов . . . . .	261
5.2.6.	Оценка сложности перехода от оптимальных нормальных базисов второго и третьего типа к стандартным в общем случае . . . . .	266
5.2.7.	Пример выполнения алгоритма перехода от оптимального базиса 2-го или 3-го типа к стандартному и обратно . . . . .	266
5.2.8.	Замечание о программной реализации . . . . .	270
5.2.9.	О сложности арифметических операций в конечных полях . . . .	271
5.2.10.	Об оценках сложности возведения в степень и инвертирования в конечных полях . . . . .	273
5.3.	<b>Гауссовы нормальные базисы</b> . . . . .	274
5.3.1.	Построение гауссовых нормальных базисов . . . . .	274
5.3.2.	Сложность умножения, инвертирования и возведения в степень в ГНБ . . . . .	278
5.3.3.	Гауссовы базисы и гауссовы периоды . . . . .	280
5.3.4.	Еще один вывод таблицы умножения для ГНБ . . . . .	283
5.3.5.	Примеры гауссовых нормальных базисов в полях $GF(2^n)$ . . . .	285
5.3.6.	Порядки генераторов базисов низкой сложности и быстрый алгоритм возведения в степень . . . . .	292
5.3.7.	О сложности порождения нормальных базисов, примитивных элементов и неприводимых многочленов . . . . .	294
5.3.8.	Редундантные базисы . . . . .	296
5.4.	<b>Операции в нормальных базисах</b> . . . . .	301
5.4.1.	Пример построения схемы для умножения и инвертирования в оптимальных нормальных базисах второго типа . . . . .	301
5.4.2.	Пример схемного инвертирования с использованием редундантного базиса . . . . .	306
5.4.3.	Пример схемы умножения в ГНБ . . . . .	307
5.4.4.	Быстрое программное инвертирование с помощью ГНБ . . . . .	308
	<b>Литература</b> . . . . .	312
	<b>Предметный указатель</b> . . . . .	321
	<b>Уточнения и дополнения к первому изданию</b> . . . . .	325