ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Федеральное государственное образовательное учреждение
высшего профессионального образования
СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Методические указания к самостоятельной работе

Красноярск 2008

Криптографические методы защиты информации: Методические указания к самостоятельной работе по освоению дисциплины «Криптографические методы защиты информации» для подготовки студентов по направлению 230100.68 – «Информатика и вычислительная техника» по магистерской программе 230100.68.25 – «Безопасность и защита информации»

Авторы: Е.А. Новиков, С.Ф. Пятаев

Рекомендации

Структура методического указания по самостоятельной работе студентов условно разделена на две части. В первой части предлагаются возможные самостоятельные работы по разделам программы, во второй – конкретный набор самостоятельных работ для разработанного курса. По желанию преподаватель, в зависимости от уровня подготовки студентов, может добавлять или заменять отдельные виды работ из второй части.

Студент должен завести папку, в которую по разделам фиксируется этапы самостоятельной работы по изучению криптографических методов защиты информации.

При выполнении работы студент может включать дополнительный материал, с которым он ознакомился самостоятельно и который не был включен в данное методическое указание.

Желательно, чтобы студент указывал материал, который для него был интересен в процессе самостоятельной работы, но с которым он не сумел основательно разобраться.

При выполнении каждого раздела самостоятельной работы студент должен указать источники, которые он использовал при ее выполнении, а также номера страниц, из которых он черпал данный материал.

Если студент не нашел указанную в методическом руководстве литературу, то он должен самостоятельно найти доступные источники для изучения соответствующей темы. Можно использовать Интернет.

З а м е ч а н и е. Нумерация самостоятельных работ совпадает с номерами разделов учебной программы по дисциплине «Криптографические методы защиты информации», в которой данные работы запланированы.

В завершение общего списка возможных самостоятельных работ предлагаются усложненные самостоятельные работы для разработанного курса.

Раздел 1. История криптографии, основные понятия криптографии, классификация шифров

В результате развития криптографии возникли и совершенствовались следующие классы шифров:

- простая замена;
- замена для блока символов;
- многоалфавитная замена;
- перестановка;
- маршрутная перестановка.

Задание на самостоятельную работу

Создать информационную систему, в которой присутствуют все классы перечисляемых шифров. Выбор шифров из перечисляемых классов свободный. В оболочке информационной системы надо предусмотреть:

- выбор метода шифрования или дешифрования;
- способ задания ключа по умолчанию или определяется пользователем;
- удобные способы ввода начальной информации и вывода результатов работы системы.

Составить наиболее полный список (базу данных) способов (алгоритмов) шифрования, которые использовались в процессе исторического развития криптографии. В списке алгоритмы должны быть сгруппированы по классам (замены, перестановки, блочные и т.д.). Каждый шифр сопроводить алгоритмом шифрования и расшифрования текста.

Литература

1. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В.. Основы криптографии / М.: Гелиос АРВ.
2. Бабаш А.В., Шанкин Г. П. История криптографии / М.: Гелиос АРВ, ч.1, 2002г., 240 с.
3. Жельников В. Криптография от папируса до компьютера / М.: ABF, 1996, 336с.
4. Нечаев В.И. Элементы криптографии (основы теории защиты информации) / М.: Высшая школа, 1999, 109 с.

Раздел 2. Теоретико-численные методы в криптографии

Задание на самостоятельную работу

Изучить алгоритмы, которые широко применяются в криптографии.

Элементы теории чисел:

- расширенный алгоритм Евклида;
- решение уравнения сравнения

$$ax=b \bmod n;$$

- вычисление символа Лежандра;
- вычисление символа Якоби;

- арифметические операции в модулярной арифметике;
- вычисление квадратных корней по простому модулю;
- вычисление квадратных корней по составному множителю.

Тестирование чисел на простоту и построение больших простых чисел:

- решето Эратосфена;
- тест на основе малой теоремы Ферма;
- тест Соловея – Штрассена;
- тест Рабина – Миллера;
- полиномиальный тест распознавания простоты.

Алгоритмы факторизации целых чисел:

- метод Полларда;
- факторизация Ферма;
- метод квадратичного решета;
- (p-1)-метод факторизации Полларда.

Литература

1. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии / М.: Гелиос АРВ.
2. Зубов А. Ю. Совершенные шифры / М.: Гелиос АРВ, 2003, 160 с.
3. Мао Венбо. Современная криптография / М.: С-П., Киев, изд. Дом Вильямс.
4. Смарт Н. Криптография / М.: Техносфера.
5. Фомичев В.М. Дискретная математика и криптология / М.: Диалог-МИФИ, 2003, 400 с.

Раздел 3. Криптографические алгоритмы с симметричными ключами

Задание на самостоятельную работу

Изучить и подготовить реферат по алгоритму *RIJNDEAL*. В реферат включить минимальный теоретический материал по конечным полям над многочленами. Особо выделить те моменты теории, которые используются в алгоритме *RIJNDEAL*. Включить демонстрационные примеры, на которых поясняются операции в алгоритме. Разработать структуру данных для реализации алгоритма шифрования *AES*, описать структуру данных. Для структуры данных разработать алгоритм реализации, описать разработанный алгоритм по шагам. Разработать блок схему алгоритма. Оформить доклад (презентацию) по алгоритму *AES* с набором слайдов для пояснения основных шагов алгоритма.

Изучить и подготовить реферат по алгоритму *IDEA*. В реферат включить демонстрационные примеры, на которых поясняются операции в алгоритме. Разработать структуру данных для реализации алгоритма шифрования *IDEA*, описать структуру данных. Для структуры данных разработать алгоритм реализации, описать разработанный алгоритм по шагам. Создать блок схему алгоритма. Оформить доклад (презентацию) по алгоритму *IDEA* с набором слайдов для пояснения основных шагов.

Изучить и подготовить реферат по алгоритму ГОСТ. В реферат включить демонстрационные примеры, на которых поясняются операции в алгоритме. Разработать структуру данных для реализации алгоритма шифрования ГОСТ, описать структуру данных. Для структуры данных разработать алгоритм реализации, описать разработанный алгоритм по шагам. Создать блок схему алгоритма. Оформить доклад (презентацию) по алгоритму ГОСТ с набором слайдов для пояснения основных шагов алгоритма.

В качестве задание на самостоятельную работу студентам важно выдавать один из четырех режимов ГОСТ.

Литература

1. Зензин О.С., Иванов М.А. Стандарт криптографической защиты AES. Конечные поля / М.: Кудиц-Образ, 2002, 176 с.
2. Мао Венбо. Современная криптография / М.: С-П., Киев, изд. Дом Вильямс.
3. Смарт Н. Криптография / М.: Техносфера.
4. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / М.: Радио и связь, 1999, 328 с.
5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке **Си** / М.: Триумф, 2003, 816 с.

Раздел 4. Криптографические алгоритмы с несимметричными ключами

Задание на самостоятельную работу

Выбрать алгоритмы с открытыми ключами, которые не используются в лабораторных работах, например, криптографическая система для задачи о рюкзаке, и реализовать их.

Ниже приведен список основных криптографических схем с открытыми ключами:

- *RSA*;
- схема Рабина;
- схема Шнорра;
- схема Эдь-Гамаля;

• схема на основе задачи о рюкзаке;
• российские стандарты;
• схема Фиата-Шамира.

Реализацию любой задачи можно разбить на отдельные этапы. Например, задачу о рюкзаке можно разбить на такие отдельные задачи:

• генерация быстрорастущего вектора A;
• выбор модуля m;
• определение множителя t для вычисления маскирующего вектора B;
• вычисление обратного значения (t-1) для значения маскирующего множителя t.
• вычисления маскирующего вектора B;
• формирование битовых последовательностей из открытого текста, размер которых совпадает с размером векторов A и B;
• реализация алгоритма шифрования на базе задачи о рюкзаке;
• реализация алгоритма расшифрования на базе задачи о рюкзаке.

При формировании задачи для самостоятельной работы любой сложный алгоритм можно разбить на отдельные этапы и каждый этап давать для реализации разным группам студентов. Например, рассмотрим криптосистему *RSA*.

Формирование системы RSA

1. Выбираем два различных простых числа p и q.
2. Вычисляем $n = pq$ и $\varphi(n)=(p-1)(q-1)$.
3. Выбираем число e, взаимнопростое с $\varphi(n)$.
4. Вычисляем число d из уравнения

$$de \equiv 1 \ mod \ \varphi(n).$$

5. Определяются открытые ключи e и n.
6. Определяются закрытые ключи d, p, q и $\varphi(n)$.

Алгоритм шифрования

1. Дан текст сообщения M.
2. Шифротекст C вычисляется по формуле:

$$C = E_k(M) = M^e \ mod \ n.$$

Алгоритм дешифрования

1. Дан шифротекст C.
2. Текст сообщения M вычисляется по формуле

$$M = D^k(C) = C^d \ mod \ n =$$
$$= (M^e)^d \ mod \ n = M.$$

Четыре шага формирование системы *RSA*, два шага алгоритма шифрования и два шага расшифрования можно рассмотреть как восемь отдельных задач и распределить эти задачи по студентам. Точно так же можно поступать, рассматривая любую криптографическую систему с открытыми ключами.

Литература

1. Мао Венбо. Современная криптография / М.: С-П., Киев, изд. Дом Вильямс.
2. Смарт Н. Криптография / М.: Техносфера.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке **Си** / М.: Триумф, 2003, 816 с.
4. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / М.: Мир, 2006, 471 с.
5. Саломаа А. Криптография с открытым ключом / М.: Мир, 1996, 318 с.

Раздел 5. Криптографические хеш-функции

Задание на самостоятельную работу

Выбрать алгоритм вычисления хеш-функции, которые не используются в лабораторных работах, и сделать программную реализацию этой хеш-функции.

Список основных хеш-функций:

- *MD4*;
- *MD5*;
- *SHA*;

• *RIPEMD*-160;
• ГОСТ.

При реализации алгоритма вычисления хеш-функции этот алгоритм можно разбить на отдельные самостоятельные независимые задачи и эти этапы распределять между студентами или группами студентов, которые сформировал преподаватель для выполнения задания. В пособии все алгоритмы представлены таким образом, что представить их в виде отдельных заданий несложно.

Литература

1. Мао Венбо. Современная криптография / М.: С-П., Киев, изд. Дом Вильямс.
2. Смарт Н. Криптография / М.: Техносфера.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке **Си** / М.: Триумф, 2003, 816 с.
4. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / М.: Мир, 2006, 471 с.
5. Саломаа А. Криптография с открытым ключом / М.: Мир, 1996, 318 с.

Раздел 6. Псевдослучайные последовательности (ППС)

Для генерации псевдослучайных последовательностей можно использовать следующие подходы:

• поточные шифры;
• блочные шифры;
• односторонние функции;
• регистры сдвигов с обратной связью;
• конгруэнтные генераторы.

Задание на самостоятельную работу

Для самостоятельной работы можно предложить реализацию генераторов псевдослучайных последовательностей из следующего списка:

• генераторы на основе конгруэнтных генераторов, например, генератор на основе формулы

$$x_{n+1} = (ax_n + b) \bmod m;$$

• генератор *BBS* (Блюм-Блюм-Шуба) на базе односторонней функции;
• генератор на базе алгоритма *RSA*;
• генератор на базе блочного шифра (любого);

• стандарт генератора *ANSI X*9.17 (на базе алгоритма «тройного» *DES*).
• генератор на базе поточного шифра (любого).

Литература

1. Иванов М.А., Чугунков И.В. Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М.: КУДИЦ-ОБРАЗ, 2003, 204с.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях / М., КУДИЦ-ОБРАЗ, 2001, 368с.
3. Столингс Вильям. Криптография и защита сетей. Принципы и практика / М.: изд. дом Вильямс, 2001, 672 с.

Раздел 7. Электронная цифровая подпись (ЭЦП).

Для электронной цифровой подписи можно использовать следующие схемы с открытыми ключами:

• *RSA*;
• схема Рабина;
• схема Шнорра;
• схема Эдь-Гамаля;
• Российские стандарты;
• схема Фиата-Шамира.

Задание на самостоятельную работу

Для самостоятельной работы можно предложить реализацию схем электронной цифровой подписи из следующего списка:

• Российские стандарты;
• Американский стандарт *DSA*;
• схемы цифровых подписей, которые используют трудную задачу вычисления дискретных логарифмов (схемы Эль-Гамаля, Шнорра);
• схема Рабина.

Литература

1. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы Криптографии / М.: Гелиос АРВ.
2. Столингс Вильям. Криптография и защита сетей. Принципы и практика / М.: изд. дом Вильямс, 2001, 672 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке **Си** / М.: Триумф, 2003, 816 с.

Раздел 8. Криптографические протоколы.

Обычно криптография в протоколе используется для выполнения криптографических функций, т.е. для обеспечения безопасности задач, которые решаются при использовании протокола.

Криптографические протоколы применяются:

- в электронных платежах;
- в электронном обмене данных;
- в электронной коммерции;
- в электронном голосовании;
- в играх по телефону или по компьютерным сетям.

Используя учебники, научные журналы, пособия и Интернет, составить по возможности максимальный каталог схем криптографических протоколов.

В пособии представлены следующие схемы протоколов:

- схема аутентификации Шнорра;
- протокол подбрасывания монеты;
- протоколы распределения ключей (ПРК):
- протоколы передачи сгенерированных ключей;
- протоколы совместной выработки общего ключа;
- протоколы предварительного распределения ключей.

Задание на самостоятельную работу

Для самостоятельной работы можно предложить реализовать одну из схем перечисленных протоколов.

Литература

1. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости./ М., 2007, 254 с.
2. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В.. Основы криптографии / М.: Гелиос АРВ.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке **Си** / М.: Триумф, 2003, 816 с.
4. Мао Венбо. Современная криптография / М., С-П., Киев, изд. Дом Вильямс.

5. Столингс Вильям. Криптография и защита сетей. Принципы и практика / М.: изд. дом Вильямс, 2001, 672 с.
6. Чмора А.Л. Современная прикладная криптография / М.: Гелиос АРВ, 2001, 256 с.

Раздел 9. Криптографические стандарты шифров

Задание на самостоятельную работу

На базе научных журналов, монографий, литературы по криптографии, Интернета составить обзор (реферат) по теме:

«Надежность, стойкость и имитостойкость шифров»

В обзоре проанализировать вопрос о том, какие математические курсы используются при изучении данной темы. Кратко сформулировать основные результаты, которые получены по этой теме и для каких классов шифров. Сгруппировать по возможности советы, позволяющие усилить качество шифров и одновременно избежать ошибок при шифровании.

Особое внимание обратить на вопрос о том, существуют ли методы и алгоритмы, при помощи которых можно исследовать хотя бы простейшие шифры на надежность и стойкость. Если такой алгоритм будет обнаружен, то его следует включить в обзор с подробным описанием данного алгоритма.

Литература

1. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии / М.: Гелиос АРВ.
2. Зубов А.Ю. Совершенные шифры / М.: Гелиос АРВ, 2003, 160 с.
3. Мао Венбо. Современная криптография / М.: С-П., Киев, изд. Дом Вильямс.
4. Смарт Н. Криптография / М.: Техносфера.
5. Фомичев В.М. Дискретная математика и криптология / М.: Диалог-МИФИ, 2003, 400 с.

Раздел 10. Эллиптическая криптография

Задание на самостоятельную работу

Подготовить отчет (реферат) по теме

«Эллиптическая кривая над конечным полем»

Можно использовать материал из приложения, дополнительную литературу и Интернет. В подготовленном отчете включить теоретический материал и демонстрационные примеры по разбираемой теме. В качестве источника можно использовать монографию [4], реферат которой дан в приложении.

Литература

1. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Алгебраические и алгоритмические основы / М.: КомКнига, 2006, 328 с.
2. Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых / М.: КомКнига, 2006, 320 с.
3. Мао Венбо. Современная криптография./ М., С-П., Киев, изд. Дом Вильямс.
4. Смарт Н. Криптография / М.: Техносфера.
5. Тилборг ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник / М.: Мир, 2006, стр. 2006, 471 с.

Список самостоятельных работ

Самостоятельная работа (54 часа)

Самостоятельная работа состоит из изучения теоретического материала и выполнения заданий с помощью компьютера. Теоретический материал, вынесенный на самостоятельное изучение, сформулирован в виде вопросов к темам, которые выносятся на зачет. Задания находятся в методических указаниях к дисциплине, выдаются преподавателем на лабораторных занятиях, контроль их выполнения осуществляется в виде дополнительных вопросов при защите работ по одноименной теме.

Теоретическое изучение

Теоретико-численные методы в криптографии. Изучить следующие алгоритмы, которые широко применяются в криптографии:

Элементы теории чисел:

- расширенный алгоритм Евклида;
- решение уравнения сравнения

$$ax=b \bmod n;$$

- вычисление символа Лежандра;
- вычисление символа Якоби;
- арифметические операции в модулярной арифметике;
- вычисление квадратных корней по простому модулю;
- вычисление квадратных корней по составному множителю.

Тестирование чисел на простоту и построение больших простых чисел:

- решето Эратосфена;
- тест на основе малой теоремы Ферма;
- тест Соловея – Штрассена:
- тест Рабина – Миллера.
- полиномиальный тест распознавания простоты.

Алгоритмы факторизации целых чисел:

- метод Полларда;
- факторизация Ферма;
- метод квадратичного решета;
- (p-1)-метод факторизации Полларда.

Самостоятельная работа (36 часов)

Создать информационную систему для демонстрации основных классов шифров классической криптографии. Шифровать все символы клавиатуры компьютера.

Шифры замены:

- шифр Цезаря;
- квадрат Полибия;
- аффинная криптосистема.

Многоалфавитные криптосистемы:

- таблица Тритемия;
- квадрат Виженера;
- квадрат Бьюфорта;
- шифр Гронсфельда.

Блочные шифры замены:

- шифр Плейфера;
- двойной квадрат.

Шифры перестановки:

- криптосистема по заданной перестановке k чисел;
- шифры маршрутной перестановки по столбцам таблицы, столбцы пронумерованы по порядку;
- шифры маршрутной перестановки по столбцам таблицы, столбцы пронумерованы в произвольном порядке;
- шифры маршрутной перестановки по столбцам и строкам таблицы, строки и столбцы таблицы пронумерованы по порядку;
- шифры маршрутной перестановки по столбцам и строкам таблицы, строки и столбцы таблицы пронумерованы в произвольном порядке, некоторые поля таблицы исключаются для записи символов.

Криптографические машины:

- колесо Джефферсона.

Шифры гаммирования:

- Шифр Вернама.

Реализация численных алгоритмов:

- расширенный алгоритм Евклида;
- решение уравнения сравнения

$$ax=b \bmod n;$$

- вычисление символа Лежандра;
- вычисление символа Якоби;
- арифметические операции в модулярной арифметике;
- вычисление квадратных корней по простому модулю;
- вычисление квадратных корней по составному множителю.

Тестирование чисел на простоту и построение больших простых чисел:

- решето Эратосфена;
- тест на основе малой теоремы Ферма;
- тест Соловея – Штрассена;
- тест Рабина – Миллера;
- полиномиальный тест распознавания простоты.

Алгоритмы факторизации целых чисел:

- метод Полларда;
- факторизация Ферма;
- метод квадратичного решета;
- (p - 1)-метод факторизации Полларда.

Реализация алгоритма хеш-функции ГОСТ.

Реализация американского стандарта ЭЦП DSS.

Реализация конгруэнтных генераторов псевдослучайных последовательностей.

Реализация простейших криптографических протоколов.

Дополнительный теоретический материал к самостоятельным работам Государственный стандарт Российской Федерации

Введение

Возрастающая роль применения информационных технологий при создании, обработке, передаче и хранении документов требует в определенных случаях сохранения конфиденциальности их содержания, обеспечения полноты и достоверности.

Одним из эффективных направлений защиты информации является криптография (криптографическая защита). Она широко применяется в различных сферах деятельности государственных и коммерческих структур.

Криптографические методы защиты информации являются объектом серьезных научных исследований и стандартизации на национальных, региональных и международных уровнях.

Настоящий стандарт определяет процедуры выработки и проверки электронной цифровой подписи на базе асимметрического криптографического алгоритма с применением функции хеширования.

Электронная цифровая подпись обеспечивает целостность сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения, с гарантированной идентификацией ее автора (лица, подписавшего документ).

Область применения

Настоящий стандарт устанавливает процедуры выработки и проверки электронной цифровой подписи (ЭЦП) сообщений (документов), передаваемых по незащищенным телекоммуникационным каналам общего пользования в системах обработки информации различного назначения на базе асимметричного криптографического алгоритма с применением функции хеширования.

Внедрение системы ЭЦП на базе настоящего стандарта обеспечивает защиту передаваемых сообщений от подделки, искажения и однозначно позволяет доказательно подтвердить подпись лица, подписавшего сообщение.

Обозначения

В настоящем стандарте используются следующие обозначения:

- β^* – множество всех конечных слов в алфавите $\beta=\{0,1\}$.
- $|A|$ – длина слова $A\in\beta^*$.
- $V_k(2)$ – множество всех бинарных слов длины k.
- $z \mod n$ – наименование по значению неотрицательного числа, сравнимого с числом z по модулю числа n.
- $\langle N\rangle_k$ – слово длины k, содержащее двоичную запись вычета

$$N \mod 2^k$$

неотрицательного целого числа N.

- A – неотрицательное целое число, имеющее двоичную запись, $A\in\beta^*$. Под длиной числа будем понимать номер старшего значащего бита в двоичной записи числа.
- $A||B$ – конкатенация слов A, $B\in\beta^*$ – слово длины $|A|+|B|$, в котором левые $|A|$ символов образуют слово A, а правые $|B|$ символов образуют слово B. Можно также использовать обозначение $A||B=AB$.
- A^k – конкатенация k экземпляров слова A, $A\in\beta^*$.

- M – передаваемое сообщение, $M \in \beta^*$.
- M_1 – полученное сообщение, $M_1 \in \beta^*$. Отправляемые и получаемые последовательности, в том числе сообщения и подписи, могут отличаться друг от друга из-за случайных или преднамеренных искажений.
- h – хеш-функция, отображающая сообщение M в слово $h(M) \in V_{256}(2)$.
- p – простое число, где $2^{509} < p < 2^{512}$ либо $2^{1020} < p < 2^{1024}$.
- q – простое число, $2^{254} < q < 2^{256}$ и q являвется делителем для $(p\text{-}1)$.
- a – целое число, $1 < a < p\text{-}1$, при этом

$$a^q \bmod p = 1.$$

- k – целое число, $0 < k < q$.
- $\lceil d \rceil$ – наименьшее целое число, которое не больше d.
- $\lfloor d \rfloor$ – наименьшее целое число, которое не меньше d.
- $e := g$ – присвоение параметру e значения g.
- x – секретный ключ пользователя для формирования подписи, $0 < x < q$.
- y – открытый ключ пользователя для проверки подписи

$$y = a^x \bmod p.$$

Общие положения

- Система электронной цифровой подписи базируется на методах криптографической защиты данных с использованием хеш-функции.
- Алгоритмы вычисления функции хеширования установлен в ГОСТ Р 34.11.
- Процедуры цифровой подписи допускают как программную, так и аппаратную реализацию.
- Система электронной цифровой подписи включает в себя процедуры выработки и проверки подписи под данным сообщением.
- Цифровая подпись, состоящая из двух целых чисел, представленных в виде слов в алфавите β, вычисляется с помощью определенного набора правил, изложенных в тексте стандарта.

Откуда взялся текст ниже, он никак не связан ни с чем? Что за пункт 7?
Числа p, q и a являющиеся параметрами системы, должны быть выбраны (выработаны) по процедуре, описанной в пункте 7. Числа p, q и a не являются секретными. Конкретный набор их значений может быть общим для группы пользователей. Целое число k, которое генерируется в процедуре подписи сообщения, должно быть секретным и должно быть уничтожено сразу после выработки подписи. Число k снимается с физического датчика случайных чисел или вырабатывается псевдослучайным методом с использованием секретных параметров.

Процедура выработки подписи

Текст сообщения, представленный в виде двоичной последовательности символов, подвергается обработке по определенному алгоритму, в результате которого формируется электронная цифровая подпись для данного сообщения. Процедура подписи сообщения включает в себя следующие этапы:

1. Вычислить $h(M)$ – значение хеш-функции h от сообщения M. Если

$$h(M) \bmod q = 0,$$

присвоить $h(M)$ значение $0^{255}\quad 1$.

2. Выработать целое число k, $0< k < q$.

3. Вычислить два значения

$$r=a^k \bmod p \quad \text{и} \quad r' = r \bmod q.$$

Если $r' =0$, то перейти к этапу 2 и выработать другое значение числа k.

4. С использованием секретного ключа x пользователя (отправителя сообщения) вычислить значение

$$S = (xr' + kh(M)) \bmod q.$$

Если $s = 0$, то перейти к этапу 2, в противном случае закончить работу алгоритма.

5. Подписью сообщения M является вектор

$$< r' >_{256} \;||\; < s >_{256}.$$

Отправитель направляет адресанту цифровую последовательность символов, состоящую из двоичного представления текста сообщения и присоединенной к нему электронной цифровой подписи.

Процедура проверки подписи

Получатель должен проверить подлинность сообщения и подлинность электронной цифровой подписи, осуществляя ряд операций (вычислений). Это возможно при наличии у получателя открытого ключа отправителя, пославшего сообщение. Процедура проверки включает в себя следующие этапы:

1. Проверить условие

$$0< s < q \quad \text{и} \quad 0 < r' < q.$$

Если хотя бы одно из этих условий не выполнено, то подпись считается недействительной.

2. Вычислять $h(M_1)$ – значение хеш-функции h от полученного сообщения M_1. Если

$$h(M_1) \bmod q=0,$$

присвоить $h(M_1)$ значение 0^{255} 1.

3. Вычислить значение

$$v= (h(M_1))^{q-2} \bmod q.$$

4. Вычислить значения

$$z_1 = sv \bmod q,$$
$$z_2 = (q-r') v \bmod q.$$

5. Вычислить значение (чему равны s1 и s2?)

$$u = (a^{s1}\times y^{s2} \bmod p) \bmod q.$$

6. Проверить условие

$$r' = u.$$

При совпадении значений r и u получатель принимает решение о том, что полученное сообщение подписано данным отправителем и в процессе пере-

дачи не нарушена целостность сообщения, т.е. $M_1=M$. В противном случае подпись считается недействительной.

Процедуры получения чисел p, q и a

Получение простых чисел осуществляется с использованием линейного конгруэнтного датчика по модулю 2^{16} или по модулю 2^{32}

$$x_n = bx_{n-1} + c.$$

Пользователь должен задать начальное состояние x_0 и параметр датчика c. Заданные величины необходимо зафиксировать (запомнить) для возможности проведения проверки того, что простые числа получены по установленной процедуре. Ниже изложены процедуры получения параметров p, q и a.

Процедура А

Все замечания к процедуре А относятся ко всем процедурам!

Процедура позволяет получать простые числа p длиной t, $t \geq 17$ битов с простым делителем q длиной $\lfloor t/2 \rfloor$ битов числа $(p-1)$. Получение чисел осуществляется с использованием линейного конгруэнтного датчика

$$x_n = (19381\, x_{n-1} + c) \bmod 2^{16}.$$

Задаются число x_0 при условии $0 < x_0 < 2^{16}$ и нечетное число c при условии $0 < c < 2^{16}$. Процедура вычисления чисел включает в себя следующие шаги:

1. Определить $Y_0 := X_0$.
2. Вычислить последовательность чисел $t_0, t_1, \ldots, t_5$ по правилу:

$$t_0 := t_i,$$
$$\text{если } t_i \geq 17, \text{ то } t_{i+1} = \lfloor t_i / 2 \rfloor,$$
$$\text{если } t_i < 17, \text{ то } s := 1.$$

3. Найти наименьшее простое число p длиной *t (если это правильно, то где индекс у t?)* битов.

4. Вычислить $m := s - 1$.

5. Вычислить $r_m = \lceil t_m / 16 \rceil$.

6. Вычислить последовательность $y_1, ..., y_{rm}$ по рекурсивному правилу

$$y_{i+1} = (19381 y_i + c) \bmod 2^{16}.$$

7. Вычислить $y_m = \Sigma \; y_1 \; 2^{161}$(сомнительная формула! Что суммируется и по какому индексу?)

8. Положить $y_0 := y_{rm}$.

9. Вычислить (r и t то с индексами, то нет! Херня какая-то!)

$$N = \lceil 2^{t-1} / p_{m+1} \rceil + \lfloor (2^{t-1} y_m) / (p_{m+1} 2^{16r}) \rfloor.$$

Если N нечетно , то положить $N := N+1$.

10. Определить $k := 0$.

11. Вычислить

$$p_m = p_{m+1} (N+k) + 1.$$

12. Если $p_m > 2^t$, то перейти к шагу 6.

13. Проверить условия

$$2^{p(N+k)} \bmod p_m = 1,$$
$$2^{(N+k)} \bmod p_m \neq 1.$$

Если хотя бы одно из условий не выполнено, то положить $k := k + 2$ и перейти к шагу 11. Если оба условия выполнены, то вычислить $m := m-1$.

14. Если $m \geq 0$, то перейти к шагу 5. Если $m < 0$, то p_0 – искомое простое число p и p_1 – искомое простое число q.

Процедура А´

Процедура позволяет получать простые числа p длиной t, $t \geq 33$ битов с простым делителем q длиной $\lfloor t/2 \rfloor$ битов числа (p-1). Получение чисел осуществляется с использованием линейного конгруэнтного датчика

$$x_n = (97781173\, x_{n-1} + \text{c}) \; mod \; 2^{32}.$$

Для работы алгоритма задаются число x_0 при условии $0 < x_0 < 2^{32}$ и нечетное число c при условии $0 < c < 2^{32}$. Процедура вычисления включает в себя следующие шаги.

1. Положить $y_0 := x_0$

2. Вычислить последовательность чисел t_0, t_1, ..., t_s по правилу:

$$t_0 := t,$$
$$\text{если } t_i \geq 33, \text{ то } t_{i+1} = \lfloor t_i / 2 \rfloor,$$
$$\text{если } t_i < 33, \text{ то } s := 1.$$

3. Найти наименьшее простое число p_s длины t_s битов.

4. Вычислить $m := s$-1.

5. Вычислить $r_m = \lceil t_m / 32 \rceil$.

6. Вычислить последовательность y_1, ..., y_{rm} по рекурсивному правилу

$$y_{i+1} = (97781173\, y_i + \text{c}) \; mod \; 2^{32}.$$

7. Вычислить $y_m = \Sigma\, y_1\, 2^{321}$.

8. Положить $y_0 := y_r$.

9. Вычислить

$$N = \lceil 2^{t-1} / p_{m+1} \rceil + \lfloor (2^{t-1} y_m) / (p_{m+1} 2^{32r}) \rfloor.$$

Если N нечетно, то $N := N + 1$

10. Определить $k := 0$

11. Вычислить

$$p_m = p_{m+1}(N + k) + 1.$$

12. Если $p_m > 2^t$, то перейти к шагу 6

13. Проверить условия

$$2^{p\,(N+k)} \bmod p_m = 1,$$
$$2^{(N+k)} \bmod p_m \neq 1.$$

Если хотя бы одно из условий не выполнено, то положить $k := k+2$ и перейти к шагу 11. Если оба условия выполнены, то вычислить $m := m\text{-}1$.

14. Если $m \geq 0$, то перейти к шагу 5. Если $m < 0$, то p_0 – искомое простое число p и p_1 – искомое простое число q.

Процедура В

Данная процедура позволяет получать простые числа p длины t_p, t_p=1021 ÷ 1024 битов с делителем q длины t_q, t_q = 255 ÷ 256 битов числа (p-1). Для работы процедуры задаются число x_0 при условии $0 < x_0 < 2^{16}$ и нечетное число c при условии $0 < c < 2^{16}$. Процедура вычисления включает в себя следующие шаги.

1. С помощью процедуры A получить простое число q длины t_q битов.

2. С помощью процедуры A получить простое число Q длины 512 битов, при этом пункт 1 процедуры A не выполнять, а сохранить значение y_0, полученное в конце работы шага 1.

3. Вычислить последовательность $y_1, ..., y_{64}$ по рекурсивному правилу

$$y_{i+1} = (19381\, y_i + \text{c}) \; mod \; 2^{16}.$$

4. Вычислить $\text{y} = \Sigma\, \text{y}_1 2^{161}$.

5. Определить $y_0 := y_{64}$.

6. Вычислить

$$N = \lceil 2^{t-1} / (qQ) \rceil + \lfloor (2^{t-1} y) / (\, qQ \cdot 2^{1024}) \rfloor .$$

Если N нечетно, то $N := N + 1$.

7. Задать $k := 0$.

8. Вычислить $p = qQ(N + k) + 1$.

9. Если $p > 2^t$, то перейти к шагу 3.

10. Проверить условия

$$2^{qQ(N+k)} \; mod \; p = 1,$$
$$2^{q(N+k)} \; mod \; p \neq 1.$$

Если оба условия выполнены, то p и q – искомые простые числа. Если хотя бы одно не выполнено, то положить $k := k + 2$ и перейти к шагу 8. Последовательность шагов повторять до выполнения условий на шаге 10.

Процедура В´

Данная процедура позволяет получать простые числа p длиной t_p, t_p=1021÷ 1024 битов с делителем q длиной t_q, t_q = 255 ÷ 256 битов числа (p-1). Для работы процедуры задаются число x_0 при условии $0 < x_0 < 2^{32}$ и нечетное число c при условии $0 < c < 2^{32}$. Процедура вычисления включает в себя следующие шаги.

1. По процедуре A' получить простое число q длины t_q битов.

2. По процедуре A' получить простое число Q длины 512 битов, при этом пункт 1 процедуры A' не выполнять, а сохранить значение y_0, полученное в конце работы шага 1.

3. Вычислить последовательность y_1, ..., y_{32} по рекурсивному правилу

$$y_{i+1}= (97781173\, y_i + c)\ mod\ 2^{32}.$$

4. Вычислить y= Σ y_1 2^{321}

5. Определить $y_0 := y_{32}$.

6. Вычислить

$$N = \lceil 2^{t-1}/(qQ) \rceil + \lfloor (2^{t-1}\, y) / (\, qQ \cdot 2^{1024}) \rfloor.$$

Если N нечетно, то $N := N + 1$.

7. Задать $k := 0$.

8. Вычислить

$$p = qQ(N+k) + 1.$$

9. Если $p > 2^t$, то перейти к шагу 3.

10. Проверить условия

$$2^{qQ(N+k)}\ mod\ p = 1,$$
$$2^{q(N+k)}\ mod\ p \neq 1.$$

Если оба условия выполнены, то p и q – искомые простые числа. Если хотя бы одно из условий не выполнено, то положить $k := k + 2$ и перейти к шагу 8. Последовательность шагов повторить до выполнения условий на шаге 10.

Процедура С

Процедура позволяет получить число a при заданных p и q. Соответствующий алгоритм формулируется следующим образом.

1. Произвольно выбрать число d, $1 < d < p$-1.

2. Вычислить

$$f = d^{(p-1/q)} \bmod p.$$

3. Если $f = 1$, то перейти к шагу 1. Если $f \neq 1$, то положить a равным f. Конец работы алгоритма.

Проверочные примеры для вышеизложенных процедур получение чисел p, q и a, выработка и проверка подписи приведены в приложении А.

Приложение А (справочное)

Проверочные примеры

Значения параметров x_0, c, d, x, y и k, указанные в приложении, рекомендуется использовать только в проверочных примерах для настоящего стандарта.

А.1. Представление чисел и векторов

Длины чисел и векторов, а также элементы последовательности t записывают в десятичной системе счисления. Последовательности двоичных символов записывают как строки шестнадцатеричных цифр, в которых каждая цифра соответствует четырем знакам ее двоичного представления.

А.2 Примеры к процедурам получения чисел *p*, *q* и числа *a* для реализации ЭЦП

А.2.1.

Процедура А.

Необходимо получить простое число p длины 512 битов с простым делителем q длины 256 битов числа (p-1).

Задают числа x_0 = 5EC9 и c = 7341.

Вычисляют последовательность t = (512, 256, 128, 64, 32, 16).

ГОСТ Р 34.10-94

Тогда в процессе выполнения процедуры будет получена последовательность простых чисел:

$t_5 = 16, p_5 =$	8003
$t_4 = 32, p_4 =$	AD4BOFAB
$t_3 = 64, p_3 =$	B25D28A7 1A62D775
$t_2 = 128, p_2 =$	9C992766 8E6E4908 964A9AE1 3773AE75
$t_1 = 256, p_1 =$	98915E7E C8265EDF CDA31E88 F24809DD
	B064BDC7 285DD50D 7289FOAC 6F49DD2D
$t_0 = 512, p_0 =$	EE8172AE 8996608F B69359B8 9EB82A69

854510E2 977A4D63 BC97322C E5DC3386
EA0A12B3 43E9190F 23177539 84583978
6BB0C345 D165976E F2195EC9 B1C379E3

Здесь p_1 и p_0 – искомые числа q и p соответсвенно.

Процедура A´.

Необходимо получить простое число p длины 512 битов с простым делителем q длины 256 битов числа (p-1).

Задаются числа x_0 = 3DFC46F1 и c =D.
Вычисляют последовательность t = (512, 256, 128, 64, 32).
Тогда в процессе выполнения процедуры будет получена последовательность простых чисел:

$t_4 = 32$, p_4 = 8000000B
$t_3 = 64$, p_3 = 9AAA6EBE 4AA58337
$t_2 = 128$, p_2 = C67CE4AF 720F7BBA B5FEBF37 B9E74807

В табл. 1 приведены значения p_1 и p_0, которые совпадают с искомыми числами q и p, соответсвенно.

Таблица 1

Значения параметров p_1 и p_0

$t_1 = 256$, p_1 =	931A58FB	6F0DCDF2	FE7549BC	3F19F472
	4B56898F	7F921A07	6601EDB1	8C93DC75
$t_0 = 512$, p_0 =	8B08EB13	5AF966AA	B39DF294	538580C7
	DA26765D	6D38D30C	F1C06AAE	0D1228C3
	316A0E29	198460FA	D2B19DC3	81C15C88
	8C6DFD0F	C2C565AB	B0BF1FAF	F9518F85

Процедура B.

Необходимо получить простое число p длиной 1024 битов с простым делителем q длины 256 битов числа (p-1).

Задают начальные значения x_0 = A565 и c = 538B.

С помощью процедуры *A* получают простое число *q* длиной 256 битов. Значения числа *q* приведены в табл. 2.

Таблица 2

Значения параметра *q*

BCC02CA0	CE4F0753	EC16105E	E5D530AA
00D39F31	71842AB2	C334A26B	5F576E0F

Затем вновь с помощью процедуры *A* получают простое число *Q* длиной 512 битов. Значения числа *Q* приведены в табл. 3.

Таблица 3

Значения параметра *Q*

CCEF6F73	87B6417E	C67532A1	86EC619C
A4DB132F	CA02621A	DE216F1D	F6F8114C
DB3D9209	7D978C6F	583C3301	4174AA1C
1AFCCEB2	843B1D35	0D2E5D16	855A7477

Наконец, получают простое число *p* длиной 1024 битов (см. табл. 4).

Таблица 4

Значения параметра *p*

AB8F3793	8356529E	871514C1	F48C5CBC
E77B2F4F	C9A2673A	C2C1653D	A8984090
C0AC7377	5159A26B	EF59909D	4C984663
1270E166	53A62346	68F2A52A	01A39B92
1490E694	C0F104B5	8D2E1497	0FCCB478
F98D01E9	75A1028B	9536D912	DE5236D2
DD2FC396	B7715359	4D417878	0E5F16F7
18471E21	11C8CE64	A7D7E196	FA57142D

Процедура B´.

Необходимо получить простое число p длины 1024 битов с простым делителем q длины 256 битов числа (p-1).

Задают начальные значение x_0 = 3DFC46F1 и $c = D$.
С помощью процедуры A получают простое число q длиной 256 битов. Значения числа q приведены в табл. 5.

Таблица 5

Значения параметра q

931A58FB	6F0DCDF2	FE7549BC	3F19F472
4B56898F	7F921A07	6601EDB1	8C93DC75

Затем вновь с помощью процедуры A получают простое число Q длиной 512 битов. Значения числа Q приведены в табл. 6.

Таблица 6

Значения параметра Q

BB124D6C	255D373F	FA7D5DF5	5CE0DB44
96397506	6F8980B1	C7CB68DF	6C6E8D27
12D34BF3	3B536899	C7150C4D	F82FC171
D9529BC8	C9653929	D6682CF5	FBBA1B3D

Наконец, получают простое число p длиной 1024 битов.

Таблица 7

Значения параметра p

E2C4191C	4B5F222F	9AC27325	62F6D9B4
F18E7FB6	7A290EA1	E03D750F	0B980675
5FC730D9	75BF3FAA	606D05C2	18B35A6C
3706919A	AB92E0C5	8B1DE453	1C8FA8E7
AF43C2BF	F016251E	21B28708	97F6A27A
C4450BCA	235A5B74	8AD386E4	A0E4DFCB
09152435	ABCFE48B	D0B126A8	122C7382
F285A986	4615C66D	ECDDF6AF	D355DFB7

Процедура С.

Пусть заданы числа p и q, полученные в А.2.1 по процедуре A.

Таблица 8

Значения параметров p и q

p =	EE8172AE	8996608F	B69359B8	9EB82A69
	854510E2	977A4D63	BC97322C	E5DC3386
	EA0A12B3	43E9190F	23177539	84583978
	6BB0C345	D165976E	F2195EC9	B1C379E3
q =	98915E7E	C8265EDF	CDA31E88	F24809DD
	B064BDC7	285DD50D	7289F0AC	6F49DD2D

Выбирают число $d = 2$. Вычисляют значения параметра f (см. табл. 9) по формуле

$$f = d^{(p-1/q)} \bmod p.$$

Таблица 9

Значения параметра f

$f = d^{(p-1/q)} \bmod p$=	9E960315	00C8774A	86958D4	AFDE2127
	AFAD2538	B4B6270A	6F7C8837	B50D50F2
	06755984	A49E5093	04D648BE	2AB5AA1
	8EBE2CD4	6AC3D849	5B142AA6	CE23E21C

Так как $f \neq 1$, то f – искомое число $a := f$.

Процедуры выработки и проверки ЭЦП на базе асимметричного криптографического алгоритма

Пусть по процедуре A с начальными условиями x_0 = 5EC9 и c = 7341 выработаны числа p, q и a (см. табл. 10).

Таблица 10

Значения параметров p, q и a

p =	EE8172AE	8996608F	B69359B8	9EB82A69
	854510E2	977A4D63	BC97322C	E5DC3386
	EA0A12B3	43E9190F	32177539	84583978
	6BB0C345	D165976E	F2195EC9	B1C379E3
q =	98915E7E	C8265EDF	CDA31E88	F24809DD
	B064BDC7	285DD50D	7289F0AC	6F49DD2D
a =	9E960315	00C8774A	86958D4	AFDE2127
	AFAD2538	B4B6270A	6F7C8837	B50D50F2
	06755984	A49E5093	04D648BE	2AB5AAB1
	8EBE2CD4	6AC3D849	5B142AA6	CE23E21C

Процедура подписи сообщения.

Пусть заданы значения x согласно табл. 11,

Таблица 11

Значения параметра x

x =	30363145	38303830	34363045	42353244
	35324234	31413237	38324331	38443046

секретный ключ и M – подписываемое сообщение. Значения хеш-функции $h(M)$ от сообщения M приведены в табл. 12.

Таблица 12

Значения хеш-функция $h(M)$

$h(M)=m=$	35344541	32454236	44313445	34373139
	43363345	37414342	34454136	31454230

Пусть целое число k задано табл. 13.

Таблица 13

Значения параметра k

$k =$	90F3A564	439242F5	186EBB22	4C8E2238
	11B7105C	64E4F539	0807E636	2DF4C72A

Тогда можно вычислить значение r , r' и s по формулам (см. табл. 14).

$$r = a^k \bmod p,$$
$$r' = r \bmod q,$$
$$s = xr' + km \bmod q.$$

Таблица 14

Значения параметров r , r' и s

$R = a^k \bmod p =$	47681C97	4373B065	3C6CA965	C8F86127
	D07A7E02	E311846E	97A8C126	3F8A76AF
	FF0AD188	02643B5C	6C998775	0C6B0458
	98E4AD8C	FC689817	76BA8216	3ADBC988
$r' = r \bmod q =$	3E5F895E	276D81D2	D52C0763	270A4581
	57B784C5	7ABDBD80	7BC44FD4	3A32AC06
	3F0DD5D4	400D47C0	8E4CE505	FF7434B6
$S = xr' + km \bmod q =$				
	DBF72959	2E37C748	56DAB851	15A60955

Цифровая подпись для сообщения M прведена в табл. 15.

Таблица 15

Цифровая подпись для сообщения M

$<r'>_{256} \,\|\|\, <s>_{256} =$	3E5F895E	276D81D2	D52C0763	270A4581
	57B784C5	7ABDBD80	7BC44FD4	3A32AC06
	3F0DD5D4	400D47C0	8E4CE505	FF7434B6
	DBF72959	2E37C748	56DAB851	15A60955

А.3.2

Процедура проверки подписи

Пусть дано сообщение M_1 (в данном случаи $M_1 = M$), его цифровая подпись в табл. 15 и открытый ключ подписавшего сообщение (см. табл. 16).

Таблица 16

Открытый ключ

$y =$	EE1902A4	0692D273	EDC1B5AD	C55F9112
	8E35F9D1	65FA9901	CAF00D27	018BA6DF
	324519C1	1A6E2725	26589CD6	E6A2EDDA
	AFF1C308	1259BE9F	CEE667A2	701F4352

З а м е ч а н и е. Данный открытый ключ y соответствует секретному ключу x, использованному в примере подписи сообщения M, то есть

$$y = a^x \bmod p.$$

Пусть сообщение M задано табл. 17.

Таблица 17

Сообщение M

$m =$	35344541	32454236	44313445	34373139
	43363345	37414342	34454136	31455430

Для значений хеш-функции h сообщения M_1 выполняются условия

$$0 < r' < q \text{ и } 0 < s < q.$$

Вычисляем значения v, z_1, z_2 и u (см. табл. 18) по формулам

$$v = m^{q-2} \bmod q,$$
$$z_1 = sv \bmod q,$$
$$z_2 = (q - r')v \bmod q,$$
$$u = (a^{s1} y^{s2} \bmod p) \bmod q.$$

Таблица 18

Значения параметров v, z_1, z_2 и u

$v=m^{q-2} \bmod q =$	72515E01	DDFA6507	E3682C01	CD285CBF
	89E462EE	E37B3865	918B6730	DEA77050
$z_1 = sv \bmod q =$	776DC3C6	4E83B73B	02B78826	6873EAFF
	B87DAED5	8686009B	5D387CCA	EAF5B744
$z_2=(q-r')v \bmod q=$	18B04C46	C1D9E875	571FDA9E	95354DDE
	3AFD0A8D	FCADB67C	505C7F03	A5185DFD
$u=$ $(a^{s1}y^{s2} \bmod p) \bmod q$	3E5F895E	276D81D2	D52C0763	270A4581
	57B784C5	7ABDBD80	7BC44FD4	3A32AC06

В результате получим значения r' и u (см. табл. 19).

Таблица 19

Значения параметров r' и u

r′=	3E5F895E	276D81D2	D52C0763	270A4581
	57B784C5	7ABDBD80	7BC44FD4	3A32AC06
u=	3E5F895E	276D81D2	D52C0763	270A4581
	57B784C5	7ABDBD80	7BC44FD4	3A32AC06

Условие $r'= u$ выполнено. Это означает, что подпись подлинная.

Эллиптические кривые

Введение

О п р е д е л е н и е. *Проективная плоскость* $\mathbf{P}^2(K)$ над полем K определяется как множество троек (X, Y, Z) не равных одновременно нулю элементов $X, Y, Z \in K$, на котором введено отношение эквивалентности

$$(X, Y, Z) \sim (XX, AY, XZ)$$

для любых $A \in K^*$.

Так, например, две точки (4, 1, 1) и (5, 3, 3) эквивалентны в $\mathbf{P}^2(\mathbf{F}_7)$. Класс эквивалентности троек называется проективной точкой.

О п р е д е л е н и е. Эллиптической кривой E называется множество точек проективной плоскости, удовлетворяющих *однородному уравнению Вейерштрасса*

$$E: \; F(X, Y, Z) = \\ -X^3 + Y^2Z + a_1XYZ - a_2X^2Z + \\ +a_3YZ^2 - a_4XZ^2 - a_6Z^3 = 0,$$

где $a_1, a_2, a_3, a_4, a_6 \in K$. Это уравнение также называют *длинной формой Вейерштрасса.* Кривая должна быть неособой в том смысле, что частные производные

$$\frac{\partial F}{\partial X}, \quad \frac{\partial F}{\partial Y}, \quad \frac{\partial F}{\partial Z}$$

не должны обращаться в нуль одновременно ни в одной ее точке.

Множество K-рациональных точек кривой E, т.е. точек из $\mathbf{P}^2(K)$, удовлетворяющих уравнению кривой, обозначается через $E(K)$. Отметим, что кривая имеет ровно одну точку, чья координата Z равна нулю, а именно (0,1,0). Ее принято называть *бесконечно удаленной точкой* или просто *точкой на бесконечности* и обозначать символом O.

Для удобства будем пользоваться аффинной версией уравнения Вейерштрасса

$$E: \; Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \qquad (1)$$

где $a_i \in K$.

K-рациональные точки в аффинном случае – это решения уравнения в пространстве K^2 и бесконечно удаленная точка O. Хотя большинство протоколов в криптографии используют эллиптическую кривую в аффинном виде, с точки зрения вычислений бывает удобно перейти к проективным координатам. Такой переход легко осуществить по следующему правилу:

– точка на бесконечности всегда переходит в бесконечно удаленную точку, как при переходе от аффинных координат к проективным, так и наоборот;
– проективная точка (X, Y, Z) кривой, отличная от бесконечно удаленной точки Z, $Z \neq 0$, переходит в аффинную точку с координатами

$$\left(\frac{X}{Z}, \frac{Y}{Z}\right);$$

– чтобы найти проективные координаты аффинной точки (X,Y), не лежащей на бесконечности, достаточно выбрать произвольное значение $Z \in K^*$ и вычислить

$$(\mathrm{X} \bullet Z, Y \bullet Z, Z).$$

Ниже убедимся, что иногда удобнее пользоваться слегка модифицированной формой проективной плоскости, когда проективные координаты (X,Y,Z) представляют аффинную точку

$$(X/Z^2, Y/Z^3).$$

Для эллиптической кривой, заданной уравнением (1), вводятся следующие константы, которые будут использованы в дальнейших формулах:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= a_1a_3 + 2a_4,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= -b_3^2 + 36b_2b_4 - 216b_6.
\end{aligned}$$

Дискриминант кривой E определяется по формуле

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

Если *char* $K \neq 2, 3$, то дискриминант можно вычислить по формуле

$$\Delta = \frac{c_4^3 - c_6^2}{1728}.$$

Заметим, что $1728 = 2^6 3^3$, так что деление на это число имеет смысл только в тех полях, чья характеристика отлична от 2 и от 3. Известно, что кривая E не-

особенная тогда и только тогда, когда $\Delta \neq 0$. Поэтому ниже будем предполагать, что $\Delta \neq 0$.

Для неособенных кривых вводится понятие j-инварианта

$$j(E) = \frac{c_4^3}{\Delta}.$$

Рассмотрим пример эллиптической кривой, определенной над полем $\mathbf{F}_7$, к которому часто будем возвращаться

$$E\colon Y^2 = X^3 + X + 3. \qquad (2)$$

Вычисляя выписанные ранее константы, найдем $\Delta = 3$ и $j(E) = 5$.

Инвариант j тесно связан с понятием *изоморфизма эллиптических кривых*. Говорят, что кривая E с координатами X и Y изоморфна над полем K кривой E' с координатами X' и Y' (обе заданы уравнением Вейерштрасса), если найдутся такие константы $r, s, t \in K$ и $u \in K^*$, что при замене переменных

$$X = u^2X' + r,$$
$$Y = u^3Y + su^2X' + t$$

кривая E перейдет в кривую E'. Отметим, что изоморфизм кривых определен относительно поля K.

Вернемся к нашему примеру, т.е. к кривой E из (2) над полем $\mathbf{F}_7$. Сделаем замену переменных с набором констант

$$[u, r, s, t] = [2, 3, 4, 5],$$

т.е. положим

$$X = 4X' + 3,$$
$$Y = Y + 2X' + 5.$$

Получим изоморфную кривую, задаваемую уравнением

$$E'\colon Y'^2 + 4X'Y' + 3Y' =$$
$$= X'^3 + X' + 1.$$

Легко убедиться, что $j(E) = j(E') = 5$.

Изоморфизм эллиптических кривых является отношением эквивалентности. Следующая лемма показывает, что j-инвариант разделяет классы эквивалентности этого отношения над алгебраическим замыканием $\overline{K}$ поля K.

Л е м м а 1. Изоморфные над полем K кривые имеют один и тот же j-инвариант. Любые кривые с совпадающими j-инвариантами изоморфны над алгебраическим замыканием $\overline{K}$.

Однако кривые с одним и тем же j-инвариантом не обязательно изоморфны над основным полем. Например, j-инвариант кривой над полем $\mathbf{F}_7$, заданной уравнением

$$E'': \quad Y''^2 = X''^3 + 4X'' + 4,$$

равен 5, как и у кривой E (см. (2)). Однако эти кривые не изоморфны над $\mathbf{F}_7$, поскольку замена переменных, задающая изоморфизм, выглядит следующим образом

$$X = 3X'' \quad \text{и} \quad Y = \sqrt{6}\, Y''.$$

Однако $\sqrt{6} \notin \mathbf{F}_7$. Итак, кривые E и E'' определены над полем $\mathbf{F}_7$, но не изоморфны над ним. Эти кривые будут изоморфны над любым алгебраическим расширением поля $\mathbf{F}_7$, содержащим элемент $\sqrt{6}$, например, над полем

$$\mathbf{F}_7^2 = \mathbf{F}_7\,[\sqrt{6}\,].$$

Групповой закон

Допустим, что $char\ K \neq 2, 3$ и рассмотрим замену переменных

$$X = X' - \frac{b_2}{12},$$
$$Y = Y' - \frac{a_1}{2}\left(X' - \frac{b_2}{12}\right) - \frac{a_3}{2},$$

переводящую кривую, заданную длинной формой Вейерштрасса (1), в изоморфную ей кривую, определяемую *короткой формой Вейерштрасса*

$$E: \ Y^2 = X^3 + aX + b,$$

при некоторых $a, b \in K$. На таких представителях классов изоморфных эллиптических кривых можно наглядно ввести групповой закон *методом хорд и касательных.*

Сложение точек определяется с помощью хорд (см. рис. 1). Пусть P и Q – две точки кривой. Соединим их прямой линией. Она обязательно пересечет кривую в какой-то третьей точке R, поскольку пересекается кубическая кри-

вая прямой. Точка R будет определена над тем же полем, что сама кривая и исходные точки P и Q. Отразим затем точку R относительно горизонтальной оси координат и получим точку, определенную над основным полем. Последняя точка и будет суммой $P + Q$.

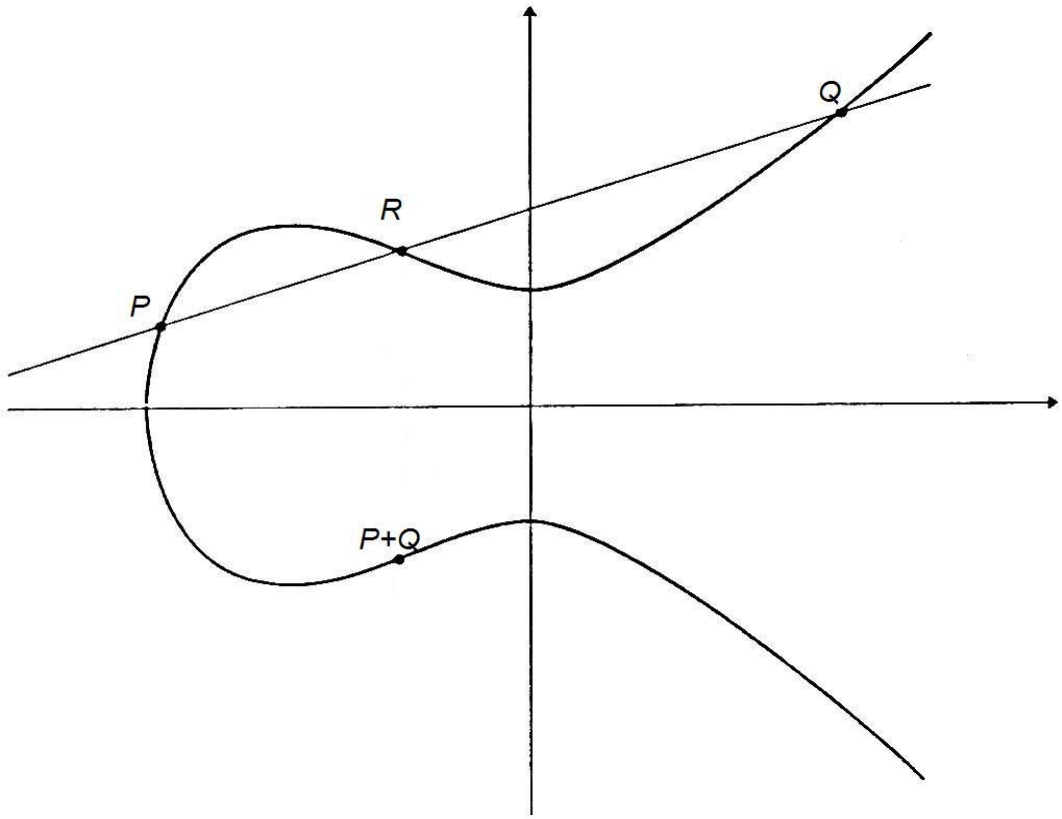

Рис. 1. Сложение точек на эллиптической кривой

Касательные служат для удвоения точек – используя хорду, нельзя сложить точку с собой.

Пусть P – произвольная точка эллиптической кривой (рис. 2). Проведем в точке P касательную к построенной кривой. Данная касательная пересечет кривую еще в какой-то одной точке R, потому что кубическая кривая пересекается с прямой в трех точках с учетом кратности пересечения. Отразив R относительно горизонтальной оси, получим точку $P = P + +P$ [2]. Вертикальная касательная в точке P «пересекает» кривую в бесконечно удаленной точке. В этой ситуации $P + P = O$ и говорят, что P есть *точка порядка* 2.

Можно показать, что метод хорд и касательных наделяет эллиптическую кривую структурой абелевой группы с бесконечно удаленной точкой в качестве единичного элемента, т.е. нуля. Определение операций можно легко перенести на случай общей эллиптической кривой, заданной длинной формой Вейерштрасса, в частности, характеристика поля может быть любой. Необходимо только заменить отражение относительно оси абсцисс на симметрию относительно прямой

$$Y = a_1X + a_3.$$

В дополнение к сказанному приведем алгебраические формулы, реализующие сложение точек по методу хорд и касательных. Это необходимо сделать, поскольку вычерчивание диаграмм в поле конечной характеристики сложно.

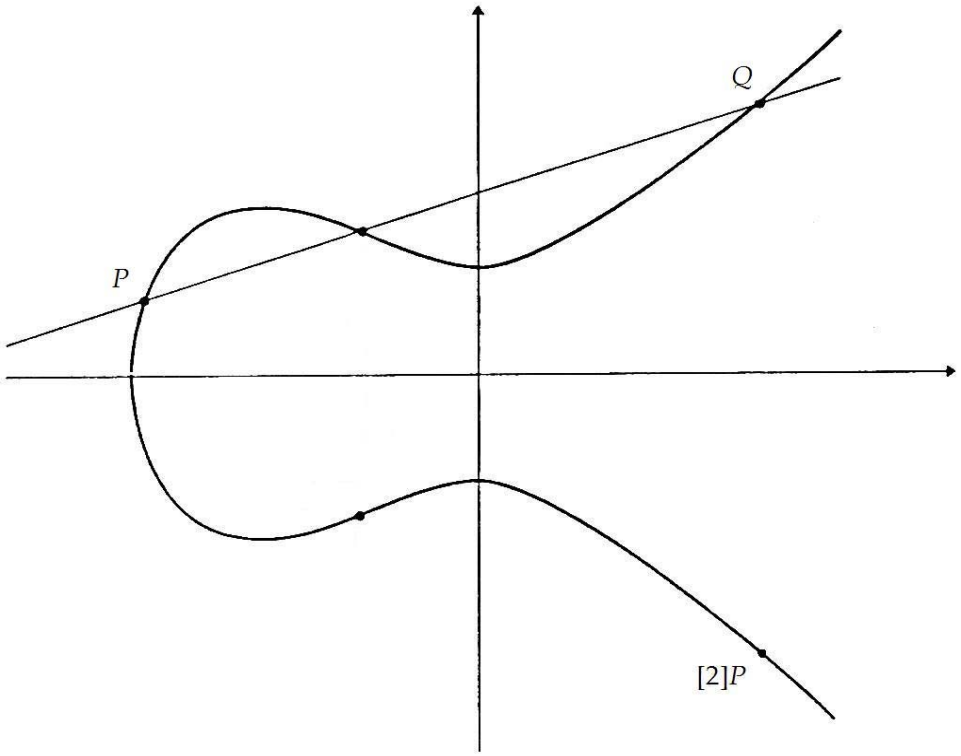

Рис. 2. Удвоение точек на эллиптической кривой

Л е м м а 2. Пусть E – эллиптическая кривая, определяемая уравнением

$$E: \quad Y^2 + a_1XY + a_3Y = \\ = X^3 + a_2X_2 + a_4X + a_6,$$

на которой выбраны точки $P_1(x_1, y_1)$ и $P_2(x_2, y_2)$. Точка P_1 имеет координаты

$$-P_1(x_1 - y_1 - a_1x_1 - a_3).$$

Введем коэффициенты

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \mu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

при $x_1 \neq x_2$ и соотношения

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},$$

$$\mu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3},$$

если $x_1 = x_2$, но $P_2 \neq P_1$. Если

$$P_3(x_3, y_3) = P_1 + P_2 \neq O,$$

то x_3 и y_3 вычисляются по формулам

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3.$$

Описанный ранее изоморфизм эллиптических кривых сохраняет структуру группы. Так что на изоморфных кривых указанные формулы определяют структуры изоморфных абелевых групп.

Зафиксируем натуральное число m и обозначим через $[m]$ отображение кривой на себя, сопоставляющее каждой точке P ее кратное $[m]P$, т.е.

$$[m]: P \mapsto \underbrace{P + P + \ldots P}_{m}.$$

Это отображение – основа криптографических систем, опирающихся на эллиптическую кривую, поскольку его можно легко вычислить, но крайне сложно обратить, т.е. по данным координатам $P(x, y)$ и $[m]P(x', y')$ найти m очень трудно. Конечно, данное высказывание о сложности обращения предполагает специальный выбор эллиптической кривой и соблюдение нескольких других условий, к чему ниже еще вернемся.

Закончим этот раздел иллюстрацией группового закона на эллиптической кривой. Вновь рассмотрим кривую E над полем $\mathbf{F}_7$, заданную уравнением (2). Оказывается, на этой кривой всего лишь шесть точек, одна из которых O, а координаты других представлены списком:

$$(4, 1),\ (6, 6),\ (5, 0),\ (6, 1),\ (4, 6).$$

Результаты сложения несложно получить по формулам леммы 2. Сведем их в табл. 20.

Таблица 20

Сложение точек на кривой (4) над полем $\mathbf{F}_7$

+	*O*	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
O	*O*	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)
(4,1)	(4,1)	(6,6)	(5,0)	(6,1)	(4,6)	*O*
(6,6)	(6,6)	(5,0)	(6,1)	(4,6)	*O*	(4,1)
(5,0)	(5,0)	(6,1)	(4,6)	*O*	(4,1)	(6,6)
(6,1)	(6,1)	(4,6)	*O*	(4,1)	(6,6)	(5,0)
(4,6)	(4,6)	*O*	(4,1)	(6,6)	(5.0)	(6,1)

Найдем координаты образов точки $P(4,1)$ при отображении $[m]$ для различных m:

$$[2]P(6, 6), \quad [5]P(4, 6),$$
$$[3]P(5, 0), \quad [6]P=O,$$
$$[4]P(6, 1).$$

Из вычислений видно, что в нашем примере $E(\mathbf{F}_7)$ – конечная циклическая группа порядка 6, а точка P(4, 1) – ее образующая. Эллиптическая кривая над любым конечным полем будет конечной абелевой группой, и, что очень удачно, циклической или близкой к циклической.

Эллиптические кривые над конечными полями

Как отмечалось выше, количество $\mathbf{F}_q$-рациональных точек эллиптической кривой конечно. Обозначим его символом $\#E(\mathbf{F}_q)$. Ожидаемое число точек кривой близко к $(q+1)$ и можно положить

$$\#E(\mathbf{F}_q)= q+1 - t,$$

где «дефект» t называется *следом отображения Фробениуса* в q. В хорошо известной теореме Хассе дана оценка порядка группы $E(\mathbf{F}_q)$.

Теорема 1 (Хассе, 1933). След отображения Фробениуса удовлетворяет неравенству

$$|t| \le 2\sqrt{q}.$$

В примере (2) кривая над полем $\mathbf{F}_7$ имеет 6 точек. Так что след отображения Фробениуса равен 2, что меньше

$$2\sqrt{q} = 2\sqrt{7} \approx 5,29\,.$$

На эллиптической кривой E над полем F_q определено отображение Фробениуса

$$\varphi : E(\overline{F_q}) \to E(\overline{F}_q),$$
$$\varphi(x, y) = (x^q, y^q),$$
$$\varphi(O) = O.$$

Оно сопоставляет точке кривой E точку на той же кривой, вне зависимости от поля, над которым эта точка определена. Кроме того, отображение Фробениуса сохраняет групповую операцию, т.е.

$$\varphi(P + Q) = \varphi(P) + \varphi(Q).$$

Другими словами, φ — эндоморфизм группы E над алгебраическим замыканием $\overline{F}_q$, который обычно называют *эндоморфизмом Фробениуса.*

След отображения Фробениуса и эндоморфизм Фробениуса связаны уравнением:

$$\varphi^2 - [t]\varphi + [q] = [0],$$

т.е. для произвольной точки $P(x, y)$ кривой выполнено соотношение

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = O,$$

в котором сложение и вычитание – суть групповые операции на эллиптической кривой. Есть два частных случая криптографически непригодных эллиптических кривых:

– Кривая $E(\mathbf{F}_q)$*)* называется *аномальной,* если ее след Фробениуса равен 1, т.е. $\#E(\mathbf{F}_q) = q$. Эта кривая особенно неудобна, когда q – простое число.

– Кривая $E(\mathbf{F}_q)$ называется *суперсингулярной,* если характеристика p поля $\mathbf{F}_q$ делит след отображения Фробениуса t. Таких кривых также стараются избегать в криптографии. При $q = p$ суперсингулярная кривая насчитывает $(p+1)$ точку, поскольку в этом случае $t = 0$. Если же $q = p^f$, то t у суперсингулярных кривых может принимать значения

$$t = 0,\ t^2 = 2q,\ t^2 = 3q;$$

при нечетном f;

$$\text{если } p = 1 \ mod\ 3, \text{ то } t^2 = 4q,\ t^2 = q,$$
$$\text{если } p \neq 1 \ mod\ 4, \text{ то } t = 0,$$

при четном f.

Выбирая кривую для шифрования, нужно стремиться к тому, чтобы число ее точек делилось на достаточно большое простое число. В связи с этим необходимо научиться вычислять порядок группы $E(\mathbf{F}_q)$.

Известно, что порядок произвольной группы $E(\mathbf{F}_q)$ над любым полем вычисляется за полиномиальное время. Это делается с помощью сложного алгоритма, который здесь не будем приводить. Достаточно запомнить, что вычисление порядка группы возможно как в теоретическом, так и в практических планах. Рассматривая алгоритмы решения задачи о дискретных логарифмах видно, что информация о порядке группы очень существенна для оценки стойкости протокола, основанного на соответствующей кривой.

Одним из достоинств эллиптических кривых является то, что они доставляют большое число возможных групп. Можно менять как основное поле, так и коэффициенты уравнения кривой. Наконец, отыскать эллиптическую кривую с хорошими криптографическими свойствами для создания безопасного протокола, относительно легко.

Как было отмечено ранее, случаи *char* $K = 2,3$ требуют дополнительных усилий. Реализация криптографических систем, основанных на эллиптической кривой, базируется на поле $\mathbf{F}_2^n$, чья характеристика равна 2, или на поле $\mathbf{F}_p$ с большим простым числом p. Поэтому в конце сконцентрируем внимание на полях характеристики 2 и $p > 3$, опустив случай *char* $K = 3$. Большинство общих рассуждений с некоторой модификацией переносится на случай характеристики три, что хорошо освещено в специальной литературе.

Кривые над полем характеристики p > 3

Пусть основное поле $K = \mathbf{F}_q$ с $q = p^n$, где $p > 3$ – простое число и $n \geq 1$. Как уже отмечалось, уравнение кривой над таким полем можно представить в виде короткой формы Вейерштрасса

$$E: Y^2 = X^3 + aX + b. \qquad (3)$$

Ее дискриминант равен

$$\Delta = -16(4a^3 + 27b^2),$$

а j-инвариант вычисляется по формуле

$$j(E) = -1728(4a)^3/\Delta.$$

Формулы из леммы 2, описывающие групповой закон, также упрощаются

$$P_1 = (x_1, -y_1).$$

Если

$$P_3(x_3, y_3) = P_i + P_2 \neq O,$$

то координаты (x_3, y_3) вычисляются следующим образом

$$x_3 = \lambda^2 - x^1 - x_2,$$
$$y_3 = (x_1 - x_3)\lambda - y_1,$$

где при $x_1 \neq x_2$ имеет место

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1},$$

а при $x_1 = x_2$ и $y_1 \neq 0$ получим

$$\lambda = \frac{3x_1^2 + a}{2y_1}.$$

Кривые над полем характеристики 2

Здесь ограничимся конечными полями $\mathbf{F}_q$ с $q = 2^n$ при $n \geq 1$. В этом случае j-инвариант кривой E вычисляется по формуле

$$j(E) = \frac{a_1^{12}}{\Delta}.$$

Условие $j(E) = 0$, т.е. $a_1 = 0$ в характеристике 2 равносильно суперсингулярности кривой E. Мы уже отмечали, что суперсингулярные кривые – очень специфический случай, который не используется в криптографии. Поэтому будем предполагать, что $j(E) \neq 0$.

В этих предположениях представитель любого класса изоморфизма эллиптических кривых над $\mathbf{F}_q$ записывается уравнением

$$E: Y^2 + XY = X^3 + a_2X^2 + a_6, \qquad (4)$$

где $a_6 \in \mathbf{F}_q^*$ и $a_2 \in \{0,\gamma\}$. Здесь γ — фиксированный элемент поля $\mathbf{F}_q$, удовлетворяющий соотношению

$$\mathrm{Tr}_{q|2}(\gamma) = 1,$$

где $\mathrm{Tr}_{q|2}$ — абсолютный след, вычисляющийся по формуле

$$\mathrm{Tr}_{2^n|2}(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}.$$

Когда характеристика поля равна 2, формула для противоположного элемента эллиптической кривой из леммы 2 преобразуется к виду

$$-P_1 = (x_1, y_1 + x_1).$$

Если

$$P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$$

то

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2,$$
$$y_3 = (\lambda + 1)x_3 + \mu = (x_1 + x_3)\lambda + x_3 + y_1,$$

где при $x_1 \neq x_2$

$$\lambda = \frac{y_2 + y_1}{x_2 + x_1}, \qquad \mu = \frac{y_1 x_2 + y_2 x_1}{x_2 + x_1};$$

а если $x_1 = x_2 \neq 0$, то получим

$$\lambda = \frac{x_1^2 + y_1}{x_1}, \quad \mu = x_1^2.$$

Проективные координаты

Одна из проблем, возникающих при использовании формул группового закона как при большой, так и при четной характеристике поля, связана с необходимостью деления. Деление в конечном поле считается дорогой операцией, потому что деление включает в себя некий вариант расширенного алгоритма Евклида. Данный алгоритм хотя и имеет приблизительно ту же сложность, что и умножение, однако обычно не может быть реализован достаточно эффективно.

Во избежание операции деления применяют проективные координаты. При этом уравнение эллиптической кривой записывается через три координаты (X, Y, Z) вместо двух (X, Y). Однако вместо стандартного варианта уравнения кривой, который был приведен ранее, используется уравнение вида

$$E: Y^2 + a_1 XYZ + a_2 YZ^4 =$$
$$= X^3 + a_2 X^2 Z^2 + a_4 XZ^4 + a_6 Z^6.$$

Точка на бесконечности здесь также имеет координаты (0, 1, 0), но переход от проективных координат к аффинным осуществляется по правилу

$$(X, Y, Z) \mapsto (X / Z^2, Y / Z^2).$$

Выбор таких проективных координат обусловлен стремлением сделать арифметические операции более эффективными.

Большая характеристика

Формулы сложения точек эллиптической кривой, заданной уравнением

$$Y^2 = X^3 + aXZ^2 + bZ^6,$$

над полем большой характеристики выглядят теперь следующим образом

$$(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2),$$

где тройка координат (X_3, Y_3, Z_3) вычисляется последовательно по правилу

$$\begin{aligned} \lambda_1 &= X_1 Z_2^2, & \lambda_2 &= X_2 Z_1^2, \\ \lambda_3 &= \lambda_1 - \lambda_2, & \lambda_4 &= Y_1 Z_2^3, \\ \lambda_5 &= Y_2 Z_1^3, & \lambda_6 &= \lambda_4 - \lambda_5 \end{aligned}$$

$$\begin{aligned} \lambda_7 &= \lambda_1 + \lambda_2, & \lambda_8 &= \lambda_4 + \lambda_5, \\ Z_3 &= Z_1 Z_2 \lambda_3, & X_3 &= \lambda_6^2 - \lambda_7 \lambda_3^2, \\ \lambda_9 &= \lambda_7 \lambda_3^2 - 2X_3, & Y_3 &= (\lambda_9 \lambda_6 - \kappa_8 \lambda_3^3)/2 \end{aligned}$$

Следует обратить внимание на тот факт, что здесь нет ни одной операции деления, кроме деления на 2, которая легко заменяется умножением на заранее вычисленное чисто

$$2^{-1} \bmod p.$$

Удвоение точек $(X_3, Y_3, Z_3) = [2] (X_1, Y_1, Z_1)$ упрощается с помощью формул

$$\begin{aligned} \lambda_1 &= 3X_1^2 + aZ_1^4, & Z_3 &= 2Y_1 Z_1, \\ \lambda_2 &= 4X_1 Y_1^2, & X_3 &= \lambda_1^2 - 2\lambda_2, \\ \lambda_3 &= 8Y_1^4, & Y_3 &= \lambda_1(\lambda_2 - X_3) - \lambda_3. \end{aligned}$$

Четная характеристика

Уравнение эллиптической кривой над полем четной характеристики записывается в виде

$$Y^2 + XYZ = X^3 + a_2 X^2 Z^4 + a_6 Z^6.$$

Сложение точек

$$(X_3, Y_3, Z_3) = (X_1, Y_1, Z_1) + (X_2, Y_2, Z_2)$$

в этом случае осуществляется следующим образом

$$\lambda_1 = X_1 Z_2^2, \qquad \lambda_2 = X_2 Z_1^2,$$
$$\lambda_3 = \lambda_1 + \lambda_2, \qquad \lambda_4 = Y_1 Z_2^3,$$
$$\lambda_5 = Y_2 Z_1^3, \qquad \lambda_6 = \lambda_4 + \lambda_5$$

$$\lambda_7 = Z_1 \lambda_3, \qquad \lambda_8 = \lambda_6 X_2 + \lambda_7 Y_2,$$
$$Z_3 = \lambda_7 Z_2, \qquad \lambda_9 = \lambda_6 + Z_3,$$
$$X_3 = a_2 Z_3^2 + \lambda_6 \lambda_9 + \lambda_3^4, \qquad Y_3 = \lambda_9 X_3 + \lambda_8 \lambda_7^2.$$

Наконец, координаты удвоенной точки определяются по правилу:

$$Z_3 = X_1 Z_1^2, \qquad X_3 = (X_1 + a_6 Z_1^2)^4,$$
$$\lambda = Z_3 + X_1^2 + Y_1 Z_1, \qquad Y_3 = X_1^4 Z_3 + \lambda X_3.$$

Итак, в обоих интересных случаях, при большой и четной характеристиках поля, исключили дорогостоящую операцию деления.

Сжатие точек

Во многих криптографических протоколах возникает необходимость хранить в памяти или передавать по сети отдельные точки эллиптической кривой. В аффинных координатах это можно сделать с помощью двух элементов поля – координат *x* и *y*. Однако экономнее применять так называемую технику сжатия точек.

Метод сжатия точек работает благодаря тому что уравнение кривой в аффинных координатах при фиксированном значении *x* превращается в квадратное уравнение относительно координаты *y*. Поэтому каждому возможному значению координаты *x* точки кривой соответствует не более двух значений координаты *y*. Значит, вместо двух координат для идентификации точки кривой можно хранить в памяти компьютера только координату *x* и еще некий

двоичный параметр b, сообщающий о том, какое именно значение координаты y нужно брать. Остается только решить, как вычислять параметр b и как по нему и данному x восстановить y - координату нужной точки.

Случай большой характеристики поля

Заметим, что если $p > 2$, то квадратные корни $\pm\beta$ элемента $a \in \mathbf{F}_p$ представляются натуральными числами разной четности из промежутка 1, ..., (p-1), поскольку имеет место

$$-\beta = \boldsymbol{p} - \beta \bmod p.$$

Таким образом, в качестве параметра b можно выбрать четность y- координаты соответствующей точки. Покажем теперь, как восстановить полную информацию о координатах точки по паре (x, b). Сначала вычисляется значение

$$\beta = \sqrt{x^3 + ax + b} \bmod p,$$

а затем переменной y присваивают значение β, если четность β совпадает с четностью b, и (p- β), когда четности разные. Если же оказалось, что $\beta = 0$, то, не обращая внимания на параметр b, можно положить $y = 0$.

В качестве примера рассмотрим кривую

$$E: Y^2 = X^3 + X + 3$$

над полем $\mathbf{F}_7$. Для представления каждой из ее точек (4, 1) и (4, 6) в двоичной системе счисления потребуется шесть разрядов

$$(0\text{b } 100,0\text{b } 001) \quad \text{и} \quad (0\text{b } 100,0\text{b } 110),$$

в то время как при использовании метода сжатия точек всего четыре

$$(0\text{b } 100,0\text{b } 1) \quad \text{и} \quad (0\text{b } 100,0\text{b } 0).$$

В реальных криптографических протоколах получается более существенная экономия компьютерной памяти. Рассмотрим, например, ту же кривую, но над полем $\mathbf{F}_p$ при значении

$$p = 1\ 125\ 899\ 906\ 842\ 679 = 2^{50} + 55.$$

На ней есть точка с координатами

$$(1\ 125\ 899\ 906\ 842\ 675,245\ 132\ 605\ 757\ 739),$$

для записи которой потребовалось 102 разряда. При сжатии информации эту точку можно представить в виде

(1 125 899 906 842 675,1),

где использовано только 52 разряда.

Четная характеристика

В случае четной характеристики необходимо проявить больше изобретательности. Предположим, что дана точка $P(x, y)$ на эллиптической кривой

$$Y^2 + XY = X^3 + a_2 X^2 + a_6. \qquad (5)$$

Если $y = 0$, то можно положить $b = 0$. В противном случае вычисляют $z = y/x$ и присваивают переменной b самый младший двоичный разряд числа z. Для восстановления y по данной паре (x, b) в случае $x \neq 0$ вычисляют

$$\alpha = x + a_2 + \frac{a_6}{x^2}$$

и обозначают через β одно из решений уравнения

$$z^2 + z = a.$$

Если наименьший двоичный разряд числа β совпадает с b, то $y = x\beta$. В противном случае $y = x(\beta+1)$. Для объяснения того, почему этот метод правильно восстанавливает y - координату точки, напомним, что координаты (x, y) точки P есть решение уравнения (5). Поэтому пары $(x, y/x)$ и $(x, 1+y/x)$ удовлетворяют соотношению

$$Z^2 + Z = X + a_2 + \frac{a_6}{X^2}.$$