ISSN: 2181-3906 2024

International scientifijournal
«MODERN SCIENCE AND RESEARCH»
VOLUME 3 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

ИЗУЧЕНИЕ СВОЙСТВ ПРОСТЫХ ЧИСЕЛ И ИХ РОЛИ В КРИПТОГРАФИИ.

Хидиров Бехзод
ученик 11 класса, Школы №2 города Ташкент, Янгихаятского района.
Тел: 33-262-92-95 *Mail:* *hidirovbehzod003@gmail.com*
Элмуродова Гулсум Зарифовна
научной руководитель. Учтельница по математике.
Тел: 90 805 97 87

https://doi.org/10.5281/zenodo.11193358

Аннотация. *В данной статье я разберу свойства простых чисел и их роль и важность в криптографии. А затем опишу как простые числа используются в криптографии для защиты данных и как их использование связано с проблемой факторизации.*

Ключевые слова: *Простые числа и их свойства, криптография, защита данных, применение простых чисел в криптографии.*

STUDY OF THE PROPERTIES OF PRIME NUMBERS AND THEIR ROLE IN CRYPTOGRAPHY.

Abstract. *In this article I will analyze the properties of prime numbers and their role and importance in cryptography. And then I will describe how prime numbers are used in cryptography to protect data and how their use is related to the problem of factorization.*

Keywords: Prime numbers and their properties, cryptography, data protection, use of prime numbers in cryptography.

Введение. Так ну что же, пожалуй, начнем с самого начала! Что такие простые числа и как это забытая школьная тема может быть столь полезной для защиты данных. Эта тема меня заинтриговала поэтому я делюсь им с вами! Ведь кто бы мог подумать, что школьная тема по простым числам по математике 6-го класса могла быть очень даже полезной. И то, что сейчас в наши дни большие простые числа повсеместно используются в нашей повседневной жизни, например, в кредитных картах и персональных компьютерах, поэтому постоянно существует потребность в новых простых числах (чем больше, тем лучше) для генерации секретных кодов.

В повседневной жизни нам, конечно, не интересно что число простое, натуральное, целое или сложное или еще какое-то, но роль таких чисел из разных множеств[1] очень важны хоть мы этого не замечаем вот к примеру: чтобы банально посчитать что то мы пользуемся числами из множества натуральных или целых чисел. А числа из множества рациональных чисел используются для вычислений, например, при расчете соотношении чего то к чему то. Вообще сами по себе простые числа имеют множество интересных и загадочных свойств и статей по этим темам в интернете много поэтому я разберу основные его свойства и свойства, относящиеся криптографии.

[1] Множества – это совокупность набор определенных чисел, существуют разные множества (натуральных, целых, рациональных) чисел и также есть пустое множество, где нет ни одного элемента.

Актуальность темы: Я считаю, что это тема на нынешний момент актуальна, так как сейчас эпоха информационных войн, где как никогда нужна хоть какая-то защита.

Сейчас многие хоть и не осознают этого пользуются системами защиты, основанными на простых числах. Кроме этого так же как я говорил ранее простые числа имеют интересные свойства, но многие из них остаются загадкой и их решение может привести к новым открытиям в математике в целом.

Цель исследований: выяснить основные свойства простых чисел, как они относятся к криптографии, а также их необходимость в современном мире для защиты информации от злых рук.

Задачи исследования: Конечной целью данной статьи является исследование свойств простых чисел и их роли в криптографии. Для достижения этой цели необходимо решить следующие задачи:

- Изучение основных свойств простых чисел.
- Анализ применения простых чисел в криптографии и их роли в защите данных, то как они применяются в алгоритмах шифрования и дешифрования.
- Рассмотрение современных методов генерации больших простых чисел и их применения в криптографии.
- Обзор существующих проблем и уязвимостей в использовании простых чисел в криптографии.

Гипотеза: использование больших простых чисел в криптографии обеспечивает более надежную защиту данных.

Определения простого числа и зачем они нужны в криптографии

Как вы знаете из школьной программы 6-го класса простые числа — это числа, которые делятся без остатка на 1 и на самого себя, иначе говоря, имеют только 2 делителя.

Простые числа-это одно из самых интересных математических явлений который имеет множество загадок и на некоторые из них вот как уже 2 тысячи лет нет ответа даже в наши с вами эпоху современных технологии. Математики зовут простые числа «кирпичами» в здании математики, «атомами» математики и «генетическим кодом» числа, и ведь не зря простые числа "кирпичами" в здании математики, потому что они являются основой для всех других чисел и связаны со многими другими важными концепциями.

Также их называют "атомами" математики, потому что они не могут быть разделены на более мелкие части. Кроме того, простые числа похожи на генетический код в том смысле, что они являются "базовым" элементом для всех других чисел и имеют свои уникальные свойства и характеристики, которые передаются другим числам.

Так что вот, простые числа - это как "кирпичики" или "атомы" математики, которые используются для создания больших и сложных чисел, а также для защиты информации в криптографии. Или, говоря чуть попроще любое составное (то есть число, которое имеет более 2-ух делителей) можно представить как произведение простых чисел. Это теория еще была сформулировано еще Евклидом и звучит как «основная теорема арифметики».

Теперь давайте перейдем к вопросу, зачем они нужны в криптографии. Простые числа играют очень важную роль в криптографии. Криптография — это наука о защите электронной информации от злоумышленников. Для шифрования сообщений используется алгоритм RSA, который основан на сложности факторизации[2] больших составных чисел (более подробно напишу далее в статье). В основе этого алгоритма лежит принцип умножения двух простых чисел, которые называются «ключами». Один ключ используется для шифрования сообщения, а другой для его расшифровки. Таким образом, без знания обоих ключей невозможно прочитать зашифрованное сообщение. Простые числа являются основой для создания ключей, и чем больше число, тем сложнее его факторизовать, что делает криптосистему более надежной. Вот так вкратце, зачем простые числа нужны в криптографии.

Как проверить, является ли число простым?

Еще древний математик, живший примерно 2 300 лет назад один из величайших математиков Эратосфен. Он придумал такой способ, сначала он написал все натуральные числа от 1 до какого-то n-го числа и начал вычеркивать числа начиная с 1-го (так как он не является ни простым не ни составным) затем он начал вычеркивать четные числа, потому что кроме себя и единицы они еще делятся на другие числа и наконец убрал числа, которые кратные. И так он составил таблицу простых чисел из первых 1000 натуральных чисел. Этой таблицей мы пользуемся по сей день в школах. Но этот метод слишком долгий, поэтому ученые многие года пытались найти формулу простых чисел, но нет точной формулы для генерации простого числа, но есть алгоритмы проверок.

Сейчас существует несколько способов проверки числа на простоту.

Первый способ - проверка делителей. Чтобы определить, является ли число простым, необходимо проверить, делится ли оно на какие-либо числа, кроме 1 и самого себя. Если число делится только на 1 и на само себя, то оно является простым. Например, число 7 можно проверить, разделив его по очереди на все числа от 2 до 6. Если число не делится на какое-либо из этих чисел без остатка, то оно простое.

Второй способ - тест Ферма. Тест Ферма основан на малой теореме Ферма, которая гласит, что если **p** - простое число, **а q** - любое целое число, не делящееся на p, то $\mathbf{q^{p-1} = 1}$ **(mod p)**[3]. Если это условие не выполняется, то число, скорее всего, является составным. Однако существуют исключения - числа Кармайкла[4], которые обманывают тест Ферма.

Третий способ - тест Миллера-Рабина. Это более сложный тест основан он на том же тесте Ферма на простоту числа, который также используется в криптографии. Он выглядит так пусть m это нечетное число и $\mathbf{m - 1 = 2^s t}$ где t это нечетное. Тогда для любого a из $\boldsymbol{Z_n}$[5] выполняется одно из условий :

1) $\boldsymbol{a^d \equiv 1}$ **(mod n)**

2)Существует целое число **r<s** такое что $\boldsymbol{a^{2^r d} = -1}$ **(mod n)**

Теперь вы знаете несколько способов проверки числа на простоту.

---

[2]Факторизация – это разложение числа на его составляющие, например 12 это 2*6.

[3] В математике этот символ обычно используют для обозначения того что числа делятся на m с одинаковым остатком, например: $a \equiv b$ (mod m), это означает что a и b дают одинаковый остаток при делении на m.

[4] Это составные числа, которые удовлетворяет условию формулы, хоть такие числа и редки, но их бесконечно много.

[5] Z_n это тоже множество(о них я рассказывал выше) его еще называют системой наименьших вычетов по модулю n.

ISSN: 2181-3906 2024
International scientifijournal
«MODERN SCIENCE AND RESEARCH»
VOLUME 3 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

Как использовать простые числа для создания криптографических ключей?

Создание криптографического ключа на основе простых чисел основано на теории чисел. Простые числа выбираются как основа для создания ключа, потому что они не могут быть разложены на множители, кроме единицы и самих себя. Это делает их идеальным выбором для создания безопасного ключа.

Для создания криптографического ключа на основе простых чисел мы должны сначала выбрать два различных простых числа. Затем мы перемножаем эти числа, чтобы получить большое составное число, которое служит открытым ключом. Чтобы получить закрытый ключ, мы должны найти два числа, которые при перемножении дадут нам исходные простые числа. Этот метод придумали еще в 1975 г. Уитфилду Диффи и Мартину Хеллману.

Например, если мы выберем простые числа 11 и 17, то перемножив их, мы получим число 187. Это число будет служить открытым ключом. Чтобы получить закрытый ключ, мы должны найти два числа, которые при перемножении дадут нам 11 и 17. В данном случае эти числа будут 7 и 13.

Но на данный момент он не является безопасным так как сейчас есть методы, позволявшие его легко взломать. Но существует боле сложный алгоритм шифрования.

И он называется RSA.

Алгоритм RSA — это асимметричный алгоритм шифрования, который использует два разных ключа для защиты данных. Это значит, что вы можете зашифровать сообщение, используя открытый ключ, который может быть распространен публично, но для расшифровки сообщения требуется секретный ключ, который известен только получателю сообщения.

Ключевой особенностью RSA является использование математических функций, которые сложно обратить. Алгоритм создает ключи, используя два больших простых числа, которые перемножаются между собой. Этот процесс называется генерацией ключей. Один из этих ключей используется для шифрования сообщений, а другой для их расшифровки.

Для шифрования сообщения отправитель использует открытый ключ получателя, чтобы зашифровать сообщение в виде числа, которое затем может быть отправлено по открытым каналам связи. После получения зашифрованного сообщения получатель использует свой секретный ключ для расшифровки сообщения.

Одной из главных преимуществ RSA является то, что он обеспечивает высокий уровень безопасности, так как расчеты, необходимые для обратного шифрования, являются вычислительно сложными и требуют большого количества времени и вычислительных ресурсов. Это делает алгоритм RSA идеальным для защиты информации, которую нужно хранить в безопасности.

Однако, важно отметить, что даже RSA не является абсолютно непроницаемым.

Многие атаки на RSA основаны на подборе ключа, использовании слабых ключей или простого перебора ключевого пространства. Поэтому важно использовать достаточно длинные ключи и обновлять их регулярно для обеспечения максимальной защиты данных.

И поэтому мы нуждаемся в генерации больших простых чисел.

Алгоритм RSA сейчас самый распространённый алгоритм шифрования, но также есть алгоритм Эль-Гамаля. В некотором смысле алгоритм Эль-Гамаля и алгоритм RSA похожи друг на друга, так как оба используют математические операции с большими числами для создания криптосистемы с открытым и закрытым ключами.

Однако, у них есть и существенные отличия. В алгоритме Эль-Гамаля используется операция возведения в степень, которая выполняется по модулю большого простого числа.

Это позволяет создать открытый и закрытый ключи для шифрования и расшифровки сообщений. В отличие от RSA, где закрытый ключ вычисляется как произведение двух больших простых чисел, в алгоритме Эль-Гамаля закрытый ключ является случайным числом, которое выбирается в процессе генерации ключей. Но можно их даже комбинировать эти два алгоритма и тем самым улучшить защиту своих данных.

Рассмотрение современных методов генерации больших простых чисел и их применения в криптографии.

Есть несколько способов создания больших простых чисел, например, можно проверять случайные числа на простоту с помощью алгоритма Миллера-Рабина. Ранее его метод применялся для проверки числа на простату. И другой метод — это искать простые числа в качестве делителей числа, близкого к произведению двух больших простых чисел.

Эти методы генерируют числа, которые достаточно безопасны для использования в криптографии. Чтобы создать криптографический ключ, нужно выбрать два разных простых числа, назовем их **p** и **q**. Затем перемножаем их, получаем число **n = p * q**, которое станет модулем для алгоритма RSA. Далее выбираем целое число e, которое не имеет общих делителей **c (p-1) (q-1)**, и это число становится открытым ключом. И, наконец, находим число d, которое является мультипликативным обратным к e по **(mod(p-1)(q-1))**, и это число становится закрытым ключом.

Интересны факт самое большое известное простое число на сегодняшний день имеет порядка 26 миллионов цифр и было найдено в декабре 2018 года его проверка на простоту потребовала многих лет и тысячи компьютеров, и это самое большое известное простое число на сегодняшний день. Оно называется M82589933 и является одним из множителей числа 2^82589933-1, которое также известно как число Мерсенна. И его числа играю важную роль в криптографии, но и в теории чисел. Числа Мерсенна — это числа вида $M = 2^p - 1$, где p - простое число. Они названы в честь французского монаха Марина Мерсенна, который первым исследовал их свойства еще в 17 веке. Они имеют удивительное свойство они могут быть как составные, так и простые. И если оно простое, то оно будем самым большим простым числом чем любое другое простое число.

Проблемы и уязвимости в использовании простых чисел в криптографии

Простые числа очень важны для защиты информации, но их использование имеет свои проблемы. Одна из них заключается в том, что создание больших простых чисел может быть очень трудным. Если мы используем случайный генератор чисел, то есть риск получить не простое число, а число, которое легко можно раскрыть.

Еще одна проблема связана с тем, что большие числа могут быть разложены на простые множители, и это может подорвать системы шифрования, основанные на простых числах.

ISSN:
2181-3906
2024

International scientifijournal
«MODERN SCIENCE AND RESEARCH»
VOLUME 3 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

Также существуют атаки, которые основаны на свойствах простых чисел, и они могут быть использованы для взлома некоторых систем шифрования.

А теперь давайте перейдем к возможным путям их решения.

Первым способом является использование более сложных алгоритмов генерации простых чисел, которые могут обеспечить более высокий уровень безопасности. Эти алгоритмы включают в себя, например, алгоритмы на основе эллиптических кривых[6] или квантовой криптографии.

Второй способ - использование более длинных ключей шифрования. Чем больше длина ключа, тем сложнее его взломать. Однако увеличение длины ключа может также повлечь за собой увеличение вычислительных затрат.

Наконец, третьим способом является использование комбинации разных алгоритмов шифрования. Например, можно использовать алгоритм RSA для зашифровки сообщения, а затем использовать алгоритм Эль-Гамаля для дополнительной защиты, как говорил ранее.

REFERENCES

Статьи из сайтов:

1. Простые числа и их использование в криптографии (school-science.ru)
2. https://proglib.io/p/prosto-o-slozhnom-primenenie-prostyh-chisel-v-kriptografii-2022-01-19
3. https://moluch.ru/archive/113/20400/
4. https://cyberleninka.ru/article/n/rol-prostyh-chisel-v-sovremennoy-kriptografii/viewer
5. https://habr.com/ru/companies/otus/articles/486116/
6. https://ru.wikipedia.org/wiki/Число_Кармайкла
7. Джиянмуратова Г.Ш., Гафуров О.У. Совершенствование государственной молодежной политики в Новом Узбекистане. Ijtimoiy davlat sharoitida jamiyatni faollashtirish va davlat fuqarolik xizmatini rivojlantirish imkoniyatlari. Xalqaro ilmiy-amaliy konferensiya materiallari. 2023-yil 26-may. – B. 182-185. / https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=fdboTmYAAAAJ&pagesize=80&citation_for_view=fdboTmYAAAAJ:MLfJN-KU85MC
8. https://school-science.ru/8/7/41356?ysclid=lg3yc1pezw400405369
9. https://ru.wikipedia.org/wiki/Тест_Миллера_—_Рабина
10. https://intuit.ru/studies/curriculums/3410/courses/408/lecture/9351?page=4
11. https://habr.com/ru/articles/188958/

[6] Эллиптическая кривая — это набор точек, описывающихся уравнением Вейерштрассе: $y^2 = x^3 + ax + b$. Думаю, эта тема велика и тянет на отдельную статью, поэтому ограничимся этими знаниями.