МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.ЧЕРНЫШЕВСКОГО»**

Кафедра компьютерной алгебры и теории чисел

Основные теоретико-числовые алгоритмы в криптографии

АВТОРЕФЕРАТ ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ

студентки 4 курса 421 группы

направление 02.03.01 — Математика и компьютерные науки

механико-математического факультета

Ивановой Ольги Владимировны

Научный руководитель
доцент, к.ф.-м.н., доцент _____ В.В. Кривобок

Зав. кафедрой
зав. каф., к.ф.-м.н., доцент _____ А.М. Водолазов

Саратов 2022

Введение. Всемирная сеть Интернет во многом изменила нашу повседневную жизнь. Новые формы коммерческой деятельности позволяют приобретать любые товары и услуги, не выходя из дома. Всемирная Паутина (World Wide Web) предоставляет возможность пользоваться общей информацией. Технология Электронной почты (e-mail) позволяет общаться друг с другом людям из самых удаленный уголков планеты. Неотъемлемой частью этого прогресса стала зависимость современного общества от Интернета.

В Интернете, как в доступной всем системе обмена данными, существует проблема информационной безопасности. Для обмена информацией необходимо соблюдение конфиденциальности, целостности и удостоверения ее подлинности. Совершая покупки в интернете посредством диалога, люди хотят быть уверены, что продавцы подлинны и средства связи обеспечивают полную конфиденциальность. Осуществляя платежные операции, пользователи должны быть убеждены, что целостность сообщения не нарушена и цифры не искажены.

Безопасность сети обеспечивается набором протоколов, которые позволяют нам спокойно использовать Интернет, не думая о возможных атаках на целостность и подлинность информации. Самый общий инструмент для обеспечения сохранности данных, — криптография. Криптография - слово греческого происхождения, которое переводится как «скрытие написанного». Сейчас этот термин используется для обозначения отрасли знаний, изучающей принципы, средства и методы преобразования данных, с целью сокрытия их информационного содержания. Хотя в прошлом криптография заключалась только в шифровании и дешифровании сообщений с применением секретных ключей, сегодня она определяется как совокупность трех различных механизмов: шифрование симметричными ключами, шифрование асимметричными ключами и хеширование.

В данной работе будет рассмотрена одна из самых распространенных асимметрично-ключевых криптографических систем: RSA (RIVERST-SHAMIR-ADLEMAN). В первой главе будут рассмотрены некоторые теоретико-числовые методы криптографии, такие как факторизация и задача дискретного логарифмирования. Затем рассмотрим киптографию с открытым ключом. Далее приступим к самой системе шифрования RSA: гене-

рация ключей, шифрование и дешифрование. Будут исследованы варианты атак RSA, например: атака разложения на множители и атака анализом времени (timing attack). Будут описаны рекомендации для шифрования. Также будет описана цифровая подпись и ее схема в RSA.

Основное содержание работы. Криптография изучает методы пересылки сообщений в замаскированном виде, при которых только намеченные отправителем получатели могут удалить маскировку и прочитать сообщение. Предназначенное для пересылки сообщение называется открытым текстом, а замаскированное сообщение - шифрованным текстом. Процесс преобразования открытого текста в шифртекст называется шифрованием, а обратная процедура называется дешифрованием. Шифрующее преобразование является функцией, которая преобразует элемент открытого текста в элемент шифртекста. Другими словами, это - отображение f из множества $\mathbb{P}$ всех возможных элементов открытого текста в множество $\mathbb{C}$ всех возможных элементов шифртекста. Будем всегда предполагать, что это отображение взаимно однозначное. Дешифрующее преобразование действует в обратном направлении, это - функция f^{-1}, восстанавливающая открытытй текст по шифртексту. Всю эту ситуацию можно изобразить следующей схемой:

$$\mathbb{P} \xrightarrow{f} \mathbb{C} \xrightarrow{f^{-1}} \mathbb{P}$$

Любая такая конструкция называется криптосистемой. Термин "криптосистема"чаще применяется к целому семейству таких преобразований, зависящих от выбора некоторых параметров.

Например, при фиксированном N-буквенном алфавите можно рассмотреть криптосистему (или "семейство криптосистем"), которая при каждом $a \in (\mathbb{Z}/N\mathbb{Z})^*$ и $b \in \mathbb{Z}/N\mathbb{Z}$ является отображением из $\mathbb{P} = \mathbb{Z}/N\mathbb{Z}$ в $\mathbb{C} = \mathbb{Z}/N\mathbb{Z}$ заданным формулой $C \equiv aP + b \ (mod \ N)$. В этом примере множества $\mathbb{P}$ и $\mathbb{C}$ фиксированны, но шифрующее преобразование f зависит от выбора параметров a и b. Поэтому, шифрующее преобразование можно задать: алгоритмом, единым для всего семейства и значениями параметров. Значения параметров называются ключом шифрования K_E. В данном примере K_E - это пара (a, b). Для дешифрования (т.е. вычисления f^{-1}) также необходимы

алгоритм и ключ. Этот ключ называется ключом дешифрования K_D. В приведенном примередешифрование производится аффинным преоьразованием $P \equiv a^{-1}C - a^{-1}b \ (mod\ N)$. т.е. алгоритм дешифрования совпадает с алгоритмом шифрования, но с другим ключом, а именно $(a^{-1}, -a^{-1}b)$. Долгое время для любой криптосхемы знание способа шифрования и знание способа дешифрования рассматривались как эквивалентные. Однако, в 1976 году Диффи и Хеллман открыли принципиально новый тип криптосистем и изобрели "криптографитю с открытым ключом".

Криптосистема с открытым ключом обладает тем свойством, что знание шифрующего преобразования не позволяет по ключу шифрования найти ключ дешифрования, избежав длинных и сложных вычислений. Другими словами, шифрующая функция $f : \mathbb{P} \to \mathbb{C}$ легко вычисляется, если ключ шифрования K_E известен, но вычислять значения обратной функции $f^{-1} : \mathbb{C} \to \mathbb{P}$ очень сложно. С точки зрения практической вычислимости это значит, что функция f необратима (без дополнительной информации - ключа дешифрования). [1]

Смысл названия "открытый ключ"состоит в том, что информация, используемая при отправке секретных сообщений - ключ шифрования K_E - может быть раскрыта без риска, что кто-либо получит возможность прочесть секретные сообщения.

Теория чисел стала широко применяется в криптографии примерно 40 лет назад. Это было вызвано необходимостью обмена большими массивами конфиденциальной информации, а также возможностью такого обмена, в связи с появлением доступных и эффективных компьютерных средств обработки этой информации.

Криптографические потребности стимулировали исследования в некоторых областях теории чисел. Стойкость криптографических алгоритмов напрямую зависит от невозможности найти быстрые алгоритмы для решения некоторых задач, другими словами, от того, что некоторые задачи теории чисел сложны в вычислительном отношении. Одной из самых важных таких задач является задача дискретного логарифмирования. [2]

---

[1]Коблиц, Н. Курс теории чисел и криптографии / Н. Коблиц М.: Научное изд-во ТВП, 2001. - 62 с.

[2]Герман, О.Н. Теоретико-числовые методы в криптографии/ О.Н. Герман, Ю.В. Нестеренко - М.: Издательский центр "Академия 2012. - 4 с.

Рассмотрим конечную группу G (с умножением в качестве групповой операции). Пусть задан элемент y, допускающий представление b^x (будем считать, что основание b задано); как найти степень элемента b, в которой он равен y? Этот вопрос называется задачей дискретного логарифмирования.

Определение 1. Пусть G - конечная абелева группа, b - элемент группы G и y - элемент группы G, являющийся степенью b. Любое целое число x, для которого $b^x = y$ называется дискретным логарифмом y по основанию b.

В простейшем и более важном случае $G = (\mathbb{Z}/n\mathbb{Z})$, где p - большое простое число, речь идет о разрешимости сравнения

$$a^x \equiv b \tag{1}$$

Если a - первообразный корень по модулю p, то сравнение (1) для b, не делящихся на p, всегда разрешимо. При этом найдется решение, удовлетворяющее неравенству $0 \leq x < p - 1$.[3]

Определение 2. Наименьшее целое неотрицательное число x, удовлетворяющее соотношению (1), называется индексом или дискретным логарифмом числа b по основанию a.

Определение 3. Под классической криптосистемой понимается криптосистема, в которой, имея информацию о преобразовании шифрования, можно реализовать преобразование дешифрования примерно за такое же время, что и преобразование шифрования.

Процедуру согласования ключей классической криптосистемы можно очень эффективно реализовать с помощью системы с открытым ключом. Первая такая детально проработанная схема, предложенная Диффи и Хеллманом, основана на задаче дискретного логарифмирования.

Алгоритм 1. Протокол выработки общего секретного ключа

1) A и B независимо друг от друга выбирают по одному натуральному числу X_A и X_B. Эти элементы они держат в секрете.

2) Каждый из них вычисляет новый элемент

$$Y_A \equiv a^{X_A} \ (mod\ p), \qquad Y_B \equiv a^{X_B} \ (mod\ p),$$

[3]Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии/ О.Н. Василенко - М.: МЦНМО, 2003. - 131 с.

причем числа p и a считаются общедоступными. Потом они обмениваются этими элементами по каналу связи.

3) А получив Y_B и зная свой секретный элемент X_A вычисляет новый элемент

$$Y_B^{X_A} = (a^{X_B})^{X_A} \mod p.$$

Аналогично поступает В:

$$Y_a^{X_B} = (a^{X_A})^{X_B} \mod p.$$

После этого у А и В появился общий элемент $a^{X_a X_B} \mod p$, который и объявляется общим ключом.

Задача А Противник знает $p,\ a,\ a^{X_A}, a^{X_B}$, но не знает X_A и X_B и хочет узнать $a^{X_A X_B}$.

По гипотезе Диффи-Хеллмана такая задача — вычислительно трудна[4].

Еще одной задачей теории чисел, требующей больших вычислительных ресурсов, является задача факторизация.

Большие простые числа могут быть построены сравнительно легко. Перемножив два из них, можно получить большое целое число, разложение которого на множители представляет практически непреодолимые трудности для тех, кто не знает исходные простые числа. На этом факте и строится одна из систем шифрования информации — RSA.[5].

RSA применяет два типа ключей — e и d, где e — открытый, а d — секретный. Предположим, что P — исходный текст и C — зашифрованный текст. В соответствии с рисунком 1 отправитель использует $C = Pe\ (mod\ n)$, чтобы создать зашифрованный текст из исходного текста ; Получатель использует $P = Cd\ (mod\ n)$, чтобы извлечь исходный текст (файл), переданный отправителем. Модулей n создается очень большое количество с помощью процесса генерации ключей.

Для шифрования и дешифрования применяют возведение в степень по модулю. Нахождение модульного логарифма так же сложно, как и разложение

[4]Шокуров, А.В Решетки, алгоритмы и современная криптография / А.В. Шокуров, Н.Н. Кузюрин, Фомин С.А. М.:[б. и.], 2008. - 125 с.

[5]Ященко, В.В. Введение в криптографию / В.В. Ященко, Н.П. Варновский, Г.А. Кабатянский, - 4-е изд., доп. М.: МЦНМО, 2012 - 91 с.

числа по модулю. Для него нет алгоритма с полиномиальным временем. Это означает, что Отправитель может зашифровать сообщение общедоступным ключом (e) в полиномиальное время. Получатель также может расшифровать его в полиномиальное время (потому что он знает d). Но Злоумышленник не может расшифровать это сообщение, потому что он должен был бы вычислить корень e-той степени из с использованием модульной арифметики.

Другими словами, Отправитель применяет одностороннюю функцию (возведение в степень по модулю) с лазейкой, известной только Получателю. Злоумышленник не знает лазейку, поэтому не может расшифровать сообщение.

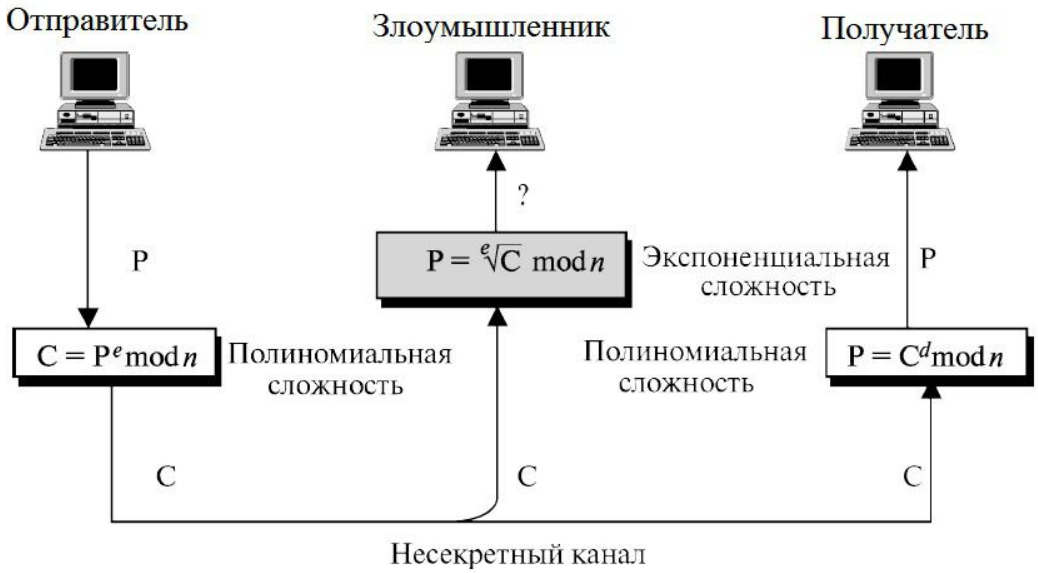

Рисунок 1 — Сложность операций в RSA

В соотвестии с рисунком 2 видно, что RSA использует возведение в степень по модулю для шифрования — дешифрования. Для того чтобы атаковать закрытый текст, Злоумышленник должен вычислить $\sqrt[e]{C}(mod\ \ n)$. RSA задействует две алгебраические структуры: кольцо и группу. Шифрование и дешифрование сделаны с использованием коммутативного кольца $R = \langle Z_n, +, \times \rangle$ с двумя арифметическими операциями: сложение и умножение. В RSA это кольцо общедоступно, потому что модуль n общедоступен. Любой может послать сообщение Получателю, применяя это кольцо для шифрования.

RSA использует мультипликативную группу $G = \langle Z^*_{\phi(n)}, \times \rangle$ для генерации ключей. Группа поддерживает только умножения и деление (мультипликативную инверсию), которые необходимы для того, чтобы создать открытые и секретные ключи. Эту группу надо скрыть, потому что ее модуль $\phi(n)$ является секретным. Видно, что если Злоумышленник найдет этот модуль, он сможет легко атаковать криптографическую систему.

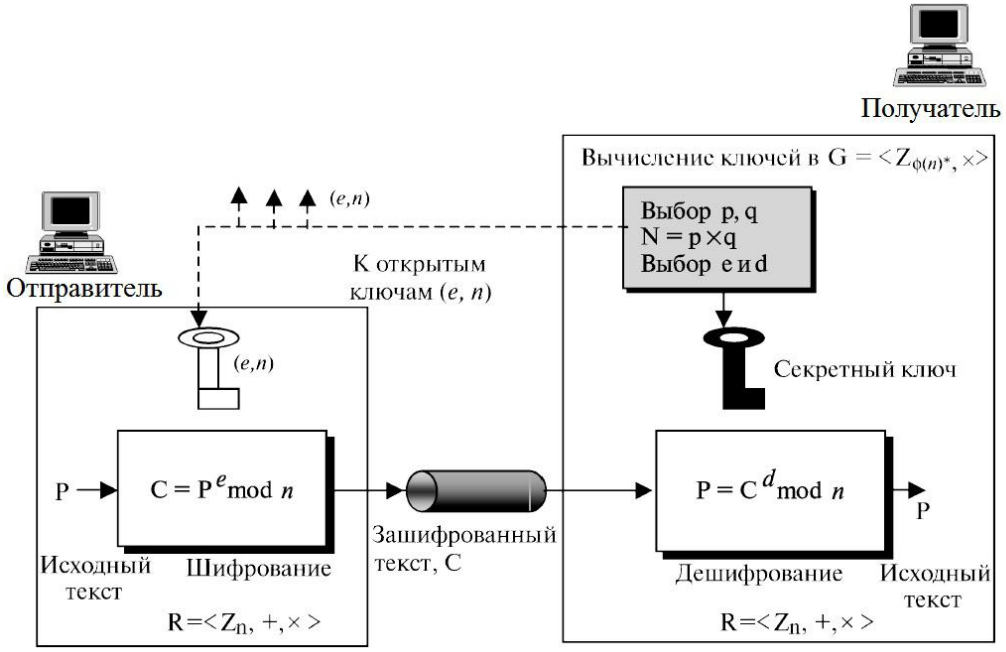

Рисунок 2 — Шифрование, дешифрование и генерация ключей в RSA

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

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).[6].

Идея RSA может также применяться для того, чтобы подписать и подтвердить сообщение. В этом случае это называется схемой цифровой подписи

[6]Ростовцев, А.Г. Теоретическая криптография / А.Г. Ростовцев, Е.Б. Маховенко - Издательство АНО НПО Профессионал, 2004. - 264 с.

RSA. В соответствии с рисуком 3 представлена схема цифровой подписи RSA.

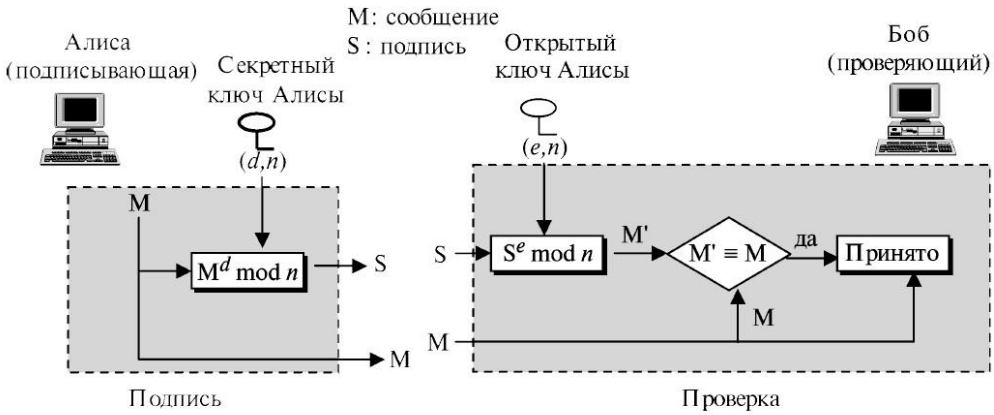

Рисунок 3 — Схема цифровой подпсии RSA

Генерация ключей в схеме цифровой подписи RSA точно такая же, как и генерация ключей в криптографической системе RSA. Отправитель выбирает два простых числа p и q и вычисляет $n = pq$ и $\phi(n) = (p-1)(q-1)$.

Затем он выбирает e для общедоступного ключа и вычисляет d для частного ключа, такое, что $ed \equiv 1(mod\ \phi(n))$. Отправитель сохраняет d и публично объявляет n и e.

Подписание. Отправитель на основе сообщения создает подпись, используя секретный ключ $S = M^d(mod\ n)$, и передает сообщение и подпись Получателю.

Проверка. Получатель получает M и S. Он применяет общедоступный ключ Алисы к подписи, чтобы создать копию сообщения $M' = S^e(mod\ n)$. Получатель сравнивает значение M' со значением M. Если два значения совпадают, он принимает сообщение. Чтобы доказать правильность этой процедуры, применим критерий проверки:

$$M' \equiv M(mod\ n) \rightarrow S^e \equiv M(mod\ n) \rightarrow M^{de} \equiv M(mod\ n)$$

Заключение. Живя в информационную эпоху, необходимо внимательно сохранять информацию о каждом аспекте жизни. Другими словами, информация — собственность, и, подобно любой другой собственности, имеет важное

значение. И в этом качестве информация должна быть защищена от нападений.

Информация должна быть защищена от неправомочного доступа (конфиденциальность), защищена от неправомочного изменения (целостность) и доступна только разрешенному объекту, когда это ему необходимо (готовность).

В течение прошлых двух десятилетий компьютерные сети произвели революцию в использовании информации. Информация теперь распределена. Люди при наличии полномочий могут передавать информацию и искать ее на расстоянии, используя компьютерные сети. Но три уже упомянутых требования — конфиденциальность, целостность и готовность — не изменились. Они лишь приобрели некоторые новые аспекты. Теперь недостаточно того, что информация должна быть конфиденциальной, когда она сохраняется в компьютере. Должен также существовать способ поддержки конфиденциальности, когда эта информация передается от одного компьютера к другому.

Все это подчеркивает актуальность данной темы в наше время. Средства и системы криптографической защиты информации играют важную роль в современных компьютерных информационных системах, используемых в сфере финансовой и коммерческой деятельности.

Криптосистема RSA используется в самых различных продуктах, на различных платформах и во многих отраслях. В настоящее время криптосистема RSA встраивается во многие коммерческие продукты, число которых постоянно увеличивается.

Итогом работы можно считать созданную функциональную модель вычисления функции Эйлера. Данная модель применима к положительным целым числам. Созданная функциональная модель и ее программная реализация могут служить органической частью решения более сложных задач.