

**МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ
«СРЕДНЯЯ ШКОЛА № 102
С УГЛУБЛЕННЫМ ИЗУЧЕНИЕМ ОТДЕЛЬНЫХ ПРЕДМЕТОВ»**

Шифрование информации

Выполнил:
Новоселов Тимофей Андреевич, 6 «а» класс

Руководитель:
Гражданинова Елена Владимировна
учитель математики
МАОУ СШ № 102

г. Нижний Новгород
2024 год

Содержание

Введение.....	3
Основные понятия.....	4
Заглянем в историю	5
Шифр Цезаря	7
Шифр Виженера	8
Решётка Кардано	11
Практическая часть	13
Шифрование с помощью метода “Решетка Кардано”	13
Заключение	17
Список используемых источников и литературы.....	18

Введение

Информация окружает человека повсюду с самого рождения. Ещё в древности люди задумались о том, как сохранить важную для них информацию от посторонних лиц. Различные способы тайной переписки (криптографии) существовали и в Древнем Египте, и в Древней Греции и Риме, и в средневековой Европе, и в Древней Руси. Тайными посланиями обменивались короли и дипломаты, военачальники и купцы. Нередко от того, будет ли прочитано неприятелем секретное сообщение, зависела судьба целой страны.

А в наше время защита данных особенно важна, так как с развитием цифровых технологий информация стала самым ценным ресурсом. Когда мы совершаем банковские переводы, пользуемся электронными услугами, вводим свои личные данные в различные мобильные приложения, ведем переписку в мессенджерах, мы хотим быть уверенными, что наши данные не попадут в руки злоумышленников. Поэтому защита информации различными методами и алгоритмами шифрования так актуальна сегодня.

И чем больше цифровые технологии проникают в повседневную жизнь, тем важнее каждому человеку понимать, как это работает, поэтому я выбрал данную тему.

Целью работы является начальное знакомство с самим понятием шифрования и некоторыми методами шифрования и дешифрования текстовой информации.

Задачи работы:

- Разобраться с основными понятиями
- Изучить информацию о следующих способах шифрования “Шифр Цезаря”, “Шифр Виженера”, “Решетка Кардано”.
- Научиться шифровать и дешифровать текст с помощью изученных методов.

Основные понятия

Рассмотрим основные понятия.

Шифрование – это преобразование открытой информации в зашифрованную, недоступную для понимания посторонних лиц.

Для процесса шифрования используется *шифр* (от фр. chiffre «цифра» от араб. sifr «ноль») - это сам алгоритм (метод) преобразования данных с использованием ключа для обеспечения секретности передаваемой информации.

Ключ шифрования – это тайная информация (например, набор цифр или букв), которая используется алгоритмом для шифрования и расшифровки сообщения.

Задача шифрования — превратить данные, которые могут прочитать все, в данные, которые может прочитать только тот, у кого есть специальное знание (алгоритм и ключ).

Дешифрование - обратный шифрованию процесс, зашифрованный текст преобразуется в исходный с использованием секретного ключа.

Криптографическая стойкость шифра – это свойство шифра противостоять взлому.



Рис.1 Схема преобразований текста

Криптология (kryptós - “скрытый” и lógos “слово”) – наука, исследующая криптографические преобразования информации

Криптология разделяется на два направления – *криптографию* и *криптоанализ*. Цели этих направлений прямо противоположны.



Рис.2 Схема преобразований текста

Само слово «криптография» происходит от древнегреческого *κρυπτός*, что означает «скрытый», и *γράφω*, что означает «пишу». То есть дословно слово «криптография» означает «тайнопись». Учитывая, что слово «шифр» произошло от слова «цифра», эта тайнопись использует математические методы при преобразовании и шифровании информации.

Заглянем в историю

Первые шифры появились ещё в Древнем мире — в Индии, Месопотамии и в Египте.

Предположительно самый древний криптографический текст был найден в гробнице древнеегипетского чиновника Хнумхотепа II, который жил около четырёх тысяч лет назад.

В этом тексте были использованы необычные иероглифы, которые скрывали истинное значение текста. По сути, был использован шифр подстановки, когда буквы, слова или иероглифы заменяются другими по определённым правилам.

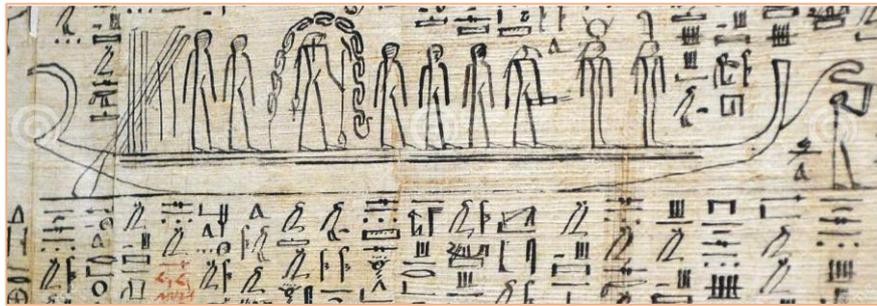


Рис.3 Древний криптографический текст

Криптография Древней Греции известна несколькими изобретениями. Например, в 500 году до нашей эры спартанцы придумали устройство, которое назвали *скитала*. Оно представляло из себя цилиндр, вокруг которого была намотана по спирали полоска пергамента. На этом пергаменте писалось письмо. А потом разворачивалось и становилось нечитаемым. Чтобы его прочесть, требовалась скитала точно такого же размера. Использовали устройство для отправки секретных посланий.



Рис.4 Скитала

Системный подход к шифрованию посланий появился только в Древнем Риме, где криптографию впервые начали использовать в военных целях. Император Юлий Цезарь изобрел шифр, который можно было использовать многократно, даже если неприятель умудрялся разгадать одно из посланий. Шифр Цезаря мы подробно рассмотрим далее.

Возникнув в Древнем мире, криптография использовалась и в Средние века, и в эпоху Возрождения. Криптографией увлекались различные известные деятели и учёные, такие как Пифагор, Платон, Паскаль, Галилей, Леонардо да Винчи, Ньютон, Бэкон и другие.

Однако как самостоятельная наука криптография сформировалась только в конце XIX века. Когда научно-технический прогресс набрал обороты, появились государственные шифры, а скорость шифрования вышла на новый уровень. После появления радиосвязи криптографию стали активно использовать в разведке. Появились специалисты, которые занимались исключительно шифрованием и дешифровкой.

После того, как криптография прошла «боевое крещение» в двух войнах начала XX века, её начали использовать и в гражданских мирных целях — для сохранения конфиденциальности при пересылке данных.

Теперь перейдем к более подробному рассмотрению некоторых шифров.

Шифр Цезаря

Одним из первых документально зафиксированных шифров является шифр Цезаря (около 100 г. до н.э.). Это моноалфавитный шифр. Его принцип был очень прост: каждая буква исходного текста заменялась на другую, отстоящую от нее по алфавиту на определенное число позиций. Этот сдвиг и является ключом.

Более сложной версией шифра Цезаря является шифрование с ключевым словом: текст делится на произвольное количество частей, и сдвиг для каждой части задаётся одной из букв ключевого слова. То есть, если ключевое слово «ключ», то в первой части текста сдвиг будет такой, что буква «а» открытого текста будет буквой «к» зашифрованного текста, во 2 части текста – буквой «л» и так далее.

Зашифруем крылатое выражение «Перейти Рубикон» при помощи простого шифра Цезаря со сдвигом на 5 вправо.

Если сдвиг (он же ключ) равен 5, это значит, что каждая буква открытого текста будет заменяться на другую, которая находится на 5 букв дальше в алфавите, например А заменится на Е.

Для удобства составим таблицу: первую строку заполним буквами русского алфавита, а строку ниже заполним со сдвигом влево так, чтобы букве А

исходного алфавита соответствовала буква Е.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
	↓				↓				↓	↓	↓				↓	↓	↓	↓		↓	↓			
Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь

Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Э	Ю	Я	А	Б	В	Г	Д

Теперь находим в первой строке буквы шифруемой фразы и заменяем их на буквы, которые расположены под ними.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Сообщение	П	Е	Р	Е	Й	Т	И	Р	У	Б	И	К	О	Н
Шифр	Ф	Й	Х	Й	О	Ч	Н	Х	Ш	Ё	Н	П	У	Т

Получаем закодированную фразу: ФЙХЙОЧНХШЁНПУТ

Для расшифровки требуется выполнить обратную операцию: ищем буквы из зашифрованного текста во второй строке и заменяем их на буквы, расположенные над ними.

Шифр Виженера

Шифр Виженера - это классический метод шифрования, который был разработан в 16 веке французским дипломатом и криптографом Блезом де Виженером на основе многоалфавитного шифра Альберти. Шифр Виженера благодаря устойчивому алгоритму долгое время считался невозможным для взлома.

Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Чтобы лучше разобраться, о чем идет речь, рассмотрим таблицу Виженера (квадрат Виженера) для русского

языка. Применительно к русскому алфавиту квадрат Виженера составляется из строк по 33 символа, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 33 различных шифра Цезаря.

Рассмотрим работу шифра на примере фразы «шифр Виженера». Для шифрования нужно выбрать ключевое слово — пусть им будет слово «пароль». Теперь начнем шифрование. Для этого запишем ключ столько раз, чтобы количество букв из него соответствовало количеству букв в шифруемой фразе, путем повтора ключа(лишние буквы обрезаются):

	1	2	3	4	5	6	7	8	9	10	11	12
Сообщение	Ш	И	Ф	Р	В	И	Ж	Е	Н	Е	Р	А
Ключ	П	А	Р	О	Л	Ь	П	А	Р	О	Л	Ь

Буквы исходного текста

	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

Рис.5 Квадрат Виженера

Теперь по таблице Виженера ищем ячейку, которая является пересечением пар букв, и получаем: Ш + П = И, И + А = Ё, Ф + Р = Е и т. д.

Получаем зашифрованный текст:

	1	2	3	4	5	6	7	8	9	10	11	12
Шифр	И	Ё	Е	Я	О	Е	Ц	Ж	Ю	Ф	Ь	Э

Для дешифрования составим таблицу:

	1	2	3	4	5	6	7	8	9	10	11	12
Шифр	И	Ё	Е	Я	О	Е	Ц	Ж	Ю	Ф	Ь	Э
Ключ	П	А	Р	О	Л	Ь	П	А	Р	О	Л	Ь

Мы находим строку, соответствующую первой букве ключа и ищем в ней букву, соответствующую первой букве шифрованного текста: название столбца, где находится эта буква и будет первой буквой дешифрованного сообщения, в нашем случае это буква “ш”. То же самое мы сделаем со вторыми буквами шифрованного текста и ключа, потом с третьими буквами и т.д. В результате мы снова получим открытый текст сообщения.

Данный шифр на порядок более устойчив к взлому, чем моноалфавитные, хотя представляет собой шифр простой замены текста.

Взломать шифр Виженера так сложно, потому что для взлома необходимо знать длину ключевого слова. Поэтому взлом заключается в том, чтобы наугад бросать длину ключевого слова и пытаться взломать засекреченное послание. Следует также упомянуть, что помимо абсолютно случайного ключа может быть использована совершенно разная таблица Виженера. В данном случае квадрат Виженера состоит из построочно записанного русского алфавита со смещением на единицу. И точно так же, как и в шифре Цезаря, смещение может быть любым. Более того, порядок букв не обязательно должен быть алфавитным. В данном случае сама таблица может быть ключом, не зная которую невозможно будет прочесть сообщение, даже зная ключ.

На основе шифра Виженера позже был разработан шифр Вернама, который обладает абсолютной криптографической стойкостью, то есть его невозможно взломать.

Решётка Кардано

В 1556 году увлечение теорией магических квадратов привело математика и философа Джероламо Кардано к открытию нового класса шифра перестановок, названного решёткой или трафаретом.

Решетка Кардано может быть двух видов — простая и симметрично-поворотная.

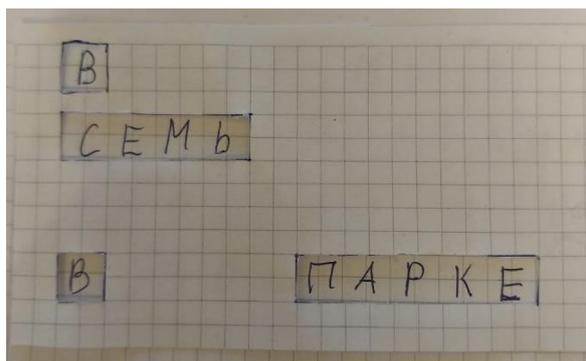
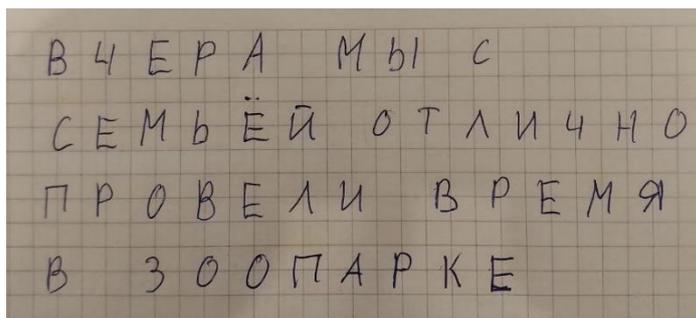
В первом случае для шифрования применяется трафарет с отверстиями, через которые "фильтруется" полезный текст.

Шифрующий помещает решётку на лист бумаги и пишет сообщение в прямоугольных вырезах, в которых помещается отдельный символ, или целое слово. Затем решётка убирается и пустые места на бумаге заполняются посторонним текстом так, чтобы скрываемый текст стал частью письма. Такое заполнение требует литературного таланта.

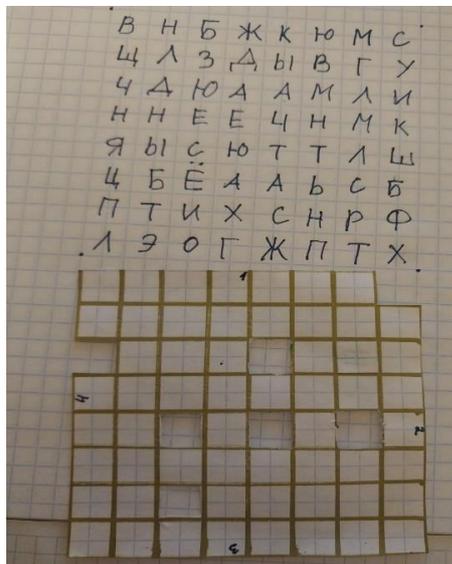
Этим методом пользовался великий русский поэт А.С. Грибоедов. Под видом обычных писем он посылал секретные дипломатические сообщения из Персии, где служил русским послом.

Ключ-решетка одинаково вида должна быть у отправителя и получателя сообщения.

Например, напишем сообщение “Вчера мы с семьей отлично провели время в зоопарке”. После наложения простой решётки видим текст: “В семь в парке”.



Другой вариант решетки симметрично-поворотная, более интересный, он состоит в том, чтобы использовать симметричный (квадратный) трафарет, который можно применять несколько раз, просто поворачивая его вокруг центра. В результате получается заполненный буквами квадрат. Пустые места заполняются случайными буквами



При подобном методе использования шифр является очень стойким.

Количество подобных решёток быстро растёт с их размером. Так, решётка 2x2 единственная, решёток 4x4 уже 256, а решёток 6x6 свыше 100 тысяч.

Обычно использовали квадраты 8x8, по 16 отверстий, то есть вписать текст можно было из 64 букв. Если послание короче 64 букв, оставшиеся места можно было заполнить случайными буквами (символами). Если же послание длиннее, то решетку можно использовать второй раз, создавая рядом еще один квадрат с буквами.

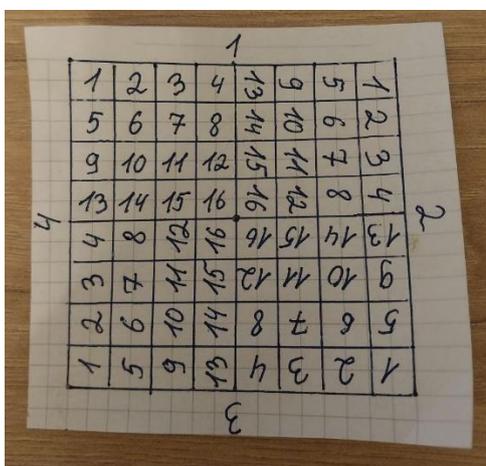
Практическая часть

Шифрование с помощью метода “Решетка Кардано”

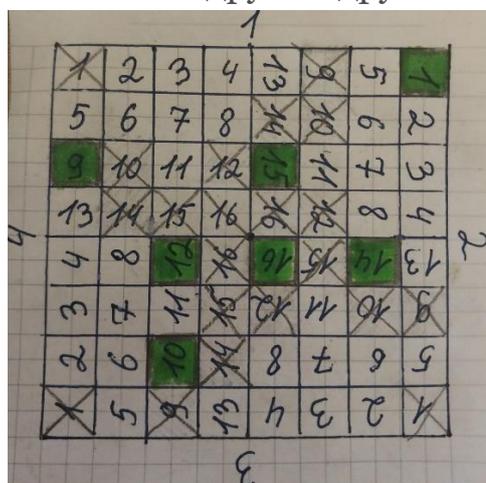
Сначала мы должны разработать свою решетку, которая является ключом. Пусть она будет размером 8x8.

Вспользуемся следующим алгоритмом:

1. Разделить квадрат 8×8 на четыре квадрата размером 4×4
2. Пронумеровать клетки внутри каждого малого квадрата от 1 до 16 (с учетом поворота на 90 градусов против часовой стрелки)
3. Для удобства пронумеровать стороны

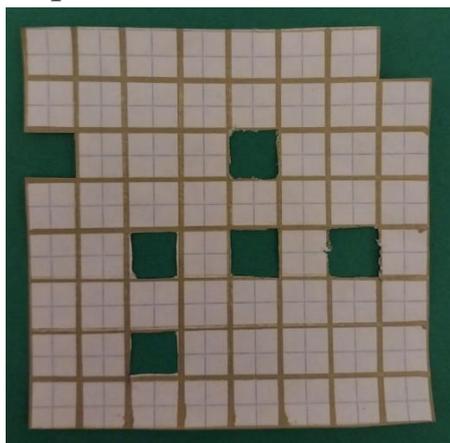


4. В левом верхнем квадрате выбрать ячейку/ячейки для вырезания
5. Зачеркнуть ячейки с этими номерами в остальных мини-квадратах, их нельзя будет использовать, чтобы при повороте текст в окнах не наложился друг на друга



6. Выбрать ячейки для вырезания в следующем квадрате, зачеркнуть ячейки с этими номерами в остальных мини-квадратах

7. Повторить для оставшихся двух квадратов
8. Вырезать окошки в ячейках, отмеченных для вырезания

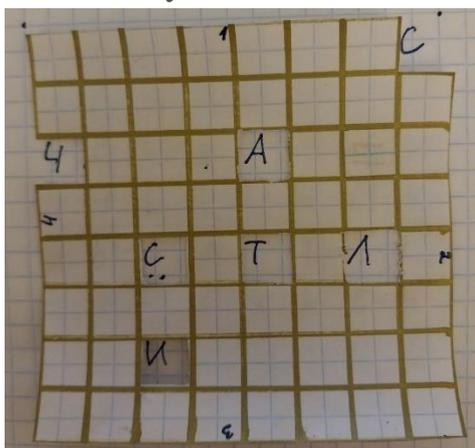


Решетка готова.

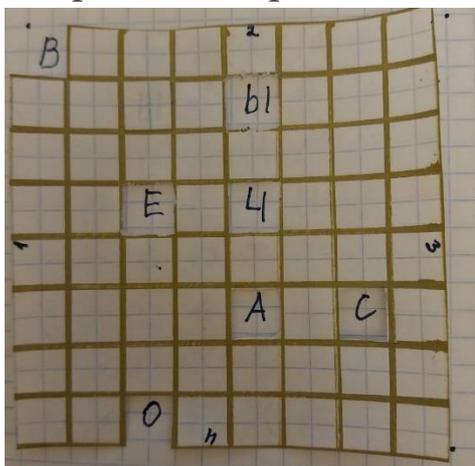
Теперь можно приступать к шифрованию.

Зашифруем крылатую фразу из произведения А.С. Грибоедова “Счастливые часов не наблюдают”

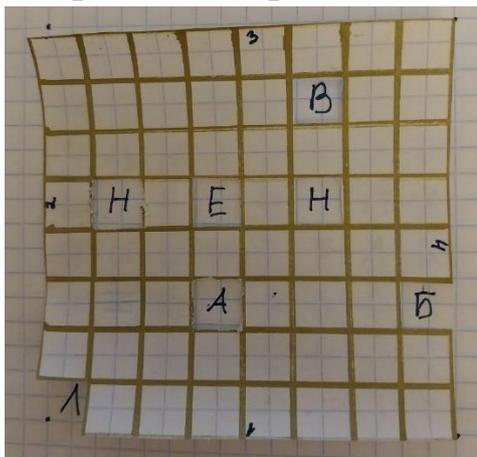
- Накладываем решетку на лист (стороной 1 вверх) и вписываем в окошки буквы



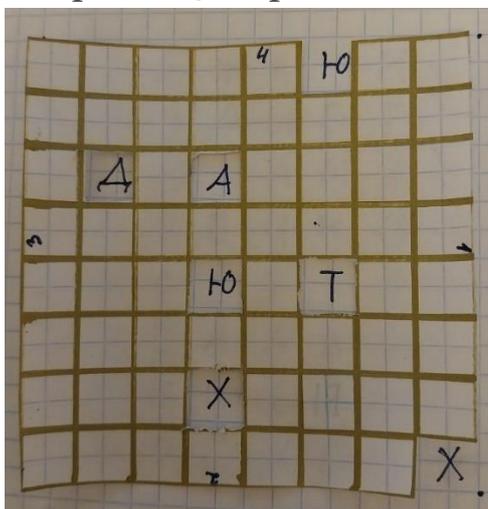
- Поворачиваем решетку на 90 градусов против часовой стрелки (стороной 2 вверх)



- Поворачиваем решетку на 90 градусов против часовой стрелки (стороной 3 вверх)

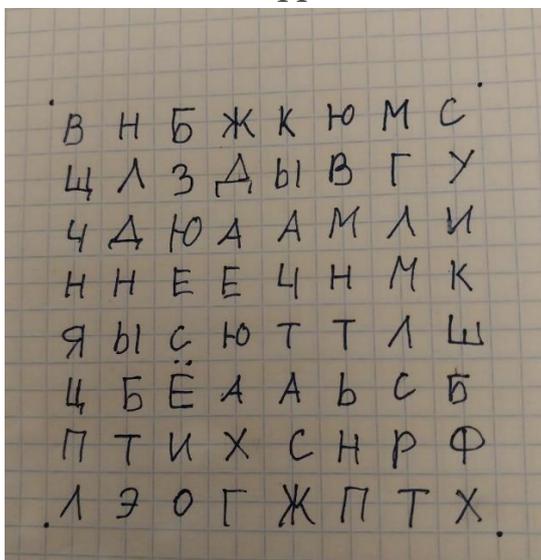


- Поворачиваем решетку на 90 градусов против часовой стрелки (стороной 4 вверх)



(две последние буквы “х” не несут смысла – ими мы заполнили оставшиеся пустыми окошки)

- Оставшиеся пустыми клетки заполняем произвольными буквами. Вот такой зашифрованный текст мы получили.



Для расшифровки на стороне получателя прикладываем ключ-решетку к квадрату с зашифрованным текстом сначала стороной с цифрой 1 вверх, а затем последовательными поворотами на 90 градусов против часовой стрелки читаем текст.

Для еще большего повышения стойкости можно также переписать этот текст в строку без пробелов и дописать несколько букв, чтобы не сразу можно было догадаться, какой метод шифрования использовался.

ВНБЖКЮМСЦЛЗДЫВГУЧДЮААМЛИННЕЕЧНМКЯЫСЮТТЛЩЦ-
БЁААЬСБПТИХСНРФЛЭОГЖПТХЧТК

Тогда дешифровальщику еще пришлось бы проверять гипотезы о примененной системе шифрования.

Заключение

В данной работе я познакомился с основными понятиями криптографии и историей её развития. Изучил принципы работы трех алгоритмов шифрования: “Шифр Цезаря”, “Шифр Виженера”, “Решетка Кардано” и на практике попробовал шифровать и дешифровывать текст с помощью изученных методов, а также разработал свою ‘решётку Кардано’.

Тема криптографической защиты информации очень интересна и актуальна в современном мире, я рад, что начал изучать азы этой науки и хочу продолжить погружение в этот увлекательный мир.

Список используемых источников и литературы

- В.Журавлёва “История шифров”, 2-е издание, 2019 год
- Статья “Криптография. Зашифрованные послания”
<https://nasledie.digital/articles/kriptografiya-zashifrovannye-poslaniya/?ysclid=lt4b5gfh3g422761542>
- Статья “Защита ячеек шифром Виженера”
<https://www.planetaexcel.ru/techniques/5/212/index.php?page=user&id=46156>
- Статья “Решетка Кардано”
<https://vuc.urfu.ru/ru/junarmija/kakie-byvajut-shifry/reshetka-kardano/>
- Статья “Шифры из прошлого: тайнопись и загадки докомпьютерной эпохи”
<https://3dnews.ru/916293/shifri-iz-proshlogo-taynopis-i-zagadki-dokompyuternoy-epohi>