ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ
**«ШКОЛА № 1912 ИМЕНИ
БАУЫРЖАНА МОМЫШУЛЫ»
(ШКОЛА № 1912)**

Дисциплина: «Математика в Криптовалюте»
Профиль: «Физико-математический»
Учебный 2021/2022 год

Исследовательский проект на тему:
«Малая Теорема Ферма в Криптовалюте»

Выполнил:
ученик 10 «Б» класса
Барбарич Е. И.

Руководитель:
учитель математики
Досычева В. С.

Москва 2022

Содержание

Введение

Актуальность

Актуальность данной работы обусловлена огромной популярностью в мире, несмотря на то, что появилась криптовалюта относительно недавно. Этому способствуют такие факторы, как удобство оплаты товаров в интернет магазинах, высокая скорость проведения транзакций, применение современных технологий для обеспечения безопасности сделок.

Цель

Целью моей проектной работы заключается в подробном изучении роли математики в современном шифровании криптовалюты.

Задачи

1. Собрать и провести анализ материала по теме проекта.
2. Дать свое определение.
3. Дать историческую справку развития изучаемого понятия.
4. Разобрать способы шифрования криптовалюты.
5. Определить роль математики в шифровании.
6. Донести проанализированную информацию до слушателей.

Методы

1. Анализ.
2. Классификация.
3. Формализация.
4. Аналогия.

Теоретическая справка

Сравнение по модулю

Пусть a и b– целые числа, $a - b$ делится на некоторое натуральное число m, то говорят, что a сравнимо с b по модулю m. Сравнение по модулю записываются так:

$a \;\equiv\; b \; (mod\, m)$

другими словами данное сравнение можно записать так: $a - b = mk$, где k - какой-то целый множитель

Малая Теорема Ферма[1]

Данная теорема утверждает, что:

$$a^{p-1} \;\equiv\; 1 \quad (mod\, p) \tag{1}$$

где p - просто число, a - целое число, которое не делится на p.

Пример: $a = 2$ и $p = 5$, тогда $a^{p-1} = 2^{5-1} = 2^4 = 16$ и $16 - 1 = 15$, а 15 делится на 5, т.е. $2^{5-1} \;\equiv\; 1 \quad (mod\, 5)$.

Основная теорема арифметики

Данная теорема гласит, что каждое натуральное число $n > 1$ можно разложить на произведение простых числе в некой степени, математическая запись будет выглядеть так:

$$n = \prod_{k=1}^{r} p_k^{s_k} = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r}, \tag{2}$$

где r - кол-во простых делителей числа n, p_k - k-ый простой делитель, s_k - максимальная степень делителя, который входит в разложение числа n.

Функция Эйлера

Функция Эйлера - арифметическая функция, значение которой равно количеству натуральных чисел, не превышающих n и взаимно простых с ним. Для вычисления такой функции от простого числа используется формула:

$$\varphi(n) = \prod_{k=1}^{r} (p_k^{s_k} - p_k^{s_{k-1}}) = (p_1^{s_1} - p_1^{s_0}) \cdot \ldots \cdot (p_r^{s_r} - p_r^{s_{r-1}}) \tag{3}$$

[1]Пьер де Ферма - французский математик-самоучка, один из создателей аналитической геометрии, математического анализа, теории вероятностей и теории чисел.

Открытая Экспонента и Мультипликативно Обратное Число

Открытая экспонента - это целое число e, которое лежит в промежутке: $e \in (1; \varphi(n))$ и является взаимно простым с числом $\varphi(n)$, т.е. числа e и $\varphi(n)$ не имеют никаких общих делителей кроме ± 1.

Мультипликативно обратное число - число, которое при умножении на него, исходное число становится сравнимо по модулю n с единицей. Записывая это число в стандартных обозначениях модульной арифметики, мы получим вот такое сравнение:

$$ed \; \equiv \; 1 \quad (mod\, n) \tag{4}$$

где e - некое исходное число, d - мультипликативно обратное число.

Пример: $e = 3, n = 7$, тогда $3d \; \equiv \; 1 \; (mod\, 7)$, применяя базовые знания из модульной арифметики, вычисляем d:

1. Для начала вычислим $a = (e, n) = 1$[2], т.к. 3 и 7 взаимно простые числа.
2. Вторым действием проверим кратность 1 на (e, n), 1 делится на 1 $\Rightarrow$ существует единственное решение по модулю $\frac{n}{a}$, иначе решений нет.
3. Для нахождения единственного корня нам необходимо поделить все сравнение на a, тогда получим следующее: $\frac{3d}{a} \; \equiv \; \frac{1}{a} \; (mod\, \frac{7}{a})$
4. Раз получившееся сравнение целое (мы все поделили на $a = 1$), т.е. мы можем найти такое число c, что $c \cdot 3 \; \equiv \; 1 \; (mod\, 7) \Rightarrow c = 5$
5. В конечном итоге получаем, что $d \; \equiv \; c \cdot e \cdot d \; \equiv \; c \; \equiv \; 5 \; (mod\, 7) \Rightarrow d = 12$

Проверим наш пример $ed \; \equiv \; 1 \quad (mod\, n)$:

$$ed \; \equiv \; 1 \quad (mod\, n)$$
$$3 \cdot 12 \; \equiv \; 1 \quad (mod\, 7)$$
$$36 \; \equiv \; 1 \quad (mod\, 7)$$
$$36 - 1 \; \equiv \; 0 \quad (mod\, 7)$$
$$35 \; \equiv \; 0 \quad (mod\, 7)$$

35 делится на 7, значит наш способ нахождения мультипликативно обратного числа является правильным.

[2] НОД(e, n) - наибольший общий делитель.

Что такое Крипто...?

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), шифрования (кодировка данных).

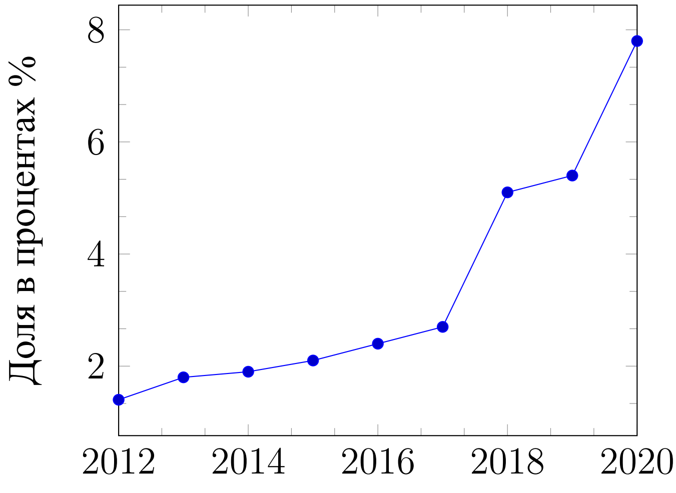
Впервые термин **криптовалюта** начал использоваться после появления платёжной системы «Биткойн», которая была разработана в 2009 году человеком или группой людей под псевдонимом Сатоси Накамото.

С развитием электронных систем возникали идеи создать электронный аналог наличных денег для удалённой оплаты. Но камнем преткновения становилась потенциальная возможность двойного расходования одних и тех же средств. При оплате наличными двойного расходования никогда не возникает из-за того, что оплата сопровождается передачей денег и покупатель не может ещё раз их заплатить другому продавцу — ведь у него этих денег уже нет. Но электронным системам органично присуща возможность копирования состояния, что позволяет сделать полные копии системы и затем произвести несколько платежей из одного и того же стартового состояния, то есть потратить одни и те же средства в разных направлениях. Проблема решалась лишь с помощью доверенных посредников, которые ведут учёт платежей и гарантируют оплаты исключительно в рамках наличия средств. Технология криптовалют изначально была нацелена на отсутствие доверенного узла — того, чьи действия гарантированно истинны и кто может подтвердить корректность чужих операций. Отсутствие у криптовалют какого-либо администратора приводит к тому, что государственные или частные органы(банки, налоговые и т.п.) не могут воздействовать на транзакции участников платёжной системы

В вышеперечисленном и кроется актуальность. Докажем это с помощью графика:

Динамика доли цифровой экономики в ВВП

(принять ВВП = 100%):



Что такое ключи?

Криптографический ключ - специальный набор данных, с помощью которого выполняется шифрование и дешифровка информации, отправляемой по сети пользователями. Такие криптоключи используются при определении кодов аутентичности и для проверки электронных цифровых подписей.

Код аутентичности сообщения (message authentication code – MAC) – это функция, которая принимает на вход два аргумента: ключ K фиксированной длины и сообщение M произвольной длины и выдает значение фиксированной длины. Для обеспечения аутентификации сообщения пользователь отсылает не только сообщение M, но и код аутентичности этого сообщения CK (M).

Аутенфикация - процедура проверки подлинности (пользователя, данных и т.п.)

Успешность дешифровки будет зависеть от используемого ключа, и, если по какой-либо причине доступ к нему будет утерян, расшифровать данные будет невозможно.

Виды ключей

1. Симметричные ключи.

   Один из самых распространенных видов шифровки, он используется в банковских платежах, онлайн-переводов и даже в самых известных мессанджерах. Берутся данные, их с помощью ключа шифруют, получатель этих данных с помощью этого же ключа их дешифрует и на этом заканчивается работа симметричного ключа. Такой способ беспечивает высокую конфиденциальность информации, но возникает сложность передачи ключа. Самым простым примером является всеми привычный замок и ключ. Представим, что вы поставили замок на дверь и раздали ключи от него свои сожителям, тогда замок - наш шифр, а ключи - криптоключи.

2. Асимметричные ключи.

   Такое шифрование основано на парах чисел. Первое — открытый ключ, С помощью которого любой может зашифровать сообщение, но для расшифровки берут второе число - закрытый ключ, который конфиденциальный. Это не могут быть два случайных ключа. Открытый и закрытый ключ всегда связаны между собой алгоритмом, который их выдаёт. Смысл в том, что внутри этого алгоритма есть третье, тоже секретное, число, которое связано с обоими ключами. Пример: у вас есть два больших простых числа, вы их перемножаете и кладете его в основу шифра, а внутри этого шифра будет ключ, который зависит от разложения чисел на множители. Если мы не знаем начального простого числа, то найти делители такого числа - задача непростая.

Система шифрования RSA

В основу своего проекта я положу систему шифрования RSA и расскажу вам о ее связи с математикой. Вспомогательным инструментом в расчетах взят язык программирования Python.

Система шифрования RSA(аббревиатура от фамилий Rivest, Shamir и Adleman) - криптографический алгоритм с открытым ключом, основываю- щийся на вычислительной сложности задачи факторизации[3] больших целых чисел.

Для того, чтобы Ярик смог послать сообщение Ване с помощью рассматриваемой системы шифрования, необходимо сгенерировать ключ, зашифровать данные и в конечном итоге дешифровать их. Предлагаю рассмотреть первый этап передачи сообщения:

Математическая часть - генерация ключа

Самым началом является генерация ключа шифровки, для этого используется определенный ряд математических действий, все необходимые знания для шифровки можно найти в теоретической справке.

1. Выберем простые числа $p = 43$ и $q = 47$
2. Найдем произведение этих чисел: $n = a \cdot b = 2021$.
3. Затем найдем Функция Эйлера для числа n по формуле 3:
   $\varphi(n) = (p - 1) \cdot (q - 1) = (43 - 1) \cdot (47 - 1) = 1932$
4. Выберем открытую экспоненту: $e = 13$
5. Вычислим мультипликативно обратное число d к числу e по модулю $\varphi(n)$: d = 1189
6. Теперь публикуем пару чисел (e, n) как открытый ключ, а пару (d, n) как закрытый ключ. Получаем, что открытый ключа - $(13, 2021)$, закрытый - $(1189, 2021)$

```
for d in range(1, 10000):  # d - мультипликативно обратное число
    k = (d * 13 - 1) / 1932  # k - интерпретация сравнения по модулю
    if k % 1 == 0:  # проверка сравнения по модулю
        print(d)
        break
```

```
1189
```

[3] Факторизация - разложение натурального числа на произведение простых множителей

Шифровка и Дешифровка

После успешной генерации ключа, Ярику необходимо зашифровать и передать данные, а Ване принять и дешифровать их. Рассмотрим для начала второй этап системы RSA - шифровка данных:

1. Берем отрытый ключ Вани - $(e, n) = (13, 1189)$
2. Выберем какой-то произвольный текст в качестве данных: $W = 111$
3. Шифруем данные с помощью открытого ключа Вани:
   $c = E(W) \Rightarrow c \equiv W^e \ (mod\, n),\ c \equiv\ 111^{13}\ (mod\, 2021)$
   $c = 1734$

```
a = 111 ** 13  # Пусть W^e = a
for c in range(1, 10000):
    if (c - a) % 2021 == 0:  # - проверка mod(n)
        print("c = ", c)
        break
```

```
c =  1734
```

После шифровки данных W, получили зашифрованные данные c. Последним этапом является дешифровка данных со стороны Вани:

1. Берем зашифрованные данные c, полученные от Ярика
2. Берем закрытый ключ - $(d,n) = (1189, 2021)$
3. Начинаем дешифровку:
   $W = D(c) \Rightarrow W \equiv c^d \ (mod\, n),\ W \equiv\ 1734^{2021}\ (mod\, 1189)$
   $W = 111$

```
b = 1734 ** 1189  # Пусть c^d = b
for w in range(1, 10000):
    if (w - b) % 2021 == 0:  # - проверка mod(n)
        print("w  = ", w)
        break
```

```
w  =  111
```

После дешифровки данных , Ваня получил исходные данные W, следовательно алгоритм шифрования RSA является рабочим и показательным для моего проекта.

Заключение

Подводя итог своего научного проекта на тему «Малая Теорема Ферма в Криптовалюте», хочу сказать, что роль математики в современной криптовалюте огромна, именно на ней строиться шифрование ключей, в которых заключается актуальность данной сферы.

Разбирая конкретный пример, мы с вами поняли, что математика входит в новые научные отрасли не на уровне арифметики и тривиальных преобразованиях, а на невероятном сложном уровне, что и говорит о величии, важности и актульности данной науки.

Список литературы

[1] *Миланов Е.* The «RSA» Algorithm

https://sites.math.washington.edu/ morrow/336_09/papers/Yevgeny.pdf

[2] *Авинаш Как* Lecture 12: Public-Key Cryptography and the «RSA» Algorithm https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf

[3] *Гущина О.А., Неешпапа Т.А.* СРАВНЕНИЯ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ. Учебно-методическое пособие