МУНИЦИПАЛЬНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА №1 с.КРАСНОУСОЛЬСКИЙ МР ГАФУРИЙСКИЙ РАЙОН РЕСПУБЛИКИ БАШКОРТОСТАН

Криптография. Азы шифрования и

практическое применение.

Выполнил ученик 4в класса

научный руководитель

учитель начальных классов

Наталенко Светлана Юрьевна

Красноусольский, 2023г.

СОДЕРЖАНИЕ

Введение............................................................................................. 3

I. Теоретическая часть

I.1 История развития шифров и криптографии...........................4

I.2 Типы шифров.............................................................................5

II. Практическая часть........................................................................9

Заключение........................................................................................11

Библиографический список.............................................................12

Приложение………………………………………………………...13

**ВВЕДЕНИЕ.**

Мы пользуемся телефоном, где есть PIN-код, электронной почтой, где есть пароль, контактом, который могут взломать. Ценную информацию следует защищать. Именно поэтому меня и заинтересовала тема «Криптография. Азы шифрования и практическое применение.»

Как только люди научились писать, у них сразу же появилось желание сделать написанное понятным не всем, а только узкому кругу. Даже в самых древних памятниках письменности учёные находят признаки намеренного искажения текстов: изменение знаков, нарушение порядка записи и т. д.

Изменение текста с целью сделать его понятным только избранным дало начало науке криптографии (греч. «тайное письмо»). Процесс изменения текста, написанного общедоступным языком, в текст, понятный только адресату, называют шифрованием.

Хотя сами методы криптографии до недавнего времени были не очень тесно связаны с математикой, во все времена многие известные математики участвовали в расшифровке важных сообщений. И часто именно они добивались заметных успехов, ведь математики в своей работе постоянно имеют дело с разнообразными и сложными задачами, а каждый шифр — это серьезная логическая задача. Постепенно роль математических методов в криптографии стала возрастать, и за последнее столетие они существенно изменили эту древнюю науку.

В наши дни информация приобрела коммерческую ценность и стала обычным товаром. Её продают и покупают, производят, хранят, транспортируют и, следовательно, воруют и подделывают. Поэтому **актуальность** нашей работы очевидна - необходимость защиты важной информации (вспомним крылатую фразу: *«Кто владеет информацией, тот владеет миром».*)

Мы выдвинули **гипотезу**о том, что шифрование информации интересно и доступно нам, ученикам начальной школы

**Цель работы**: Исследование истории криптографии, её основ и способов применения шифров в деятельности человека.

**Задачи проекта**:

1. Изучить историю развития криптографии.
2. Исследовать некоторые типы шифров, их описание и ключи.
3. Попрактиковаться в шифровании
4. Популяризировать знания о криптографии среди одноклассников.
5. Выяснить, какие шифры удобнее использовать на практике

**I. 1.** **ИСТОРИЯ РАЗВИТИЯ ШИФРОВ И КРИПТОГРАФИИ.**

История криптографии - ровесница истории человеческого языка. Священные книги древнего Египта, древней Индии тому примеры. Искусство шифрования и тайной передачи информации было присуще практически всем государствам и в прошлом использовалось, прежде всего, в военных целях. Но есть и другие примеры использования шифров: один из сохранившихся шифрованных текстов Месопотамии представляют собой табличку, написанную клинописью и содержащую рецепт изготовления глазури для гончарных изделий. В рукописях Древнего Египта шифровались религиозные тексты и медицинские рецепты. Шифрование использовалось в Библии. Итак, первый период криптографии (с III тыс. до н.э.): господство моноалфавитных шифров. Основной принцип этого шифра – принцип замены. Ярким примером является шифр Цезаря, о котором будет сказано ниже в данной работе

Второй период (XV - XX в.) ознаменовался введением полиалфавитных шифров - применение нескольких моноалфавитных шифров. Значительный шаг вперёд криптография сделала благодаря труду Леона Альберти. Известный философ, живописец, архитектор, в 1466 году написал труд о шифрах. В этой работе был предложен шифр, основанный на использовании шифровального диска. Сам Альберти называл его шифром, «достойным королей».

Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков.

Четвертый период с середины XX века до 70-х годов XX века – период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных. Обязательным этапом создания шифра считается изучение его уязвимости к различным атакам.

Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается новыми техническими возможностями, широким распространением криптографии для использования частными лицами. Современная криптография образует отдельное научное направление на стыке математики и информатики. Практическое применение криптографии стало неотъемлемой частью жизни современного общества – её используют в таких отраслях как электронная коммерция, электронный документооборот, телекоммуникации и других.

В своей работе мы рассмотрим наиболее популярные моноалфавитные шифры.

**I. 2. ТИПЫ ШИФРОВ.**

До наших дней дошли знаменитые шифры замены, шифры перестановки или их сочетания, например, шифр «Сцитала», шифр Цезаря, «тарабарская грамота» и решетка Кардано.

*1. Шифр «Сцитала».* Одним из самых первых шифровальных приспособлений был жезл («Сцитала»), применявшийся ещё во времена войны Спарты против Афин в V веке до н.э. Сообщение было написано на поясе официального гонца следующим образом: на цилиндр виток к витку наматывали пояс (без просветов и нахлёстов), а затем на этом поясе вдоль его оси записывали необходимый для передачи текст; потом пояс разматывали, и получалось, что поперёк пояса в беспорядке написаны буквы. Чтобы расшифровать полученную информацию, Лисандр взял сциталь такого же диаметра, аккуратно намотал на него пояс и вдоль сциталя прочитал сообщение от своего агента. Такой способ шифрования осуществляет перестановку местами букв сообщения.

*2. Шифр Цезаря и совершенный квадрат Цезаря*. Великий римский полководец Юлий Цезарь (99-44 гг до н. э) придумал примитивный способ шифровки своих указаний. Он преобразовывал послания таким образом, чтобы текст выглядел бессмыслицей. Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите, чаще всего со сдвигом вправо на 3.

Например: **Меня зовут Никита**. - открытое письмо.

**Пзрв ксецх Рлнлхг**. - зашифрованное письмо.

Совершенный квадрат Цезаря использовался, когда послание состояло из числа букв, равного полному квадрату – шестнадцати, двадцати пяти, тридцати шести – в зависимости от того, какой объём информации нужно было передать. Цезарь тайно объяснил офицерам, что по получении этого якобы случайного набора букв, они должны записать текст таким образом, чтобы он составил квадрат, Тогда при прочтении сверху вниз, перед глазами появлялось тайное послание.

Например, высказывание «Математика – царица всех наук» при данной шифровке пройдёт следующие этапы преобразования: буквы располагаем в столбцы квадрата 5×5 одну за другой без знаков препинания; переписываем столбцы в строку:

**М А Ц А Н**

**А Т А В А**

**Т И Р С У**

**Е К И Е К**

**М А Ц Х**

**МАЦАНАТАВАТИРСУЕКИЕКМАЦХ.**

*3. «Тарабарская грамота».* Русские дипломаты XV – XVI в., стремившиеся сохранить тайну переписки, применяли «тарабарскую грамоту», в которой все гласные буквы оставались неизменными, а согласные менялись друг на друга по следующей схеме:

**Б В Г Д Ж З К Л М Н**

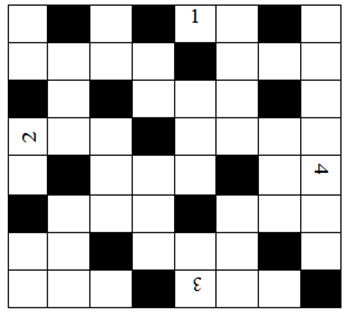
**│ │ │ │ │ │ │ │ │ │**

**Щ Ш Ч Ц Х Ф Т С Р П**

Например, вместо «Великий государь» получалось «Шеситий чолуцамь»

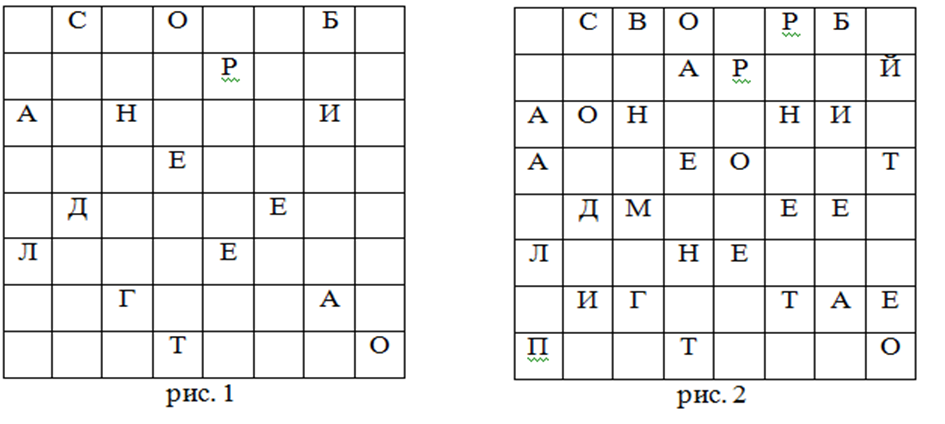
*4. Решётка Кардано.*

Революционеры-подпольщики вынуждены были вести свои записи и переписку таким образом, чтобы никто из посторонних не мог понять написанного. Для этого пользовались особым способом тайнописи – «решёткой». Желающие вести тайную переписку по этому способу запасаются каждый «решёткой» - бумажным квадратиком с прорезанными в нём окошечками. Окошечки размещены не произвольно, а в определённом порядке.



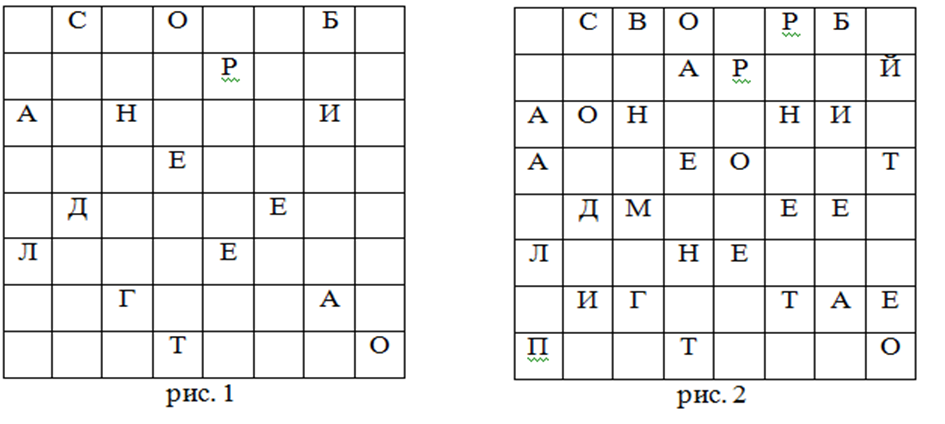
Пусть вам требуется послать товарищу такую записку: Собрание делегатов района отмените. Полиция кем-то предупреждена. Антон.

Наложив решётку на листок бумаги, подпольщик пишет сообщение (букву за буквой) в окошечках решётки. Так как окошечек 16, то сначала помещается только часть записки: Собрание делегато… Сняв решётку мы увидим запись, представленную на рис.1.

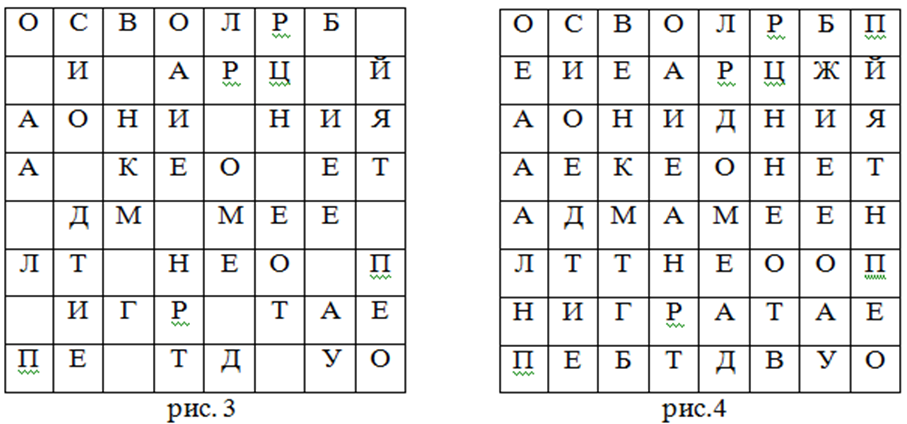


Далее подпольщик поворачивает решётку «по часовой стрелке» на четверть оборота, т.е. располагает её на том же листе так, чтобы цифра 2, бывшая ранее сбоку, теперь оказывается вверху. При новом положении решётки все ранее написанные буквы заслонены, а в окошечках появляется чистая бумага.

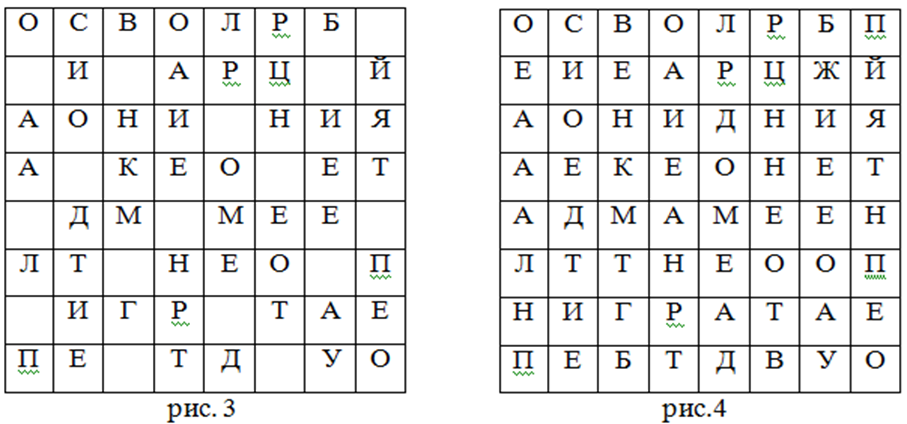
В них пишут следующие 16 букв секретного сообщения. Если теперь брать решётку, то получим запись на рис. 2.



Сделав следующий поворот решётки на четверть оборота по часовой стрелке, получим открытые новые 16 свободных клеток. В них найдут себе место ещё несколько слов, и записка приобретёт вид рис. 3.



Наконец, делается последний поворот решётки, цифрой 4 вверх, и в открывшиеся 16 чистых квадратиков вписывают окончание записки. Так как остаются три неиспользованные клетки, то их заполняют буквами А, Б, В – просто для того, чтобы в записке не осталось пробелов. Письмо имеет вид, представленный на рис. 4.



Попробуйте в нём что-нибудь разобрать! Пусть записка попадёт в руки полиции, пусть полицейские сколько угодно подозревают, что в ней скрыто важное сообщение, но догадаться о содержании записки может только адресат, имеющий в руках такую же решётку, как и та, которой пользовался отправитель.

**II. ПРАКТИЧЕСКАЯ ЧАСТЬ**

Мы решили рассказать одноклассникам о нескольких способах шифровки информации, дать им ключи к расшифровке и определить за какое время будет прочитана информация одного и того же объёма(13 слов). Моих одноклассников мы поделили на 5 команд по 4-5 человек.





Результаты практической части показали:  
*I задание "Шифр Цезаря":*                            
1команда-02.06сек.  
2команда-03.32сек  
3команда-05.42сек  
4команда-07.10сек  
5команда-07.02сек  
Среднее время:05.14сек  
  
*II задание "Тарабарская Азбука"*  
1команда-00.41сек  
2команда-00.49сек  
3команда-01.04сек  
4команда-01.41сек  
5команда-1.11сек  
Среднее время:1.52сек

*III задание «Решётка Кардано»*

1команда-01.28сек  
2команда-01.40сек  
3команда-05.07сек  
4команда-03.27сек  
5команда-02.41сек  
Среднее время:2.53сек  
  
  
*IV задание "Совершенный квадрат"*1команда-03.21сек  
2команда-01.38сек  
3команда-00.31сек  
4команда-00.40сек  
5команда-02.01сек  
Среднее время:1.38сек

Делаем выводы: для моих одноклассников проще всего оказался шифр «Тарабарская грамота», а труднее - "Шифр Цезаря". Значит, если мы будем использовать криптографию, то в зависимости от цели, можно пользоваться тем или иным шифром: если у нас много времени и мы хотим, чтобы наше послание было сложнее расшифровать, то надо пользоваться "Шифром Цезаря" и, соответственно, наоборот.

**III. ЗАКЛЮЧЕНИЕ.**

Криптография – это очень интересная и актуальная тема. Шифры использовались, используются и будут использоваться, т.к. они необходимы во многих областях и помогают людям решить те или иные логические задачи. Шифрование постоянно открывается обществу, т.к. были созданы системы, которые прогрессивнее предыдущих и позволяют разрешать серьезные задачи. Всегда существовала совершенно секретная информация, которая могла бы привести к необратимым последствиям, будь она обнародована. Нами было рассмотрено несколько примеров тайнописи, которые близко соприкасаясь с математикой, лишний раз доказывают, как разнообразны стороны «жизни» этой науки. Гипотеза, поставленная в работе, подтверждена. Цель достигнута, задачи – выполнены. Научная работа проводилась на основе рекомендованной руководителем литературы, а также интернет ресурсов.

Научиться применять криптографию в современных условиях для решения жизненных проблем не просто, но можно. Мы считаем, что каждый человек, который пользуется компьютером, должен задумываться о том, что его информация может быть взломана и использована в корыстных целях (от рассылки спама с вашей электронной почты до скачивания паролей вашей банковской карты или другой важной информации). В таком случае, проблема защиты информации в настоящее время всё более и более возрастает в связи с развитием информационных технологий.

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. Я. И. Перельман. Живая математика, М. «Наука».1978
2. Г. Фролов. Тайна тайнописи. М. 1992.
3. Т. А. Соболева. Тайнопись в истории России. М.2014
4. Словарь криптографических терминов / Под редакцией Б.А. Погорелова и В.Н. Сачкова. – М: МЦНМО, 2006.
5. Гатчин Ю.А., Коробейников А.Г. «Основы криптографических алгоритмов». Учебное пособие. Санкт-Петербургский государственный университет информационных технологий, механики и оптики 2002 год.
6. Зубов А.Ю. «Совершенные шифры». Гелиос АРВ 2003 год.
7. Интернет-ресурсы:

Шифр Цезаря — Википедия ru.wikipedia.org/wiki/Шифр\_Цезаря

[http://www.proza.ru/2009/07/26/707 Способы](http://www.proza.ru/2009/07/26/707%20Способы) шифрования. Тайнопись   
<http://www.stihi.ru/2011/02/11/9618>   
<http://www.opennet.ru/docs/RUS/inet_book/6/crypt_64.html>   
<http://www.compress.ru/article.aspx?id=10135&iid=420>   
<http://www.agentura.ru/equipment/ukarchivs/>   
<http://www.hrono.ru/statii/2008/shifr5.html>   
<http://www.phantomgallery.64g.ru/shiphry/cod2.htm>   
<http://www.phantomgallery.64g.ru/cod.htm>   
<http://www.agentura.ru/equipment/krypto/ideas19/>   
<http://bookap.info/okolopsy/ronin/gl27.shtm>

**ПРИЛОЖЕНИЕ**

*Мы выполняем I задание "Шифр Цезаря":*



*Мы выполняем II задание "Тарабарская Азбука"*



*Мы выполняем III задание «Решётка Кардано»*

**

*Мы выполняем IV задание "Совершенный квадрат"*

****