Министерство образования и науки Российской Федерации
Государственное образовательное учреждение высшего профессионального образования
Южно-Уральский государственный университет
(национальный исследовательский университет)
Факультет Математики, механики и компьютерных наук
Кафедра дифференциальных и стохастических уравнений

РАБОТА ПРОВЕРЕНА
Рецензент, доцент кафедры компьютерной топологии и алгебры ЧелГУ, кандидат физ.-мат. наук
_____ Митина О.В.
_____2016 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой дифференциальных и стохастических уравнений, ЮУрГУ, доктор физ-мат. наук, доцент
_____С.А. Загребина
_____2016 г.

Криптографические системы с открытым ключом и элементы больших порядков в группах

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К МАГИСТЕРСКОЙ ДИССЕРТАЦИИ
ЮУрГУ – 231000.68.2016.293.ПЗ МД

Руководитель, доктор физ-мат.наук, доцент
_____Н.Д. Зюляркина
_____2016 г.

Автор проекта
Студент группы ММи КН-293
_____А.В. Деев
_____2016 г.

Нормоконтролер
_____М.А. Сагадеева
_____2016 г.

Челябинск 2016

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	Срок выполнения этапов работы (проекта)	Отметка о выполнении руководителя
Постановка задачи	01.02.16 – 07.02.16	
Анализ криптографических систем с открытым ключом	08.02.16 – 28.02.16	
Анализ алгоритма шифрования Эль-Гамаля и существующих модификаций	29.02.16 – 11.03.16	
Изучение модификаций криптографической системы с открытым ключом	14.03.16 – 27.03.16	
Рассмотрение возможностей использования элементов больших порядков в группах	28.03.16 – 11.04.16	
Подготовка пояснительной записки	11.04.16 – 17.04.16	
Проверка работы руководителем, исправление замечаний, подготовка графического материала и доклад	18.04.16 – 25.04.16	
Нормоконтроль	26.04.16 – 28.04.16	
Рецензирование, представление зав. кафедрой	29.04.16 – 05.05.16	

Заведующий кафедрой _____ (подпись) С.А. Загребина

Руководитель диссертации _____ (подпись) Н.Д. Зюляркина

Студент _____ А.В. Деев

ОГЛАВЛЕНИЕ

Оглавление 3

Введение 4

1 Криптографические методы защиты информации 6

1.1 Криптосистемы с открытым ключом 7

1.2 Классический шифр Эль-Гамаля 9

1.3 Шифр Эль-Гамаля на эллиптической кривой 11

Алгоритм нахождения точки C. 11

1.4 Алгоритм цифровой подписи Эль-Гамаля (EGSA) 14

2 Защита алгоритма схемы Эль-Гамаля 17

2.1 Задача дискретного логарифмирования 17

2.2 Задача факторизации больших целых чисел 20

3 Модификации шифра Эль-Гамаля 23

3.1 Модификация алгоритма Эль-Гамаля на группе точек эллиптических кривых 23

3.2 Модификация алгоритма Эль-Гамаля (с использованием RSA) 26

3.3 Модификация алгоритма Эль-Гамаля на матричных группах 28

4 Структура группы $GL_m(Z_n)$. 32

4.1 Порядок группы $GL_m(Z_n)$. 32

4.2 Порядок элементов в группе $GL_m(Z_n)$ 34

5 Реализация алгоритмов шифрования 39

5.1 Методы реализации алгоритмов шифрования 39

5.2 Система компьютерной алгебры GAP 41

5.3 Код программы реализации шифрования/ расшифровывания методом Эль-Гамаля 42

Заключение 48

Приложения 51

ВВЕДЕНИЕ

Информация является одним из самых важных ресурсов развития человечества. Современные компьютерные технологии позволяют каждому человеку получить доступ к информации. Но скорости доступа и доступность данных с помощью компьютерных сетей, например, таких как Интернет, без каких-либо ограничений и защит создают угрозы безопасности данных [1]:

- неавторизованная модификация информации;
- неавторизованный доступ как к самой информации, так и к самим сетям и сервисам;
- целенаправленные сетевые атаки.

В настоящее время криптографические методы защиты информации используются очень широко: межбанковские расчеты по компьютерным сетям, расчеты на биржах, расчеты по кредитным картам, переводы заработной платы в банк, заказ билетов через Интернет, покупки в Интернет-магазинах и т.д. [2]

Именно криптография (наука об обеспечении безопасности данных) занимается решениями четырех глобальных проблем безопасности информации - конфиденциальности, аутентификации, целостности и контроля участников взаимодействия. Одним из главных решений ученые видят использования шифрования для обеспечения конфиденциальности, сохранения информации в тайне от тех, кому она не предназначена.

Одним из популярных способов шифрования является использование шифров с открытым ключом. В частности, в XXI веке широко используется шифр Эль-Гамаля, рассматриваемый как на конечных полях, так и на эллиптических кривых. Именно этот шифр положен в основу алгоритмов DSA, ECDSA, а также на нем основан ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» [3].

Криптосистема Эль-Гамаля является одной из первых криптосистем с открытым ключом, которая обеспечивает безопасность общения через публичные незащищенные каналы связи [4]. Криптостойкость метода Эль-Гамаля основана на сложности вычисления дискретного логарифма, поэтому модификации данного шифра связаны с группами, в которых задача дискретного логарифмирования трудно разрешима.

1 КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Криптографическими методами защиты информации называются специальные методы преобразования информации, результатами которого является недоступность информации без предъявления ключа криптограммы. В настоящее время именно криптографический метод защиты является самым надежным так как охраняется содержание (информация), а не доступ к ней.

Современные криптографические методы защиты информации можно разделить на четыре класса:

- симметричные криптосистемы, в которых для шифрования и дешифрования используется один и тот же ключ;
- криптосистемы с открытым ключом, использующие два ключа - открытый и закрытый (связаны друг с другом математически). Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только ограниченному числу лиц;
- системы электронной подписи (присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения);
- процессы управления ключами (процесс системы обработки информации, содержанием которых является составление и распределение ключей между пользователями).

1.1 Криптосистемы с открытым ключом

В 1976 г. У.Диффи и М.Хеллман дали описание криптографических систем с открытым ключом (public key cryptosystem), в основание которых положены методы классической и современной алгебры. Предлагается рассматривать такую систему шифрования и/или электронной подписи, при которой открытый ключ передаётся по незащищенному (открытому) каналу и в дальнейшем используется для проверки электронной подписи и для шифрования сообщения. При этом для создания электронной подписи и для расшифровки сообщения используется закрытый ключ [5].

В данной схеме шифрование использует открытый ключ, расшифровывание - закрытый. Расшифровывание без знания секретного ключа практически нереализуемо. Коммуникация по каналу связи предполагает передачу только открытого ключа. Именно этот факт устраняет необходимость передачи ключа в специальном защищенном канале

Основными видами асимметричных шифров являются:

- RSA (Rivest-Shamir-Adleman) - криптографический алгоритм с открытым ключом, основывающийся на сложности задачи факторизации больших целых чисел;
- DSA (Digital Signature Algorithm) - криптографический алгоритм с открытым ключом только для создания электронной подписи. Алгоритм основан на вычислительной сложности взятия логарифмов в конечных полях;
- Elgamal (Шифросистема Эль-Гамаля) - криптосистема с открытым ключом, основанная на вычислительной сложности дискретных логарифмов в конечном поле. Криптосистема включает в себя как алгоритм шифрования, так и алгоритм цифровой подписи;
- Diffie-Hellman (Обмен ключами Диффи — Хелмана) - криптографический протокол, позволяет нескольким (двум и более)

абонентам получить общий секретный ключ, используя незащищенный канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования;

– ECDSA (Elliptic Curve Digital Signature Algorithm) — алгоритм с открытым ключом для создания цифровой подписи и другие.

Одним из главных преимуществ асимметричных шифров является отсутствие необходимости предварительной передачи секретного ключа по защищённому каналу связи. В данном случае используется пара «закрытый ключ - открытый ключ», значения которых с одной стороны связаны, а с другой стороны вычисление закрытого ключа по открытому практически невозможно.

На практике ассиметричные криптосистемы используются в сочетании с другими алгоритмами. Связано это прежде всего с тем, что в чистом виде они требуют существенных вычислительных ресурсов.

Криптографические системы с открытым ключом широко применяются в различных стандартах цифровой подписи и сетевых протоколах. Такие криптосистемы строятся путем выбора класса задач, для которого не известен эффективный алгоритм решения (в произвольном случае) и в нем выделяется подзадача, для которой такой алгоритм существует. Далее выбранную задачу маскируют под задачу общего вида и выбирают ключ шифрования. При этом в качестве секретного ключа используется информация, позволяющая перевести выбранную задачу в исходный вид.

В нашей работе мы более подробно рассмотрим шифр Эль-Гамаля.

1.2 Классический шифр Эль-Гамаля

Криптосистема Эль-Гамаля была описана в 1985 году. Как уже говорилось, она основана на задаче дискретного логарифмирования.

Классическая схема Эль-Гамаля выглядит следующим образом [6]:

Пусть имеется конечное поле Z_p, где p – простое число, g – примитивный элемент поля Z_p. Выбираем случайное целое число x такое, что $1 < x < p - 1$.

Вычисляем $y = g^x \, mod \, p$.

Получаем открытый (p, g, y) и закрытый ключ x.

Шифрование.

Некоторое сообщение M шифруется следующим образом:

1. Выбираем случайное секретное число k при условии, что $1 < k < p - 1$

Вычисляем $a = g^k \, (mod \, p)$ и $b = y^k \, M \, (mod \, p)$.

Шифротекстом является пара чисел (a, b).

Расшифровывание.

Шифртекст (a, b) расшифровывается с использованием секретного ключа x по формуле:

$$M = b(a^x)^{-1} \bmod p.$$

При этом

$$(a^x)^{-1} \equiv g^{-kx} \pmod{p}$$

и поэтому

$$b(a^x)^{-1} \equiv (y^k M)g^{-xk} \equiv (g^{xk} M)g^{-xk} \equiv M \pmod{p}.$$

Или

$$M = b(a^x)^{-1} \bmod p = b \cdot a^{(p-1-x)} \bmod p$$

При этом не составляет труда проверить, что

$$a^x \equiv g^{kx}(mod\ p) \text{ и } \frac{b}{a^x} \equiv \frac{y^k M}{a^x} \equiv \frac{g^{xk} M}{g^{xk}} \equiv M(mod\ p)$$

Приведем пример шифрования, дешифрования с использованием классической схемы Эль-Гамаля.

Шифрование.

Пусть необходимо зашифровать сообщение *M=10*.

Произведем свободную генерацию ключей: пусть *p=13, g=3*.

Выберем случайное число *x=7* такое, что $1 < x < p$.

Вычислим $y = g^x \bmod p$.

$$y = 3^7 mod\ 13 = 3$$

Таким образом, получаем открытый ключ (13, 3, 3) и закрытый ключ $x=7$.

Следующим шагом выберем такое случайное целое число k, что $1 < k < (p - 1)$. Пусть k=6.

Вычисляем число $a = g^k \bmod p$.

$$a = 3^6 mod\ 13 = 1$$

Вычисляем число $b = y^k M \bmod p$.

$$b = 3^6 10 mod\ 13 = 10$$

Шифротекстом является пара чисел (1, 10).

Проведем расшифровывание и убедимся, что алгоритм реализован правильно, получив исходное *M*.

Вычисляем M по формуле: $M = b(a^x)^{-1} \bmod p$

$$M = 10(1^7)^{-1} mod\ 13$$

Получили исходное сообщение *M=10*.

1.3 Шифр Эль-Гамаля на эллиптической кривой

Криптографическую систему, основанную на дискретном логарифмировании, можно реализовать с использованием эллиптических кривых.

Эллиптической кривой над полем P называется гладкая кривая третьего порядка (эллиптическая кривая в узком смысле). В широком смысле под эллиптической кривой над P понимают эллиптическую кривую с уравнением третьей степени F(x,y)=0, таким, что над любым расширением поля P оно задает гладкую кривую. Известно, что в подходящей системе координат уравнение любой эллиптической кривой над конечным полем будет иметь вид

(*) $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$.

Если точка A с координатами (x_0,y_0) принадлежит кривой с уравнением (*), то противоположной точкой к A называется точка $-A=(x_0,-y_0-a_1x_0-a_3)$. Непосредственно проверяется, что $-(-A)=A$. Заметим, что точка $-A$ также будет принадлежать кривой. Если поле P не является полем характеристики 2, то уравнение кривой может быть сведено к виду

$y^2=x^3+a_2x^2+a_4x+a_6$.

Если характеристика поля не равна 2 или 3, то уравнение кривой можно привести к виду $y^2=x^3+ax+b$, который называется формой Вейерштрасса.

Пусть эллиптическая кривая задается уравнением (*). Добавим к точкам данной кривой так называемую бесконечно удаленную точку $\mathcal{O}$ и определим на полученном множестве G операцию сложения по следующим правилам:

1) $\forall A\in G$: $A+\mathcal{O}=\mathcal{O}+A=A$,

2) $\forall A\in G$: $A+(-A)=-A+A=\mathcal{O}$.

3) $\forall A, B\in G$, $A, B\neq\mathcal{O}$ и $A\neq -B$: $A+B=-C$, где точка C определяется по описанному ниже алгоритму.

Алгоритм нахождения точки C.

a) Через точки A и B проводится формальная прямая (AB), являющаяся секущей в случае $A \neq B$, и являющаяся касательной к данной кривой в случае A=B, проведенной в точке A.

b) Находятся точки пересечения прямой (AB) и рассматриваемой кривой. С учетом кратности этих точек будет в точности три: A, B и C.

Заметим, что точка C не обязательно отлична от A и B.

Относительно введенной операции сложения множество G будет абелевой группой, которую называют группой точек эллиптической кривой.

Шифрование по методу Эль-Гамаля в группе точек эллиптической кривой будет осуществляться следующим образом:

1) $G = (x_G, y_G)$ – выбранная точка $E(F)$;

2) n – простое число, являющееся порядком G в группе $E(F)$;

3) $h - |E(F)| / n$ – "кофактор" G.

Параметры (p, a, b, G, n, h) вместе как раз задают конкретную эллиптическую кривую с точки зрения криптографии.

d – случайное целое число из $\{1, 2, \ldots n-1\}$ – секретный ключ

$Q = dG$ – точка кривой – открытый ключ

Основным принципом построения таких криптосистем является замена операции $y = g^x \bmod p$ на $Y = [x]\, G \bmod p$.

При этом отличие состоит лишь в том, что в первом случае y – это число, а во втором Y – это уже точка.

Существует несколько подходов к построению криптосистем. В одном реализуется наиболее надежная стратегия, с точки зрения обеспечения стойкости, выбор случайной кривой. Другой подход ставит задачу повышения эффективности с вычислительной точки зрения путем систематического конструирования кривой с заданными свойствами. При этом возникает проблемы с защитой от взлома, т.к. специальные методы реализации подхода основываются на использовании кривых, которые фактически выбираются из относительно небольшого класса с возможным отсутствием некоторых специфических свойств.

Опишем теоретические реализации шифра Эль-Гамаля на эллиптических кривых.

Для пользователей $(U_1, U_2, \dots, U_n)$ некоторой сети выбираем общую эллиптическую кривую $E_p(a, b)$ и точку G на ней. Причем $G, [2]G, [3]G, \dots, [n]G$ являются разными точками и $[q]G = 0$ для некоторого простого числа q.

Каждый пользователь U выбирает число c_U, $0 < c_U < q$, являющееся секретным ключом, и вычисляет открытый ключ - точку на кривой $D_U = [c_U]G$. Список открытых ключей и параметры кривой передаются по открытому каналу пользователям сети.

Опишем реализацию шифрования и расшифровывания в системе Эль-Гамаля на эллиптических кривых.

Пусть сообщение представлено в виде числа $m < p$.

Алгоритм шифрования:

1) выбирает случайное число k, $0 < k < q$;

2) вычисляет $R = [k]G$, $P = [k]D_B = (x, y)$;

3) шифруем $e = mx \bmod p$;

4) (R, e)- зашифрованный текст.

Алгоритм расшифровывания:

1) По известному нам (R, e) вычисляем $Q = [c_B]R = (x, y)$ и $m' = ex^{-1} \bmod p$;

2) Получаем $m' = m$, так как

$Q = [c_B]R = [c_B]([k]G) = [k]([c_B]G) = [k]D_B = P$.

Суть реализации в том, что координата x точки Q остается секретной (число k не известно). Вычисление k считается трудно разрешимой задачей, так как для этого нужно решить проблему дискретного логарифмирования на кривой.

Рассмотренный протокол широко используется для передачи в качестве числа m секретного ключа для блочного или поточного шифра. При этом следует

выбирать параметры кривой так, чтобы $log_q r$ вдвое превышал длину ключа шифра.

Отметим, что ГОСТ Р 34.10-2012 и ГОСТ Р 34.10-2001 основаны на эллиптических кривых. Стойкость этих алгоритмов обуславливается сложностью вычисления дискретного логарифма в группе точек эллиптической кривой.

1.4 Алгоритм цифровой подписи Эль-Гамаля (EGSA)

Электронная цифровая подпись – это часть (реквизит) электронного документа, получаемый при использовании закрытого ключа подписи в результате некоторого криптографического преобразования информации [7].

Электронная цифровая подпись позволяет проверить целостность документа (отсутствие искажения информации), авторство (принадлежность подписи владельцу сертификата ключа подписи).

Одним из главных предназначений электронной подписи является определение лица, подписавшего электронный документ.

Сама технология применения системы электронных цифровых подписей подразумевает наличие нескольких абонентов, отправляющих по каналу связи друг другу подписанные электронные документы. При этом для каждого из них генерируются два типа ключей:

- секретные ключи (сохраняются у каждого абонента в тайне и используются для формирования электронной цифровой подписи);
- открытые ключи (известен всем другим пользователям, именно с помощью него происходит проверка авторства подписанного электронного документа).

Как уже говорилось ранее, знание открытого ключа не позволяет вычислить секретный ключ.

Защищенность от взлома определяется тем, что в основе генерации пары ключей (секретного и открытого) в алгоритмах электронной цифровой подписи

Эль-Гамаля лежат две сложные вычислительные задачи: задача факторизации больших целых чисел и задача дискретного логарифмирования.

Рассмотрим более подробно как реализуется создание подписи сообщения. Для того, чтобы сформировать подпись сообщения M выполняются следующие операции:

- вычисляется хеш-функция M: $m = h(M)$;
- выбирается случайное число $1 < k < p-1$ взаимно простое с $p-1$ и вычисляется $r = g^k \bmod p$;
- вычисляется число $s \equiv (m - x\,r)k^{-1} \,(\bmod p-1)$.

Таким образом пара $(r,\ s)$ является подписью сообщения M

При этом, зная открытый ключ (p, g, y) возможно проверить подпись $(r,\ s)$ сообщения M следующим образом:

- проверяем условия, что $0 < r < p$ и $0 < s < p-1$. Уже на этом этапе удается проверить подлинность подписи, т.к. в случае если хотя бы одно из условия не выполняется, можно с полной уверенностью утверждать, что подпись неверная;
- в случае выполнения предыдущего условия вычисляется хеш-функция $m = h(M)$. Причем подпись считается верной, если выполняется сравнение: $y^r\, r^s \equiv g^m \,(\bmod p)$.

Рассмотрим на конкретном примере создание подписи.

Допустим, что нужно подписать сообщение $M = baaqab$.

Произведем генерацию ключей:

- $p = 23$ $g = 5$, секретный ключ $x = 7$;
- Вычисляем открытый ключ y: $y = g^x \bmod p = 5^7 \bmod 23 = 17$. Таким образом, открытым ключом является тройка чисел $(23, 5, 17)$;
- вычисляем хэш-функцию: $h(M) = h(baaqab) = m = 3$;
- выберем случайное число $k = 5$;
- вычисляем $r = g^k \bmod p = 5^5 \bmod 23 = 20$;
- находим число $s \equiv (m - x\,r)k^{-1} \bmod(p-1) = 21$.

Получаем подписанное сообщение $< baaqab, 20, 21 >$.

Проверим подлинность полученного сообщения:

- вычислим хэш-функцию: $h(M) = h(baaqab) = m = 3$;
- проверим сравнение $y^r \ r^s \equiv g^m \ (mod\ p)$:
  - вычислим левую часть: $17^{20} \cdot 20^{21}\ mod\ 23 = 16 \cdot 15\ mod\ 23 = 10$;
  - вычислим правую часть по модулю 23: $5^3\ mod\ 23 = 10$.

Так как правая и левая части равны, то это означает, что подпись верна.

2 ЗАЩИТА АЛГОРИТМА СХЕМЫ ЭЛЬ-ГАМАЛЯ

Ранее мы уже отмечали, что в основе алгоритма электронной цифровой подписи Эль-Гамаля лежит задача дискретного логарифмирования, а некоторые ее модификации связаны с задачей факторизации. Рассмотрим каждую из этих задач более подробно, а также опишем существующие методы решения.

2.1 Задача дискретного логарифмирования

Одним из факторов криптостойкости алгоритма Эль-Гамаля является предположительно высокая вычислительная сложность обращения показательной функции. При этом сама показательная функция вычисляется довольно просто, тогда как алгоритмы вычисления дискретного логарифма имеют высокую сложность вычисления.

Опишем задачу дискретного логарифмирования.

Пусть G – это некоторая группа, a и b – её элементы. Дискретным логарифмом элемента b по основанию a называется любое целое x при котором выполняется равенство $b = a^x$. Заметим, что дискретный логарифм b по основанию a определен лишь в том случае, когда b является элементом подгруппы, порожденной a. Если a является элементом бесконечного порядка, то этот логарифм определен однозначно, а если порядок a конечен и равен m, то логарифм определен с точностью до периода, кратного m. Задача дискретного логарифмирования в группе G заключается в поиске некоторого дискретного логарифма b по основанию a.

Известны различные способы нахождения дискретного логарифма, одни из которых являются универсальными, а другие используют специфику конкретной группы. Рассмотрим некоторые из них.

Шаг младенца – шаг великана. Метод вычисления дискретного логарифма «Шаг младенца – шаг великана» стал одним из первых, который доказал, что данная задача может быть решена не только методом перебора.

Опишем метод вычисления дискретного логарифма «Шаг младенца – шаг великана» более подробно. Возьмем два числа $m, k \in Z \mid mk > p$.

Вычислим два ряда чисел:

$$a, g \quad \mathrm{a}, g^2 a, \dots, g^{m-1} a \pmod p$$

$$g^m, g^{2m}, \dots, g^{km} \pmod p.$$

Теперь найдем такие i и j, что $g^i a = g^{jm}$ и $x = jm - i$.

Вычисляем по модулю p:

$$g^x = g^{jm-i} = g^{jm}\left(g^i\right)^{-1} = g^{jm} a\left(g^i a\right)^{-1} = g^{jm} a\left(g^{im}\right)^{-1} = a.$$

Отметим, что числа i и j будут найдены, поскольку при $i = \overline{0, m-1}, j = \overline{1, k}$ выполняется $jm - i = \overline{1, km}$, причем $km > p$. То есть среди всех чисел вида $jm - i$

обязательно содержится $0 < x \leq p$.

Замечание: Указанный метод можно применять для разыскания дискретных логарифмов в любой циклической группе порядка n.

Более кратко можно описать следующие этапы решения:

Пусть g - порождающий элемент конечной группы G порядка n и $a \in G$.

Этап 1. Вычисляем $m = \left\lfloor \sqrt{p} \right\rfloor$ и $b = g^m$.

Этап 2. Вычисляем последовательности $u_i = b^i, v_j = a g^j$, где $i, j = \overline{1, m}$.

Этап 3. Найти такие i, j , что $u_i = v_j, x = (mi - j) mod\, n$

Получаем результат x

Наибольшую трудоемкость составляет поиск таких i, j , что $u_i = v_j$. Альтернативой перебору являются несколько способов:

1) Построение таблицы (i, u_i), её сортировка по второй компоненте и дальнейшее сравнение по мере нахождения компонент v_j.

2) Построение двух таблиц (i, u_i) и (j, v_j), сортировка каждой из них и поиск совпадений.

3) Объединение u, v в одну таблицу (с номерами последовательности и битом принадлежности к одной из двух последовательностей), проведение совместной сортировки.

Сложность данного алгоритма составляет O($\sqrt{n}$) умножений по модулю и O($\sqrt{n}\log n$) операций сравнения.

Рассмотрим на примере работу алгоритма.

Пусть n=229 (простое число), g=6, a=12.

Тогда m=16 и $b = g^a \bmod n = 6^{12} \bmod 229 = 183$

Выбирая первый способ поиска элементов составим таблицу 1, а затем будем вычислять компоненты v_j до тех пор, пока не найдется совпадение.

i,j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
u_i	183	55	218	48	82	121	159	14	43	83	75	214	3	91	16	196
v_j	72	203	73	209	109	196										

Получаем $i = 16, j = 6. x = mi — j \bmod n = 250 \bmod 228 = 22$

Алгоритм исчисления порядка. Другим популярным в последнее время алгоритмом вычисления дискретных логарифмов является «Алгоритм исчисления порядка».

Пусть $y = a^x \bmod p$

Число n называется p-гладким, если его можно разложить только на простые множители, меньшие либо равные p.

Этапы решения:

Этап 1. Формируем множество базовых множителей $S = \{p_1, p_2, \dots, p_t\}$, которое состоит из первых t простых чисел.

Этап 2. Находим $t + \epsilon$ (ϵ –небольшое целое число) p_t – гладких чисел $a^k \bmod p$, при $k = 1, 2, 3, \dots$, проверяя гладкость путем деления на элементы множества S. Каждое из полученных p_t – гладких чисел записываем как произведение базовых множителей в виде

$$a^k \bmod p = \prod_{i=1}^{t} p_i^{c_i},\ c_i \geq 0,$$

(для каждого значения k получаем свой набор чисел c_i)

Этап 3. В уравнении этапа 2 перейдем к логарифмам

$$k = \sum_{i=1}^{t} c_i \log_a p_i$$

для каждого p_t – гладкого числа.

Таким образом получаем систему из $t + \epsilon$ уравнений вида $k = \sum_{i=1}^{t} c_i \log_a p_i$ с t неизвестными. Неизвестными являются величины $\log_a p_i$.

Этап 4. Решаем систему методами линейной алгебры (проводя все вычисления по модулю $p - 1$) и получаем значения логарифмов чисел из множества S: $\log_a p_1, \log_a p_2, \ldots, \log_a p_t$.

Этап 5. Выбираем любое r и находим p_t – гладкое число $(y \cdot a^r)$:

$$y \cdot a^r \bmod p = \prod_{i=1}^{t} p_i^{e_i},\ e_i \geq 0.$$

Этап 6. Логарифмируя, получаем конечный результат

$$x = \log_a y = \left(\sum_{i=1}^{t} e_i \log_a p_i - r\right) \bmod (p - 1).$$

2.2 Задача факторизации больших целых чисел

Задача факторизации больших целых чисел предполагает поиск простых делителей этих чисел. Предположительно, задача является трудноразрешимой, так как при достаточно больших числах её решение требует значительных затрат времени.

В настоящее время существует множество алгоритмов решения этой задачи. Условно их можно разделить на две группы: экспоненциальные алгоритмы (перебор возможных делителей, метод факторизации Ферма, ρ-алгоритм Полларда, алгоритм Ленстры и другие) и субэкспоненциальные алгоритмы (алгоритм Диксона, факторизация методом непрерывных дробей, метод квадратичного решета и другие).

Рассмотрим по одному из алгоритмов из каждой группы: ρ-алгоритм Полларда и метод квадратичного решета.

ρ -алгоритм был предложен в 1975 году Джоном Поллардом как решение задачи факторизации целых чисел. Суть алгоритма состоит в построении числовой последовательности, элементы которой образуют цикл начиная с некоторого номера n.

Описание улучшенного алгоритма.

Пусть $F(x) = (x^2 - 1) mod\ N$, где N —число, которое необходимо факторизовать. Тогда, если $(x_j - x_i) \equiv 0(mod\ p)$, то $\left(f(x_j) - f(x_i)\right) \equiv 0(mod\ p)$.

Из этого следует, что если пара (x_i, x_j) дает решение, то решение также будет у пары (x_{i+k}, x_{j+k}).

Соответственно ограничимся только проверкой пары чисел(x_i, x_j), где $j = 2^k$, $k = \overline{1,2,3,\dots}$, $i \in [2^k + 1; 2^{k+1}]$.

Существует другая вариация ρ-алгоритм Полларда, разработанная Робертом В. Флойдом. Согласно Роберту В. Флойду значение y обновляется с каждым шагом по формуле: $y = F^2(y) = F(F(y))$и на шаге i получим $x_i = F^i(x_0), y_i = x_{2i} = F^{2i}(x_0)$.

Рассмотрим теперь субэкспоненциальный алгоритм - метод квадратичного решета, разработанный в 1981 году К. Померанцем. Алгоритм является универсальным, так как время его выполнения зависит исключительно от размера факторизуемого числа, а не от его особой структуры и свойств [8].

Опишем алгоритм.

Этап 1. Выбираем границы P и A порядка величины $e^{\sqrt{\log n \log\log n}}$(далее обозначим как *L(n)*), такие что $P < A < P^2$.

Этап 2. Для $t = \lceil\sqrt{n}\rceil + 1, \lceil\sqrt{n}\rceil + 2, \dots, \lceil\sqrt{n}\rceil + A$ по порядку выписываем в столбец целые числа $t^2 - n$.

Этап 3. Для каждого нечетного простого числа $p \leq P$ вычисляем символ Лежандра. При этом проверяем условие $\left(\frac{n}{p}\right) = 1$. Если оно не выполняется, то p удаляется из факторной базы.

Этап 4. Пусть p является таким нечетным простям числом, что n является квадратичным вычетом (по модулю p), тогда решаем уравнение $t^2 \equiv n(mod\ p^\beta)$, где $\beta = 1,2,....$ Значения β берутся в порядке возрастания пока не окажется, что уравнение не имеет решений t, сравнимых по модулю p^β с каким-либо из чисел в области $\left[\sqrt{n}\right] + 1 \leq t \leq \left[\sqrt{n}\right] + A$.

Пусть β является наибольшим из таких чисел, для которых в указанной области найдется такое число t, что $t^2 \equiv n(mod\ p^\beta)$.

Пусть t_1 и t_2 являются решениями $t^2 \equiv n(mod\ p^\beta)$ и $t_2 \equiv -t_1(mod\ p^\beta)$.

Этап 5. Результаты $t^2 - n$, полученные на этапе 2 просматриваются при том же значении p. В столбце, соответствующем p, ставится 1 против всех $t^2 - n$, для которых t отличается от t_1 на некоторое кратное p. После этого 1 заменяется на 2 для всех таких значений $t^2 - n$, что t отличается от t_1 на кратное p^2 и т. д. до β. Затем то же самое проделывается с t_2. Наибольшее возможное число в столбце - β.

Этап 6. В столбце, полученном на Этапе 5 при добавлении очередной единицы к числу, соответствующее число $t^2 - n$ делится на p и полученный результат сохраняется.

Этап 7. В столбце под $p = 2$ при $n \neq 1(mod\ 8)$ ставим 1 напротив $t^2 - n$ с нечетным t и соответствующее $t^2 - n$ делится на 2. При $n \equiv 1(mod\ 8)$ решается уравнение $t^2 = n(mod\ 2^\beta)$ и решение продолжается в том же ключе, как при нечетном p.

Этап 8. В результате для всех простых чисел, не превосходящих P, исключаем числа $t^2 - n$, кроме обратившихся в 1 после деления на все степени p, не превосходящих P. В итоге получается таблица, в которой в b_i столбце содержаться только такие значения t ($\left[\sqrt{n}\right] + 1 \leq t \leq \left[\sqrt{n}\right] + A$) что $t^2 - n$ есть B-число, а остальные столбцы будут соответствовать тем значениям $p \leq P$, для которых n — квадратичный вычет.

9. Далее используется обобщенный метод факторизации Ферма (метод факторных баз).

3 МОДИФИКАЦИИ ШИФРА ЭЛЬ-ГАМАЛЯ

Как уже говорилось ранее, в XXI веке большое распространение получили криптосистемы, основанные на задаче нахождения дискретного логарифма (схема распределения ключей Диффи – Хеллмана, схема Эль-Гамаля, цифровая подпись Шнорра и другие). В классическом описании схемы Эль-Гамаля используются мультипликативные группы конечных полей простого порядка. В связи с высокой уязвимостью данного подхода все более активно изучаются способы модификации схемы Эль-Гамаля, основанные на вычислениях в специально подобранных группах. Среди основных можно выделить группы точек эллиптических кривых и матричные группы.

3.1 Модификация алгоритма Эль-Гамаля на группе точек эллиптических кривых

В настоящее время получила широкое применение модификация алгоритма Эль-Гамаля на группе точек эллиптических кривых. Так например, ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» основан на эллиптических кривых. Его стойкость обосновывается сложностью вычисления дискретного логарифма в группе точек эллиптической кривой. Такие кратные точки эллиптической кривой являются неким аналогом степеней чисел в классической схеме Эль-Гамаля. В данном случае задача вычисления дискретного логарифма становится эквивалентна задаче вычисления кратности точки эллиптической кривой. При построении алгоритмов подписи в группе точек эллиптической кривой можно обойтись более короткими ключами по сравнению с простым полем при обеспечении большей стойкости.

Рассмотрим модификацию алгоритма Эль-Гамаля на группе точек эллиптических кривых более подробно, опишем процедуры шифрования и дешифрования сообщений [8].

Пусть $p > 3$ является простым числом. Рассмотрим некоторую эллиптическую кривую ξ над полем F_p, представленную следующим сравнением: $y^2 \equiv x^3 + ax + b(mod\ p)$, где $a, b \in F_p$ и удовлетворяют условию $4a^3 + 27b^2 \not\equiv 0(mod\ p)$.

Тогда для простого числа $q > 2$, делящего порядок группы точек эллиптической кривой ξ, выберем такую точку $P = (x_p, y_p) \in \xi$, которая порождает циклическую подгруппу $\langle P \rangle \subset \xi$ порядка q.

Рассмотрим такое целое число m, что $p < m < 2p^2$, чтобы $s \in Z_m$.

Пусть есть два отображения: $f: F_p \times F_p \to Z_m, h: F_p \times F_p \times F_p \to Z_m$.

Пусть r — натуральное число. Определим отображение mac: $F_p \times Z_m \to Z_m$. и функцию выработки ключа $kdf: F_p \times \xi \to F_p$.

Пусть целые числа *p, a, b, q, m, r*, точка $P = (x_p, y_p) \in \xi$; отображения *f, h, mac() и kdf()* известны отправителю, получателю и взломщику.

Описание задачи: абонент Б - получатель обладает следующими параметрами:

1. Знает секретный ключ d (целое число, удовлетворяющее неравенству $0 < d < q$.)
2. Знает открытый ключ Y (точка эллиптической кривой ξ, заданная парой координат (x_Y, y_Y) и определяемой равенством $Y = [d]D$.)

Абоненты А и Б обладают общим долговременным секретным ключом S (точка эллиптической кривой ξ, заданная парой координат (x_S, y_S) и выбрана таким образом, что координата x_S, чтобы величина $(ax_S + b)^2 + 4bx_S^3$ являлась квадратичным невычетом по модулю p).

Рассмотрим алгоритм шифрования.

1. Пусть $s \in Z_m$ исходное сообщение абонента А.

2. Вычисляем случайное целое число k, такое что $0 < k < q$.
3. Вычисляем точку $U = (x_U, y_U)$, эллиптической кривой ξ и находим

$$\alpha, \beta \in F_p: \begin{cases} \alpha \equiv \frac{y_U - y_S}{x_U - x_S} (mod\ p) \\ \beta \equiv \frac{x_U y_S - x_S y_U}{x_U - x_S} (mod\ p) \end{cases}$$

4. Вычисляем точку $W = [k]P$, $W = (x_W, y_W)$ и $t \equiv f(\alpha, y_U)s + h(\alpha, \beta, y_U)(mod\ p)$.
5. Определяем ключ $d_U = kdf(x_U, S)$ и вычисляем $mac(d_U, S)$.
6. Получаем сообщение $M = t \| (x_W, y_W) \| mac(d_U, S)$, являющееся шифротекстом.

Рассмотрим алгоритм расшифровывания.

1. Полученное сообщение $M = t \| (x_W, y_W) \| mac(d_U, S)$ раскладывается на три составляющих: $t \in Z_m$, $W = (x_W, y_W) \in \xi$ и $mac(d_U, S) \in Z_p$.
2. Проверяем выполнение условия $W \in \xi$.
3. Вычисляем $U = [d]W$, где $U = (x_U, y_U)$.
4. С помощью $\begin{cases} \alpha \equiv \frac{y_U - y_S}{x_U - x_S} (mod\ p) \\ \beta \equiv \frac{x_U y_S - x_S y_U}{x_U - x_S} (mod\ p) \end{cases}$ вычисляем значения α, β и s:

$$s \equiv \big(t - h(\alpha, \beta, y_U)\big) f^{-1}(\alpha, y_U)(mod\ m)$$

5. Вычисляем ключ $d_U = kdf(x_U, S)$ и $mac(d_U, s)$. Если $mac(d_U, s) \in \xi$, то сообщение правильно дешифровано.

Изложенная модификация схемы Эль-Гамаля допускает несколько различных вариантов, позволяющих изменить её функциональные особенности без изменения стойкости.

3.2 Модификация алгоритма Эль-Гамаля (с использованием RSA)

Капил Мадхур (Kapil Madhur), Джитендра Сингх Ядав (Jitendra Singh Yadav), Ашиш Виджай (Ashish Vijay) [9] предлагают новый вариант алгоритма цифровых подписей, основанный на двух недетерминированных полиномиальных задачах: разложение на простые множители и дискретное логарифмирование.

Некоторые определения, использующиеся в дальнейшем.

Определение 1 (Задача дискретного логарифмирования): Если $y = g^x \, mod \, p$, где p - простое число, а g - первообразный корень в Z_p, при известных $a, y,$ и p, тогда элемент x является дискретным логарифмом y по основанию g. Если g, x, p - большие числа, то нахождение x сводится к решению сложной арифметической задачи.

Определение 2 (Задача разложения на простые множители): При известном составном числе n, где $n = p \times q$; где p и q - простые числа, нахождение p и q - это задача разложения на простые множители, или задача факторизации.

Опишем алгоритм создания электронной подписи.

Создание ключа:

- выбираем большое простое число p такое, чтобы вычисление дискретного логарифма по модулю p было сложным и два больших простых числа p_1 и q_1 таких, что $p < n$, где $n = p_1 \times q_1$;
- выбираем случайные числа k и v такое, что $1 < k, \; v < p - 1$;
- выбираем случайное число b такое, что $1 < b < n - 1$;
- выбираем первообразный корень g в Z_p;
- вычисляем $\varphi(n) = (p_1 - 1) \times (q_1 - 1)$;
- выбираем e и x такие, что $e, x \in Z_{\varphi(n)}$;
- вычисляем d так, что $d \times e \, mod \, \varphi(n) = 1$;
- вычисляем c так, что $b^x \times c(mod)n = 1$;

– вычисляем u, w, и t по формулам: $u = g^k \bmod p$, $w = g^v \bmod p$, $t = u^w \bmod p$:

– получаем открытый ключ (e, x, c, g) and закрытый ключ (k, v, t, b, d).

Алгоритм создания подписи.

Этап 1: Выбрать целое число z такое, что $1 < z < (p - 1)$ и взаимно-простое число для $(p - 1)$ например: $gcd(z, p - 1) = 1$. z должно быть разным в каждом сообщении m и не быть открытым. H(.) – хэш-функция.

Этап 2: Вычисляем $h = g^z \bmod p$, $\gamma = t \times w^h \bmod p$, $s_1 = H(m)^d \bmod n$, $s_2 = (H(m) \times b^s 1) \bmod n$,

$s_3 = ((((H(m) - kw - hv) \times z^{-1})) \bmod (p - 1))$.

Если $\gamma = 0$ и/или $s_1 = 0$ и/или $s_2 = 0$ и/или $s_3 = 0$ и/или $H(m) \equiv (kw + hv) \bmod (p - 1)$, то $(\gamma, h, s_1, s_2, s_3)$ является подписью для m, в противном случае повторяем шаги 1 и 2.

Здесь $-kw$, $-hv$ противоположные элементы kw и hv соответственно и z^{-1} - обратная величина z по модулю $(p - 1)$.

Алгоритм проверки подписи

– вычисляем $H(m)$, полученное из сообщения m;

– если $g^{H(m)} \times s^{1 \times x} \equiv (\gamma \times h^s 3 \times s^2 \times c^s 1 \bmod n) \bmod p$,

подпись действительна, иначе – отвергнуть подпись.

Таким образом, авторам удалось совместить решение двух сложных математических задачах: разложение на простые множители и дискретное логарифмирование и создать еще одну модификацию схемы Эль-Гамаля.

3.3 Модификация алгоритма Эль-Гамаля на матричных группах

Применение матричных групп для модификации системы Эль-Гамаля обусловлено следующими соображениями:

- задача дискретного логарифмирования является трудно разрешимой в группах матриц,

- матричные группы обладают богатой подгрупповой структурой ввиду того, что любая конечная группа изоморфна некоторой подгруппе группы обратимых матриц.

Пусть $G = GL_n(q)$, где q – простое число, является матричной группой. Выберем матрицу $A \in G$ (A – большого порядка, $|A| = m$), случайное целое число α такое, что $1 < \alpha < m - 1$.

Получаем открытый ключ (q, A, A^{α}) и закрытый ключ α.

Опишем алгоритм шифрования Эль-Гамаля на матричных группах.

Имеется некоторое сообщение в виде матрицы B из $M_{n\times n}(q)$.

1. Выбираем сеансовый ключ $r_i \in F_q$ – случайное целое число.
2. Вычисляем c и b в группе G по формулам:

$$c = A^{r_i};$$

$$b = B(A^{a})^{r_i} = BA^{ar_i}.$$

3. Составляем матрицу $F_{2n\times n}$, являющуюся шифротекстом:

$$F = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ c_{31} & c_{32} & \cdots & c_{3n} \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix}$$