

# Проект на тему “Алгоритмы шифрования”

Васильев Тимофей, Аникин Александр, Левинский Владислав



# Цели проекта

## Цели данного проекта:

- изучение основных методов шифрования данных
- научиться разрабатывать код для шифрования данных
- научиться разрабатывать собственные алгоритмы шифрования данных
- научиться разрабатывать интерфейс для программ шифрования данных



## Задачи проекта

- научиться разрабатывать графический дизайн интерфейса с помощью различных инструментов, таких как Python, PyQt6



## Задачи проекта

- описать ход разработки алгоритмов, интерфейса и кода для них
- продемонстрировать работу программы



## Техническое задание

В техническом задании мы будем выделять 2 требования: требования к разработке интерфейса и требования к шифровальным алгоритмам.

# Требования к интерфейсу



# Требования к интерфейсу. Палитра цветов

Основной цвет заднего фона программы - темно серый. Цвет заднего фона кнопок также выделен темно - серым градиентом, для лучшего понимания.

The screenshot shows a dark-themed application window. On the left, there are two input fields: 'Ввод текста' (Text input) and 'Ввод ключа' (Key input). On the right, there is a large rectangular area labeled 'Шифрованный/дешифрованный текст' (Encrypted/Decrypted text).

The screenshot shows a control panel with a 2x2 grid of buttons: 'Зашифровать' (Encrypt), 'Метод Шифрования' (Encryption Method), 'Дешифровать' (Decrypt), and 'Шифр Цезаря' (Caesar Cipher). Below this grid are three buttons: 'Удалить текст' (Delete text), 'Предыдущее действие' (Previous action), and 'Следующее действие' (Next action).

Цвет шрифта во всех окнах программы - белый, так как таким образом текст намного лучше различается перед тёмными цветами.

# Требования к интерфейсу. Расположение элементов

The screenshot shows a web application window titled "Шифровальщик". The interface is organized into several sections:

- Buttons:** "Зашифровать" (Encrypt) and "Дешифровать" (Decrypt) are located at the top left. Below them are "Удалить текст" (Delete text), "Предыдущее действие" (Previous action), and "Следующее действие" (Next action).
- Method Selection:** A dropdown menu labeled "Метод Шифрования" (Encryption Method) is positioned to the right of the main buttons, currently showing "Шифр Цезаря" (Caesar Cipher).
- Text Input:** A large text area labeled "Ввод текста" (Text input) is on the left.
- Key Input:** A smaller text area labeled "Ввод ключа" (Key input) is located below the main text input.
- Output:** A large text area on the right is labeled "Шифрованный/дешифрованный текст" (Encrypted/Decrypted text).

Взаимодействие с интерфейсом включает в себя несколько функций:

- кнопка шифрования
- кнопка дешифрования
- кнопка выбора метода шифровки
- удаление текста
- возвращение предыдущего действия
- возвращение следующего действия



# Требования к шифровальным алгоритмам





# Требования к шифровальным алгоритмам

Каждый шифр в программе можно разделить на 2 категории: основные и собственные. 3 основных шифра включают в себя: Шифр Цезаря, Шифр Виженера и Шифр Полибия. Это три самых элементарных и классических шифра, которые можно было использовать.

Собственные шифры же включают в себя алгоритмы, лично разработанные участниками проекта, каждый из которых имеет свой уникальный алгоритм.

При нажатии кнопки с верхним заголовком “Метод Шифрования”, открывается окно выбора, в котором есть 6 вышеописанных вариантов шифрования.

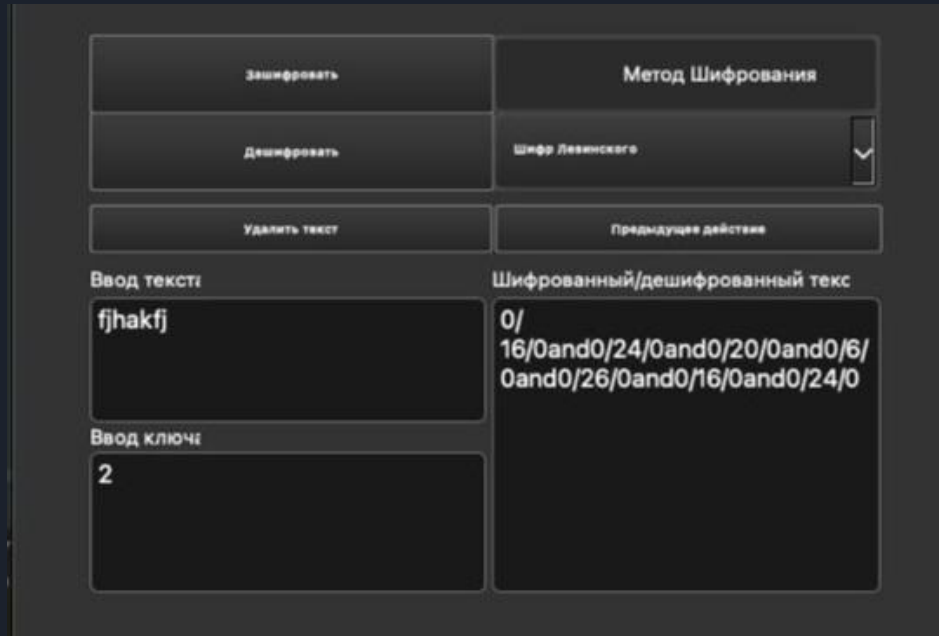


# Ход разработки

Ход разработки можно также поделить на несколько этапов:

1. Разработка собственных методов шифрования
2. Разработка интерфейса
3. Интеграция разработанных и заранее готовых алгоритмов в код

# Описание работы собственных шифров



The screenshot shows a web application interface for the Levin cipher. It features a dark gray background with white text and buttons. At the top, there are four buttons: 'Зашифровать' (Encrypt), 'Дешифровать' (Decrypt), 'Удалить текст' (Delete text), and 'Предыдущее действие' (Previous action). To the right of these buttons is a dropdown menu labeled 'Метод Шифрования' (Encryption Method) with 'Шифр Левинского' (Levin Cipher) selected. Below the buttons, there are two main input areas. The left area is labeled 'Ввод текста' (Text input) and contains the text 'fjhakfj'. Below it is a label 'Ввод ключа' (Key input) with the text '2'. The right area is labeled 'Шифрованный/дешифрованный текст' (Encrypted/Decrypted text) and contains the output: '0/16/0and0/24/0and0/20/0and0/6/0and0/26/0and0/16/0and0/24/0'.

Метод Шифрования
Шифр Левинского

Зашифровать

Дешифровать

Удалить текст

Предыдущее действие

Ввод текста

fjhakfj

Ввод ключа

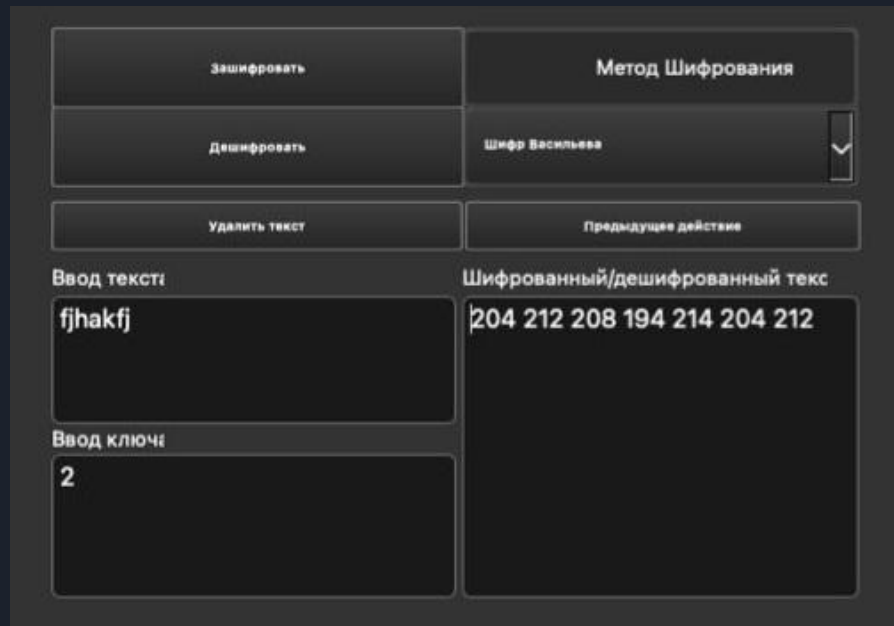
2

Шифрованный/дешифрованный текст

0/16/0and0/24/0and0/20/0and0/6/0and0/26/0and0/16/0and0/24/0

Шифр Левинского

# Описание работы собственных шифров



The screenshot shows a software interface for 'Шифр Васильева' (Vasильev's Cipher). The interface is dark-themed and contains several interactive elements:

- Buttons:** 'Зашифровать' (Encrypt), 'Дешифровать' (Decrypt), 'Удалить текст' (Delete text), and 'Предыдущее действие' (Previous action).
- Method Selection:** A dropdown menu labeled 'Метод Шифрования' (Encryption Method) currently shows 'Шифр Васильева'.
- Text Input:** A field labeled 'Ввод текста' (Text input) containing the text 'fjhakfj'.
- Key Input:** A field labeled 'Ввод ключа' (Key input) containing the number '2'.
- Output:** A large field labeled 'Шифрованный/дешифрованный текст' (Encrypted/Decrypted text) displaying the result '204 212 208 194 214 204 212'.

Шифр Васильева

# Описание работы собственных шифров

The screenshot shows a web application interface for the Anikina cipher. It features a dark gray background with white text and buttons. At the top, there are four buttons: 'Зашифровать' (Encrypt), 'Дешифровать' (Decrypt), 'Удалить текст' (Delete text), and 'Предыдущее действие' (Previous action). To the right of these buttons is a dropdown menu labeled 'Метод Шифрования' (Encryption Method) with 'Шифр Аникина' (Anikina Cipher) selected. Below the buttons, there are three input fields: 'Ввод текста' (Text input) containing 'fjhakfj', 'Ввод ключа' (Key input) containing '2', and 'Шифрованный/дешифрованный текст' (Encrypted/Decrypted text) containing '\*-)#=\*-'. The interface is clean and modern, with a focus on functionality.

Зашифровать	Метод Шифрования
Дешифровать	Шифр Аникина
Удалить текст	Предыдущее действие
Ввод текста fjhakfj	Шифрованный/дешифрованный текст *-)#=*-
Ввод ключа 2	

Шифр Аникина

Спасибо за внимание

