Муниципальное автономное общеобразовательное учреждение

Средняя общеобразовательная школа №170 г. Екатеринбурга с

Углубленным изучением отдельных предметов.

## ИНДИВИДУАЛЬНЫЙ ПРОЕКТ

## на тему:

## «История криптографии»

## Работу выполнил:

## Кузнецов Кирилл Александрович,

## ученик 10 «Б» класса,

## Руководитель:

Сковородченко Нина Павловна

## Екатеринбург 2024

## Содержание

[Введение 3](#_Toc160554311)

[Информационная часть 5](#_Toc160554312)

[Практическая часть 7](#_Toc160554321)

[Заключение 14](#_Toc160554322)

[Ссылки 15](#_Toc160554323)

# 

**Введение**

1. **Актуальность темы.** Исследование истории криптографии актуально в связи с несколькими факторами:

* Мне интересно как в прошлом происходило шифрование важнейших сообщений, как развивалась эта наука, какие методы она использовала.
* Общественная актуальность заключается в том, что изучение развития шифров может дать новые идеи для усложнения используемых методов шифрования.

1. **Цель работы**. Рассмотрев и изучив развитие методов шифрования информации, создать программу шифрования сообщений при помощи этих методов.
2. **Задачи**.

* Исследовать эволюцию криптографии в разные временные рамки.
* Анализировать ключевые события и прорывы в истории криптографии, которые повлияли на развитие этой науки.
* Изучить различные методы и алгоритмы шифрования.
* Создать программу на python, которая, применяя методы шифрования, кодирует сообщения.

1. **Проблема, решаемая проектом.** Как происходило шифрование сообщений в разные временные рамки?
2. **Этапы работы**

* Постановка объекта исследования.
* Определение целей.
* Выполнение проекта.
* Создание продукта
* Завершение проекта.

1. **Предмет исследования**. Методы шифрования.
2. **Объект исследования.** История криптографии.
3. **Методы исследования**.

* Изучение литературы и других источников информации.
* Сравнение, противопоставление.
* Самооценка.
* Практика.

1. **Теоретическая значимость.** Изучение методов шифрования, их историю и слабые места.
2. **Практическая значимость.** Создание программы на python улучшила мои знания в этом языке программирования.
3. **Продукт проекта.** Программа на python, которая, применяя методы шифрования, кодирует сообщения.

# 

**Информационная часть**

Криптография — это наука, занимающаяся изучением методов шифрования данных с целью их защиты. Шифрование представляет собой процесс преобразования информации в вид, непонятный для непосвященных. Для этого используются различные методы и алгоритмы.

## Истоки криптографии можно проследить до древних цивилизаций, таких как Египет, Греция и Рим. В те времена сообщения кодировались с помощью различных методов, таких как замена букв, изменение порядка слов или использование шифров.

## 

## В Спарте для шифрования использовали скитала - шифрованное послание на обернутом вокруг палки ремне; для прочтения нужно было вновь обернуть его вокруг палки той же длины и толщины. Это пример перестановочного шифра, в нем меняется только позиция символа, а не сам символ. Одним из самых известных примеров древней криптографии является шифр Цезаря, который был изобретен Юлием Цезарем в 1 веке до н.э. Это шифр подстановки, который основан на замене каждой буквы в тексте на другую букву, отстоящую на определенное количество позиций в алфавите.

## Шифры, представленные выше, не являются надежными, но решение есть, если каждому символу в алфавите подставить другой случайный символ, то количество их комбинации будет исчисляться триллионами. Этот метод был предложен аль-Ки́нди в 9 веке. Но и этот шифр легко взломать. Проще всего это объясняется на примере русского алфавита.  В русском языке «О» — самая частая буква, после неё «А», затем «Е» и так далее, изучив текст и опознав в нем самый популярный символ, к примеру Ё, то можно предположить, что О шифруется как Ё, повторяя эту операцию для других символов.

## Для усложнения шифра добавлялись нулевые символы, специально допускались ошибки, использовалось кодирование (замена слов другими словами), но и это все не давало полной защиты.

## В 16 веке Блез де Виженер уже описал новый шифр, который одновременно использовал все варианты шифра Цезаря применяя ключевое слово. Самое важное, что одинаковые символы исходного слова в шифре будут выглядеть по-разному. Но даже этот шифр научились взламывать, а усложнять шифр – это слишком трудозатратно.

## В 20 веке появляется Энигма, которая, благодаря электронике, решала эту проблему. Энигма могла проводить шифрование быстро, а миллионы комбинаций шифрования намекали, что взломать ее не возможно. Но в конце концов Алан Тьюринг смог разработать Turing Bombe – электронно-механическая машина, для расшифровки кода Энигмы, которая за 20 минут могла узнать, какой ключ используется в этот день. Существует мнение, что это сократило Вторую Мировую Войну на два года.

## Сегодня, из-за увеличение вычислительной мощности, криптография вышла на новый уровень, сейчас для шифрования применяются такие большие ключи, что чтобы их подобрать понадобится триллионы лет.

## В современном мире криптография имеет множество различных применений: от шифрование сотовой связи и подключение к Wi-Fi, до шифрования банковских операций. Криптография актуальна в современном мире, без ее помощи не обходится любое действие в Интернете.

# 

**Практическая часть**

Создание программы на python, которая сможет шифровать сообщения, которые вы в нее напишите.

Для начала создадим программу, которая будет шифровать сообщение по принципу шифра Цезаря.

def dannie():  
 global alfavit, shag, slovo  
 alfavit = "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯабвгдеёжзийклмнопрстуфхцчшщъыьэюя" print("Вы выбрали шифрование методом Цезаря")  
 while True:  
 shag\_input = input("Введите шаг шифровки: ")  
 if shag\_input.isdigit():  
 shag = int(shag\_input) *# шаг* break  
 else:  
 print("Шаг шифровки должен быть числом. Попробуйте снова.")  
 slovo = input("Введите сообщение для шифровки: ") *#сообщение*def Zezar():  
 global alfavit, shag, slovo  
 itog = ""  
 for i in slovo:  
 a = alfavit.find(i)  
 a2 = a + shag  
 if i in alfavit:  
 itog += alfavit[a2 % len(alfavit)]  
 else:  
 itog += i  
 print("Зашифрованный текст:", itog)

Давайте разберем ее устройство. Во-первых, мы создаём функцию dannie(), она запрашивает у пользователя шаг шифровки и сообщение для шифровки. Эти данные сохраняются в глобальных переменных shag (шаг шифровки) и slovo (сообщение для шифровки).

Функция Zezar() выполняет шифрование с использованием шифра Цезаря. Она проходит по каждому символу в сообщении slovo. Если символ присутствует в алфавите, она находит его индекс и добавляет к нему шаг шифровки shag. Результат добавляется к переменной itog. Если символ не найден в алфавите, он остается без изменений. В конце функция выводит зашифрованное сообщение. Если вы хотите расшифровать сообщение, то перед шагом шифровки в программе ставится «-».

Теперь разберем то, как с помощью python можно шифровать сообщение по методу Аль-Кинди.

import random  
  
def random\_alf(): alfavit = list("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")  
 random.shuffle(alfavit)  
 return "".join(alfavit)  
  
def alkindi(text, alfavit):  
 shifr = ""  
 a = {char.upper(): alfavit[i] for i, char in enumerate("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")}  
 for char in text:  
 if char.isalpha():  
 shifr += a.get(char.upper(), char) else:  
 shifr += char  
 return shifr

Функция random\_alf() создает случайный алфавит. Она создает список букв русского алфавита, затем перемешивает их случайным образом и возвращает строку, состоящую из перемешанных букв.

Функция alkindi(text, alfavit) выполняет шифрование текста text с использованием алфавита alfavit, который был создан в прошлой функции. Для каждого символа в тексте она проверяет, является ли он буквой. Если да, то она находит соответствующий символ в перемешенном алфавите alfavit и добавляет его к зашифрованному тексту. Если символ не является буквой, он добавляется к зашифрованному тексту без изменений. Если вы хотите расшифровать сообщение, то обычный и перемешанный алфавит в программе меняется местами.

И последний, самый сложный метод шифрования, который я реализовал – это шифр Блез де Виженера.

def de\_vigener(text, key):  
 shifr = ""  
 key\_repeat = (key \* (len(text) // len(key)) + key[:len(text) % len(key)])  
 for i in range(len(text)):  
 a = text[i]  
 if a.isalpha():  
 sdvig = ord(key\_repeat[i].upper()) - ord('А')  
 if a.islower():  
 shifr += chr((ord(a) - ord('а') - sdvig) % 33 + ord('а'))  
 else:  
 shifr += chr((ord(a) - ord('А') - sdvig) % 33 + ord('А'))  
 else:  
 shifr += a  
 return shifr

Функция de\_vigener(text, key) принимает два аргумента: text - зашифрованный текст, и key - ключ для расшифровки.

Создается пустая строка shifr, в которую будут добавляться зашифрованные символы.

Ключ key повторяется до тех пор, пока его длина не сравняется с длиной текста text.

Затем происходит проход по каждому символу текста. Если символ является буквой, вычисляется сдвиг sdvig для текущего символа.

Далее, символ шифруется путем вычитания сдвига из его кода и полученное значение добавляется к строке shifr.

Если символ не является буквой, он добавляется к строке shifr без изменений.

После завершения цикла, функция возвращает расшифрованный текст.

Если вы хотите расшифровать сообщение, то переменная sdvig должна стать отрицательной.

А теперь создадим программу, которая будет спрашивать у пользователя то, каким шифром он хочет зашифровать текст и, которая, после выбора, будет запускать определенную функцию.

def repeat\_ras\_de\_vigener():  
 while True:  
 print("Вы выбрали расшифровку методом Виженера.")  
 text = input("Введите зашифрованный текст: ")  
 key = input("Введите ключ: ")  
 ras\_text = ras\_de\_vigener(text, key)  
 print("Расшифрованный текст:", ras\_text)  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
  
  
def repeat\_Zezar():  
 while True:  
 dannie()  
 Zezar()  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
  
def repeat\_al\_kindi():  
 while True:  
 print("Вы выбрали шифрование методом Аль-Кинди")  
 text = input("Введите сообщение для зашифровки: ")  
 ranalf = random\_alf()  
 shifr = alkindi(text, ranalf)  
 print("Алфавит: ", "АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")  
 print("Ключ: ", ranalf)  
 print("Зашифрованный текст: ", shifr)  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
  
def repeat\_de\_vigener():  
 while True:  
 print("Вы выбрали шифрование методом Виженера")  
 text = input("Введите текст для шифрования: ")  
 key = input("Введите ключ для шифрования: ")  
 shifr = de\_vigener(text, key)  
 print("Зашифрованный текст: ", shifr)  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
def ras\_Zezar():  
 global alfavit, shag, slovo  
 itog = ""  
 for i in slovo:  
 a = alfavit.find(i)  
 a2 = a - shag  
 if i in alfavit:  
 itog += alfavit[a2 % len(alfavit)]  
 else:  
 itog += i  
 print("Расшифрованный текст:", itog)  
def repeat\_ras\_Zezar():  
 while True:  
 dannie()  
 ras\_Zezar()  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
  
def ras\_alkindi(text, alfavit):  
 decrypted\_text = ""  
 a = {char.upper(): alfavit[i] for i, char in enumerate("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")}  
 for char in text:  
 if char.isalpha():  
 decrypted\_text += [key for key, value in a.items() if value == char.upper()][0]  
 else:  
 decrypted\_text += char  
 return decrypted\_text  
  
  
def repeat\_ras\_al\_kindi():  
 while True:  
 print("Вы выбрали шифрование методом Аль-Кинди")  
 text = input("Введите сообщение для расшифровки: ")  
 ranalf = input("Введите ключ: ")  
 shifr = ras\_alkindi(text, ranalf)  
 print("Расшифрованный текст: ", shifr)  
 repeat = input("Хотите продолжить? (да - 1/нет - 2/возврат - 3): ")  
 if repeat.lower() == "3":  
 vopros()  
 elif repeat.lower() == "2":  
 break  
  
def vopros ():  
 vopros1 = input("Выберите режим: Шифрование - 1; Расшифрование - 2: ")  
 if vopros1 == "1":  
 while True:  
 vopros = input("Выберите режим: Цезарь - 1, Аль-Кинди - 2, Блез де Виженер - 3: ")  
 if vopros == "1":  
 repeat\_Zezar()  
 break   
 elif vopros == "2":  
 repeat\_al\_kindi()  
 break  
 elif vopros == "3":  
 repeat\_de\_vigener()  
 break  
 else:  
 print("Попробуйте ввести снова")  
 else:  
 while True:  
 vopros3 = input("Выберите режим: Цезарь - 1, Аль-Кинди - 2, Блез де Виженер - 3: ")  
 if vopros3 == "1":  
 repeat\_ras\_Zezar()  
 break  
 elif vopros3 == "2":  
 repeat\_ras\_al\_kindi()  
 break  
 elif vopros3 == "3":  
 repeat\_ras\_de\_vigener()  
 break  
 else:  
 print("Попробуйте ввести снова")  
  
vopros()

Функции repeat\_Zezar(): и repeat\_ras\_Zezar(): запрашивают данные для шифрования методом Цезаря (данные, шаг шифрования), а затем шифрует или дешифрует текст с использованием функции Zezar(). После чего программа предлагает пользователю выбрать, хочет ли он продолжить, вернуться к выбору шифрования или завершить программу.

Функции repeat\_al\_kindi(): и repeat\_ras\_al\_kindi(): запрашивают текст для шифрования методом Аль-Кинди, генерирует случайный алфавит и шифрует текст с его помощью. После этого она выводит информацию об алфавите, ключе и зашифрованном тексте. Затем предлагает пользователю выбрать, хочет ли он продолжить, вернуться к выбору шифрования или завершить программу. Чтобы расшифровать сообщение вам понадобится случайный алфавит и зашифрованный текст.

Функции repeat\_de\_vigener(): и repeat\_ras\_de\_vigener(): запрашивают текст и ключ для расшифровки или шифровки методом Блеза де Виженера, а затем расшифровывает или шифрует текст с использованием функции de\_vigener(). После чего она также предлагает пользователю выбрать, хочет ли он продолжить, вернуться к выбору шифрования или завершить программу.

vopros(): Это основная функция, которая запрашивает у пользователя выбор режима шифрования (Цезарь, Аль-Кинди или Блез де Виженер) и вызывает соответствующую функцию в зависимости от выбора пользователя. Если выбран неправильный режим, программа сообщает об этом и запрашивает ввод снова.

В конце программы вызывается функция vopros(), чтобы начать её выполнение с запроса выбора режима работы.

# 

**Заключение**

Целью данного проекта являлось, изучив развитие методов шифрования информации, создание программы шифрования сообщений при помощи этих методов. В ходе изучения данной темы были решены следующие задачи:

* Исследовать эволюцию криптографии в разные временные рамки.
* Анализировать ключевые события и прорывы в истории криптографии, которые повлияли на развитие этой науки.
* Изучить различные методы и алгоритмы шифрования.
* Создать программу на python, которая, применяя методы шифрования, кодирует сообщения.

Исследовав историю криптографии, можно сделать несколько выводов. В раннее время шифрование сообщений происходило по простым алгоритмам, которые, на то время, давали достойную защиту информации. С каждым веком алгоритмы шифрования усложнялись, создавались методы, опиравшиеся на определенные формулы.

Также, изучив эти методы, я смог создать программу на python, которая, применяя их, кодирует сообщения и понял, как происходило шифрование сообщений в разные временные рамки.

Считаю, что цель по выполнению данной работы достигнута.

**Ссылки**

## Что такое криптография и как она стала частью нашей жизни: <https://trends.rbc.ru/trends/innovation/63120ea49a7947ccdd023670>

## Фукидид. История. Перевод и примечания Г. А. Стратановского (стр88):

## <http://www.co6op.ru/sites/default/files/fukidid._istoriya.pdf>

**Как расшифровать шрифт цезаря:**

[**https://uchet-jkh.ru/i/kak-rassifrovat-srift-cezarya/**](https://uchet-jkh.ru/i/kak-rassifrovat-srift-cezarya/)

**Аль-Кинди, криптография, дешифрация и шифры:**

[**https://ummet.kz/bes-pariz/373-news-rus/article/islam-i-nauka/10793-znaete-li-vy-chto-al-kindi-pisal-trudy-o-deshifrovke-soobshchenij.html**](https://ummet.kz/bes-pariz/373-news-rus/article/islam-i-nauka/10793-znaete-li-vy-chto-al-kindi-pisal-trudy-o-deshifrovke-soobshchenij.html)

## Шифр Виженера:

## <https://findhow.org/5076-shifr-vizhenera-onlajn.html>

## Устройство Энигмы: <https://www.youtube.com/watch?v=eJXmdi41Z2U&ab_channel=%D0%9D%D0%B8%D0%BA%D0%B8%D1%82%D0%B0%D0%9A%D0%B0%D1%80%D0%B0%D0%BC%D0%BE%D0%B2>

## Расшифровка Энигмы: <https://www.youtube.com/watch?v=p8K1BTCGTXw&ab_channel=%D0%9D%D0%B8%D0%BA%D0%B8%D1%82%D0%B0%D0%9A%D0%B0%D1%80%D0%B0%D0%BC%D0%BE%D0%B2>