Инфраструктура открытых ключей

(***PKI*** *- Public Key Infrastructure*)

Основные атаки на ЭП

Инфраструктура открытых ключей

- Набор средств (технических, материальных, людских и т. д.), распределённых служб и компонентов, в совокупности используемых для поддержки криптозадач на основе закрытого и открытого ключей.

В основе PKI лежит использование криптографической системы с открытым ключом и несколько основных принципов:

- закрытый ключ известен только его владельцу;
- удостоверяющий центр создает сертификат открытого ключа, таким образом удостоверяя этот ключ;
- никто не доверяет друг другу, но все доверяют удостоверяющему центру;
- удостоверяющий центр подтверждает или опровергает принадлежность открытого ключа заданному лицу, которое владеет соответствующим закрытым ключом.

Основные компоненты PKI

Удостоверяющий центр (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей. УЦ является главным управляющим компонентом PKI:

1. он является доверенной третьей стороной (trusted third party)
2. это сервер, который осуществляет управление сертификатами.

Сертификат открытого ключа (чаще всего просто *сертификат*) — это данные пользователя и его открытый ключ, скреплённые подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет секретным ключом, который соответствует этому открытому ключу.

Регистрационный центр (РЦ) — необязательный компонент системы, предназначенный для регистрации пользователей. Удостоверяющий центр доверяет регистрационному центру проверку информации о субъекте. Регистрационный центр, проверив правильность информации, подписывает её своим ключом и передаёт удостоверяющему центру, который, проверив ключ регистрационного центра, выписывает сертификат. Один регистрационный центр может работать с несколькими удостоверяющими центрами (то есть состоять в нескольких PKI), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.

Основные компоненты PKI

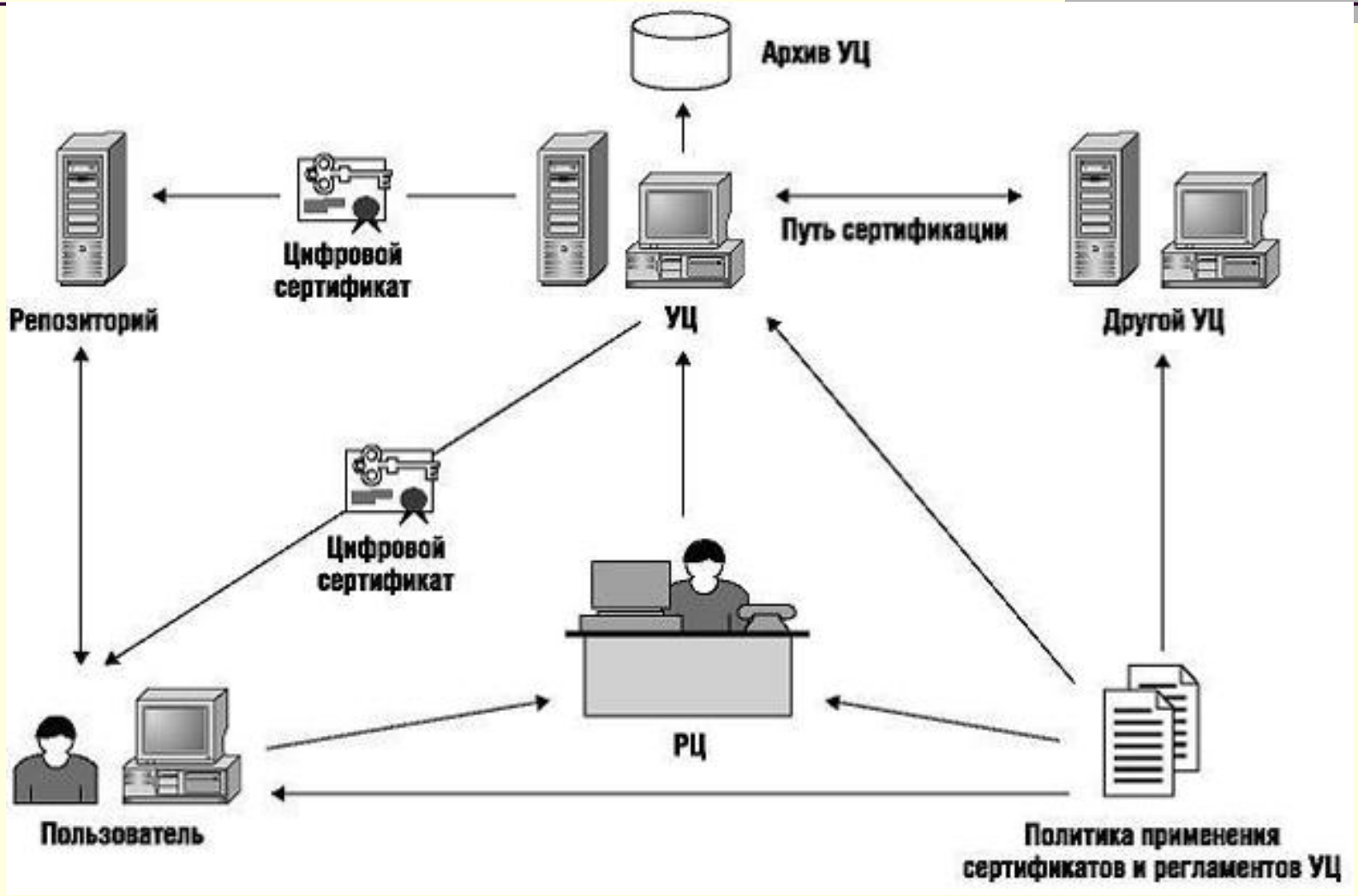
Репозиторий — хранилище, содержащее сертификаты и списки отозванных сертификатов (СОС) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется *реестр сертификатов ключей подписей*.

Архив сертификатов — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.

Центр запросов — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат.

Конечные пользователи — пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

Основные компоненты PKI



Удостоверяющий центр выполняет следующие основные функции:

- формирует собственный секретный ключ;
- создает и подписывает *сертификаты открытых ключей* подчиненных *удостоверяющих центров* и *конечных субъектов* PKI; может выпускать *кросс-сертификаты*, если связан отношениями доверия с другими PKI;
- поддерживает ***реестр сертификатов*** (базу всех изданных сертификатов) и формирует списки аннулированных сертификатов (CAC) с регулярностью, определенной регламентом *УЦ* ;
- публикует информацию о *статусе сертификатов* и списков аннулированных сертификатов.

Репозиторий сертификатов

Репозиторий - специальный объект *инфраструктуры открытых ключей*, база данных, в которой хранится *реестр сертификатов.*

Репозиторий значительно упрощает управление системой и доступ к ресурсам. Он предоставляет информацию о *статусе сертификатов*, обеспечивает хранение и распространение сертификатов и CAC, управляет внесениями изменений в сертификаты.

К *репозиторию* предъявляются следующие требования:

- простота и стандартность доступа;
- регулярность обновления информации;
- встроенная защищенность;
- простота управления;
- совместимость с другими хранилищами (необязательное требование).

Архив сертификатов

На ***архив сертификатов*** возлагается функция долговременного хранения (от имени *УЦ*) и защиты информации обо всех изданных сертификатах. *Архив* поддерживает базу данных, используемую при возникновении споров по поводу надежности электронных цифровых подписей, которыми в прошлом заверялись документы. Информация, предоставляемая *УЦ архиву*, должна быть достаточной для определения статуса сертификатов и их издателя. *Архив* должен быть защищен соответствующими техническими средствами и процедурами.

Конечные субъекты

Конечные субъекты, или **пользователи**, PKI делятся на две категории:

- владельцы сертификатов
- доверяющие стороны.

Они используют некоторые сервисы и функции PKI, чтобы получить сертификаты или проверить сертификаты других субъектов.

Владельцем сертификата может быть физическое или юридическое лицо, приложение, сервер и т.д.

Серверные компоненты PKI

Основными серверными компонентами PKI являются

сервер сертификатов,

сервер каталогов

сервер восстановления ключей, опциональными компонентами –

сервер регистрации,

OCSP-сервер, обслуживающий запросы пользователей по *онлайновому протоколу статуса сертификата*

сервер проставления меток времени.

Серверные компоненты PKI

Сервер каталогов должен обеспечивать:

- сетевую аутентификацию через IP-адреса или DNS-имена и аутентификацию *конечных субъектов* по именам и паролям или по *сертификатам открытых ключей*;
- управление доступом субъектов к информации в зависимости от их прав на выполнение операций чтения, записи, уничтожения, поиска или сравнения;
- конфиденциальность и целостность сообщений для всех видов связи.

Серверные компоненты PKI

Сервер восстановления ключей поддерживает создание резервных копий и восстановление ключей шифрования *конечных субъектов*.

Среди всех компонентов PKI *сервер восстановления ключей* должен быть наиболее защищен и обеспечивать *сильную аутентификацию* администратора и пользователей, поддержку конфиденциальности и целостности сообщений, безопасное хранение всех компонентов ключей.

Основные задачи системы информационной безопасности, которые решает инфраструктура управления открытыми ключами:

- обеспечение конфиденциальности информации;
- обеспечение целостности информации;
- обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи;
- обеспечение возможности подтверждения совершенных пользователями действий с информацией (неотказуемость или апеллируемость).
- PKI напрямую не реализует авторизацию, доверие, именование субъектов криптографии, защиту информации или линий связи, но может использоваться как одна из составляющих при их реализации.

Основные атаки на ЭП

- кража ключа и подмена подписываемой информации;
- несанкционированный доступ к средству электронной подписи (например, USB-токену) посредством кражи его PIN-кода.

Реализация атак

- Внедрение вредоносного ПО, которое способно похищать ключи, PIN-коды и делать подмену документов посредством чтения и/или подмены данных в памяти системного процесса.
- Атака man-in-the-middle, направленная на модификацию подписываемых данных на web-странице или на кражу PIN-кода или на перехват secure token для возможности подмены абонента системы.
- Атака на клиента с помощью CSS

Комплексные меры защиты клиента (организации) при получении и использовании ЭП

- Персонал;
- Режим;
- Использование СКЗИ, которые имеют сертификат ФСБ России;
- Использование современных сетевых криптографических протоколов (TLS 1.3);
- Использование специальных аппаратных средств для визуализации подписываемых данных перед наложением подписи (TrustScreen);
- Корректная реализация браузерных плагинов и расширений, которые обеспечивают ЭП в браузере;
- Регламентирование процедуры подписи для пользователя с учетом встроенных в браузер механизмов безопасности;
- Защита ОС от вредоносного ПО (создание доверенной среды).

Персонал

- Должен быть определен и утвержден список лиц (прошедших соответствующую подготовку и ознакомленных с пользовательской документацией на СКЗИ, а также другими нормативными документами по использованию электронной подписи), имеющих доступ к ключевой информации;
- В случае увольнения или перевода в другое подразделение, изменения функциональных обязанностей сотрудника, имевшего доступ к ключевым носителям (ЭП и шифрования), должна быть проведена смена ключей, к которым он имел доступ.

Режим

- Использовать автоматизированное рабочее место (АРМ) с СКЗИ в однопользовательском режиме;
- не оставлять без контроля АРМ;
- соблюдать утвержденный порядок учета, хранения и использования носителей ключевой информации с ключами ЭП;
- предусмотреть меры, исключающие возможность несанкционированного изменения аппаратной части АРМ.

Использование СКЗИ, которые имеют сертификат ФСБ России

В токенах используемых при работе с ЭП реализованы криптографические алгоритмы преобразования информации, соответственно, относятся к числу средств криптографической защиты информации (СКЗИ).

Для использования усиленной квалифицированной электронной подписи подходят только токены, для которых подтверждено соответствие требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и Приказом ФСБ РФ от 27 декабря 2011 г. № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра». Это соответствие подтверждается наличием сертификата соответствия, выданного ФСБ России, в котором соответствующая информация приводится в явном виде.

Алгоритмы электронной подписи.
Схема Эль-Гамаля
ГОСТ 34.10-2018

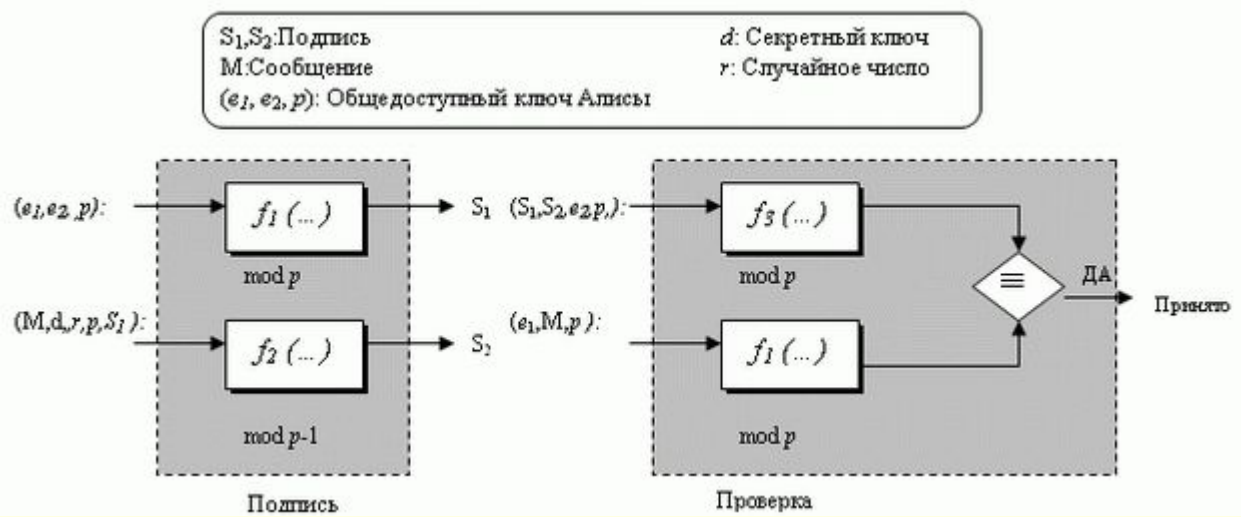
Схема Эль-Гамаля

- Алгоритм Эль-Гамаля базируется на трудности вычисления дискретного логарифма;

Алгоритм состоит из двух основных этапов:

- формирование цифровой подписи;
- ее проверка на подлинность.

Схема Эль-Гамаля



В процессе подписания две функции создают две подписи. На стороне подтверждения обрабатывают выходы двух функций и сравнивают между собой для проверки. Одна и та же функция применяется и для подписания, и для проверки, но использует различные входы. Рисунок показывает входы каждой функции. Сообщение - часть входа, для обеспечения функционирования при подписании; оно же - часть входа к функции 1 при подтверждении. Вычисления в функциях 1 и 3 проводятся по модулю p, а функции 2 - по модулю p - 1.

Генерация ключей

- Выберем достаточно большое простое число p $(\sim 10^{308}$ *или* $\sim 2^{1024})$
- Пусть e_1 - простой элемент в Z_{p^*}(мультипликативная группа по модулю p).
- Алиса выбирает свой секретный ключ d, чтобы он был меньше, чем p - 1.
- Она вычисляет $e_2 = e_1^d$.

В *схеме цифровой подписи Эль-Гамаля*

(e1, e2, p) - открытый ключ Алисы;

d **-секретный ключ Алисы**.

Подписание дайджеста

- Алиса выбирает секретное случайное число r (открытые и секретные ключи могут использоваться неоднократно, но для каждого нового сообщения Алиса выбирает новое r);
- Алиса вычисляет первую подпись $S_1 = e1^r \bmod p$.
- Алиса вычисляет вторую подпись $S_2 = (M - d \times S_1) \times r^{-1} \bmod (p - 1)$,где r - мультипликативная инверсия r по модулю p - 1.
- Алиса передает M, S_1 и S_2 Бобу.

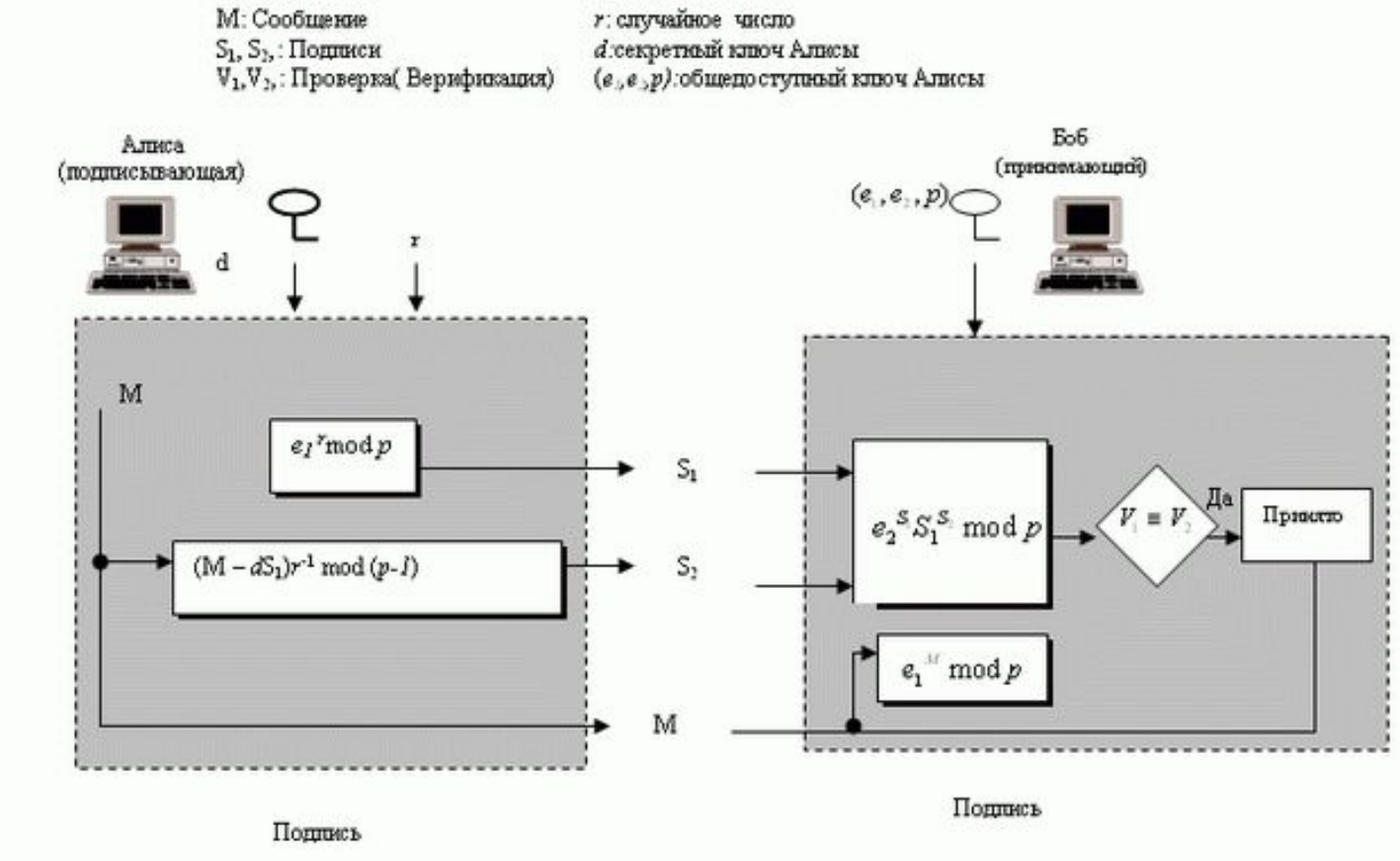
Проверка

Объект, например Боб, получает M, S_1 и S_2 и может проверить их следующим образом.

- Боб проверяет, что $0 < S_1 < p$.
- Боб проверяет, что $0 < S_2 < p - 1$.
- Боб вычисляет $V_1 = e_1^M \bmod p$.
- Боб вычисляет $V_2 = e_2^{S1} \times S_1^{S2} \bmod p$.

Если V_1 является конгруэнтным V_2, сообщение принято; иначе оно будет отклонено.

Схема цифровой подписи Эль-Гамаля



Пример подписание

- Алиса выбрала p = 3119, e_1 = 2, d = 127 и вычислила $e_2 = 2^{127} \bmod 3119 = 1702$. Она выбрала r равным 307. Она объявила e_1, e_2 и p ; она сохранила в тайне d.
- M = 320
- $S_1 = e_1^r = 2^{307} \bmod 3119 = 2083$
- $S_2 = (M - d \times S_1) \times r^{-1} = (320 - 127 \times 2083) \times 307^{-1} = 2105 \bmod 3118$

Пример проверка

Алиса передает M, S_1 и S_2 Бобу. Боб использует открытый ключ, чтобы вычислить, что сообщение подписано Алисой, потому что никто, кроме Алисы, не имеет секретного ключа d.

- $V_1 = e_1^{M} = 2^{320} = 3006 \bmod 3119$;
- $V_2 = d^{S1} \times S_1^{S2} = 1702^{2083} \times 2083^{2105} = 3006 \bmod 3119$.

Поскольку V_1 и V_2 являются конгруэнтными, Боб принимает сообщение, и он предполагает, что сообщение было подписано Алисой, потому что никто, кроме нее, не имеет секретного ключа Алисы d.

ГОСТ 34.10-2018

- *ГОСТ 34.10-2018. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи —*
действующий межгосударственный криптографический ст андарт, описывающий алгоритмы формирования и проверки электронной подписи реализуемой с использованием операций в группе точек эллиптической кривой, определенной над конечным простым полем.
- Стандарт разработан на основе национального стандарта Российской Федерации **ГОСТ Р 34.10-2012** и введен в действие с 1 июня 2019
года приказом Росстандарта № 1059-ст от 4 декабря 2018 года.

ГОСТ 34.10-2018

Механизм цифровой подписи определяется посредством реализации двух основных процессов:

- формирование подписи;
- проверка подписи.

(В настоящем стандарте процесс генерации ключей не рассмотрен. Характеристики и способы реализации данного процесса определяются вовлеченными в него субъектами, которые устанавливают соответствующие параметры по взаимному согласованию.)

ГОСТ 34.10-2018

Криптографическая стойкость данной схемы цифровой подписи основывается на сложности решения задачи дискретного логарифмирования в группе точек эллиптической кривой, а также на стойкости используемой хэш-функции.

Алгоритмы вычисления хэш-функции установлены в ГОСТ 34.11.

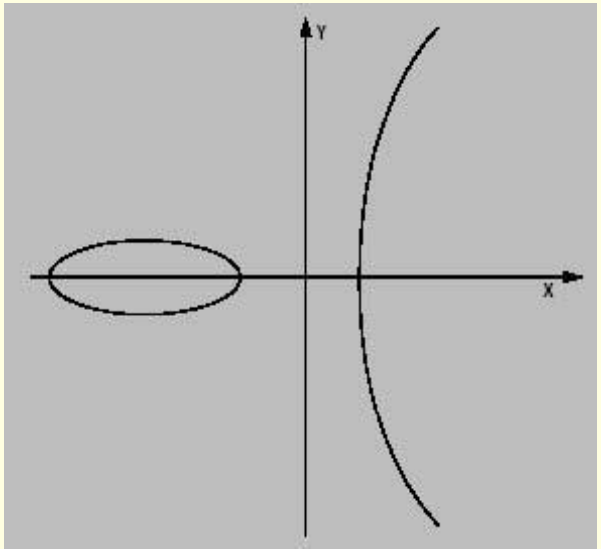
Цифровая подпись, представленная в виде двоичного вектора длиной 512 или 1024 бита

Криптография на эллиптических кривых

Эллиптической кривой называют множество пар точек (X,Y), удовлетворяющих уравнению:

$y^2 = ax^3 + bx + c$

Можно наложить ограничения на множество значений переменных x, y, и коэффициентов a, b, c. Ограничивая область определения уравнения значимым для приложений числовым множеством (полем) мы получим эллиптическую кривую, заданную над рассматриваемым полем. На рисунке изображен общий вид эллиптической кривой, определенной на множестве действительных чисел.

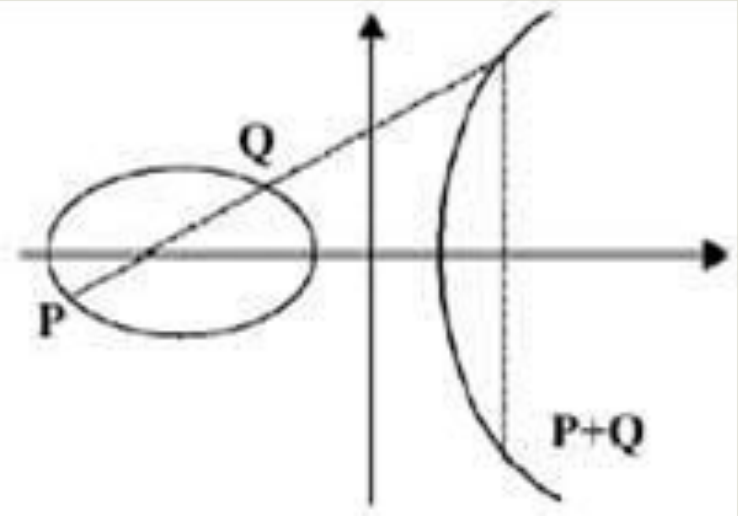


Криптография на эллиптических кривых

В приложении к криптографии (и в новом стандарте на цифровую подпись) эллиптическая кривая над конечным простым полем GF(p) определяется как множество пар (x,y), таких что x,y ≡ GF(p), удовлетворяющих уравнению:

$y^2 = x^3 + ax + b \bmod p,\ a, b \equiv GF(p)$

Пары (x,y) будем называть точками. Точки эллиптической кривой можно складывать. Сумма двух точек, в свою очередь, тоже лежит на эллиптической кривой.



Криптография на эллиптических кривых

Математическое свойство, которое делает эллиптические кривые полезными для криптографии, состоит в том, что если взять две различных точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Если мы обозначим две первоначальных точки как P и Q, то получим последнюю – отраженную – точку P+Q. Это «сложение» удовлетворяет всем известным алгебраическим правилам для целых чисел.

Кроме точек, лежащих на эллиптической кривой, рассматривается также нулевая точка. Считается, что сумма двух точек – A с координатами (X_A, Y_A) и B с координатами (X_B, Y_B) – равна 0, если $X_A = X_B$, $Y_A = -Y_B \pmod p$. Нулевая точка не лежит на эллиптической кривой, но, тем не менее, участвует в вычислениях. Ее можно рассматривать как бесконечно удаленную точку.

Криптография на эллиптических кривых

Можем определить конечную абелеву группу на точках кривой, где нулем будет являться бесконечно удаленная точка. В частности если точки P и Q совпадут, то можно вычислить P+P, т.е. 2P. Развивая эту идею, можно определить kP для любого целого числа k, и следовательно, определить значение P и значение наименьшего целого числа k, такого, что kP = F, где F – бесконечно удаленная точка.

Кратные точки эллиптической кривой являются аналогом степеней чисел в простом поле. Задача вычисления кратности точки эквивалентна задаче вычисления дискретного логарифма. На сложности вычисления кратности точки эллиптической кривой и основана надежность цифровой подписи.

Секретным ключом является некоторое случайное число x. Открытым ключом будем считать координаты точки на эллиптической кривой P, определяемую как P = xQ, где Q — специальным образом выбранная точка эллиптической кривой («базовая точка»). Координаты точки Q вместе с коэффициентами уравнения, задающего кривую, являются параметрами схемы подписи и должны быть известны всем участникам обмена сообщениями.

Формирование подписи ГОСТ 34.10-2018

Основные шаги:

1. Вычисление хэш-функции от сообщения;
2. Генерация случайного числа k (элемента секретного ключа) и вычисление точки эллиптической кривой;
3. Вычисление (на основе полученных данных) двух векторов, их конкатенация и формирование ЭП

Криптопровайдеры сертифицированные ФСБ

- КриптоАРМ
- ViPNet CSP
- Signal-COM CSP

КриптоПро

Наиболее популярный в РФ криптопровайдер. Он работает под всеми популярными системами – Windows, Linux, Mac OS. Существует также несертифицированная версия для Android.

КриптоАРМ 5
КриптоАРМ ГОСТ

- КриптоАРМ — программа для подписи и шифрования электронных документов.
- Используется для обеспечения юридической значимости при обмене электронными документами, в том числе с государственными учреждениями Росреестр, ФСРАР, Банк России, РосАккредитация и др.

Функциональные возможности программы:

- шифрование и расшифрование файлов произвольного формата (преобразования файлов функциями СКЗИ);
- создание и проверка корректности одной или нескольких ЭЦП;
- выполнение операций подписи и шифрования за одно действие;
- управление цифровыми сертификатами и ключами пользователя, списками отозванных и доверенных сертификатов;
- управление криптопровайдерами;
- совместимость с отчуждаемыми ключевыми носителями Рутокен, eToken;
- отправка подписанных и зашифрованных файлов по e-mail.

ViPNet CSP 4

Бесплатный российский криптопровайдер от компании ИнфоТеКС, имеющий все необходимые сертификаты ФСБ. Он выпускается в вариантах для Windows и Linux.

- Создание ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Шифрование и имитозащита данных по ГОСТ 28147-89

Signal-COM CSP

Signal-COM CSP – российский сертифицированный криптопровайдер, работающий исключительно под Windows. Разработан компанией Сигнал-КОМ.

- Создание ключей ЭП, формирование и проверка ЭП по ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
- Хэширование данных по ГОСТ Р 34.11-94 и ГОСТ Р 34.11-2012
- Шифрование и имитозащита данных по ГОСТ 28147-89

Задание к лекции 1

- Выписать из примера числовые значения открытого и секретного ключа;
- Найти значение r^{-1} modp, если p=11, а r=5.

Задание к лекции 2

Ознакомиться со стандартами разных лет на ЭП, провести сравнительный анализ, отметить основные отличия и записать в таблицу:

	ГОСТ Р 34.10-94	ГОСТ Р 34.10-2001	ГОСТ Р 34.10-2012	ГОСТ 34.10-2018
Длина простого числа p (по модулю которого производятся вычисления)				
Открытый ключ				
Закрытый ключ				
Алгоритм формирования				
Алгоритм проверки				
Криптостойкость				