**Государственное бюджетное общеобразовательное учреждение города Москвы «Школа №1542»**

**ШИФР ПЛЕЙФЕРА НА РУССКОМ**

Авторы работы: ученики 11 «Б» класса

ГБОУ школа №1542

Королёв Владислав Сергеевич

Научный руководитель:

Аганов Вадим Маликович

**Москва, 2023**

**Оглавление**

[Введение (обоснование актуальности темы) 3](#_heading=h.gjdgxs)

[1. Зачем нужно шифровать 3](#_heading=h.30j0zll)

[2. Понятие шифра Плэйфера 3](#_heading=h.1fob9te)

[3. Актуальность 4](#_heading=h.3znysh7)

[4. Цели, задачи и этапы работы 4](#_heading=h.tyjcwt)

[4.1 Цель: 4](#_heading=h.3dy6vkm)

[4.2 Задачи: 5](#_heading=h.1t3h5sf)

[4.3 Этапы работы: 5](#_heading=h.4d34og8)

[5 Методы и материалы 5](#_heading=h.2s8eyo1)

[5.1 Программы: 5](#_heading=h.17dp8vu)

[5.2 Методы: 5](#_heading=h.3rdcrjn)

[6 Разработка сайта 6](#_heading=h.26in1rg)

[7 Разработка программы шифрования 6](#_heading=h.lnxbz9)

[8 Результаты 6](#_heading=h.35nkun2)

[9 Перспективы 7](#_heading=h.1ksv4uv)

[10 Схема алгоритма программы 7](#_heading=h.44sinio)

[11 Литература 7](#_heading=h.2jxsxqh)

# Введение (обоснование актуальности темы)

1. **Зачем нужно шифровать**

«У меня нет никаких тайн, мне нечего скрывать», – часто можно услышать от пользователей, когда речь заходит о шифровании и других средствах защиты конфиденциальности.  Но практика показывает, что это не так. Файл, сохраненный на рабочий стол компьютера или телефон, оставленный в гостиной, довольно быстро будет изучен кем-то.

1. **Понятие шифра Плейфера**

Шифр Плейфера или квадрат Плейфера — ручная симметричная техника шифрования, в которой впервые использована замена биграмм. Изобретена в 1854 году английским физиком Чарльзом Уитстоном, но названа именем лорда Лайона Плейфера, который внёс большой вклад в продвижение использования данной системы шифрования в государственной службе. Шифр предусматривает шифрование пар символов (биграмм) вместо одиночных символов, как в шифре подстановки и в более сложных системах шифрования Виженера. Таким образом, шифр Плейфера более устойчив к взлому по сравнению с шифром простой замены, так как усложняется его частотный анализ. Он может быть проведён, но не для символов, а для биграмм. Так как возможных биграмм больше, чем символов, анализ значительно более трудоёмок и требует большего объёма зашифрованного текста.

1. **Актуальность**

В данный момент многие не понимают, как зашифровывать текст методом Плейфера на русском, или делают это неправильно. Сейчас нет никаких сайтов, которые могут зашифровать сообщение, написанное на русском, методом Плейфера. Они могут сделать это лишь на английском языке.

Вы можете попробовать поставить себя на место студента, который учиться на факультете кибер-безопасности. У него горят сроки, а ему нужно зашифровать десяток сообщений данным методом. Так же у него есть и другие задачи, которые требуют большее количество времени. Естественно этот студент захочет сократить время работы, и в этом ему поможет наш сайт. Он сможет за минуту зашифровать десяток сообщений методом Плейфера, хотя если бы он делал это на бумаге, то вышло бы в несколько раз дольше.

Так же вы можете представить себе ситуацию, когда вам нужно передать конфиденциальную информацию, но просто написать – рискованно. Тогда вам поможет наш сайт, который за мгновение зашифрует сообщение.

1. **Цели, задачи и этапы работы**
   1. **Цель:**

Повысить доступность шифра Плейфера для российской аудитории

* 1. **Задачи:**

1. Научится программировать на python
2. Научится создавать сайты
3. Изучить шифр Плейфера
4. Создать сайт, позволяющий шифровать вводимый текст методом Плейфера
   1. **Этапы работы:**
5. Разработка дизайна сайта
6. Написание сайта
7. Написание кода для сайта
8. Оформление проекта
9. **Методы и материалы**
   1. **Программы:**

Visual Studio для вёрстки сайта

PyCharm для написания кода Python

Figma для создания дизайна сайта

* 1. **Методы:**

**Изучение материалов:**

Углублённое изучение языка Python

Изучение фрейморка Flask

**Проектирование:**

Создание эскиза сайта

Создание конечного дизайна сайта

**Моделирование:**

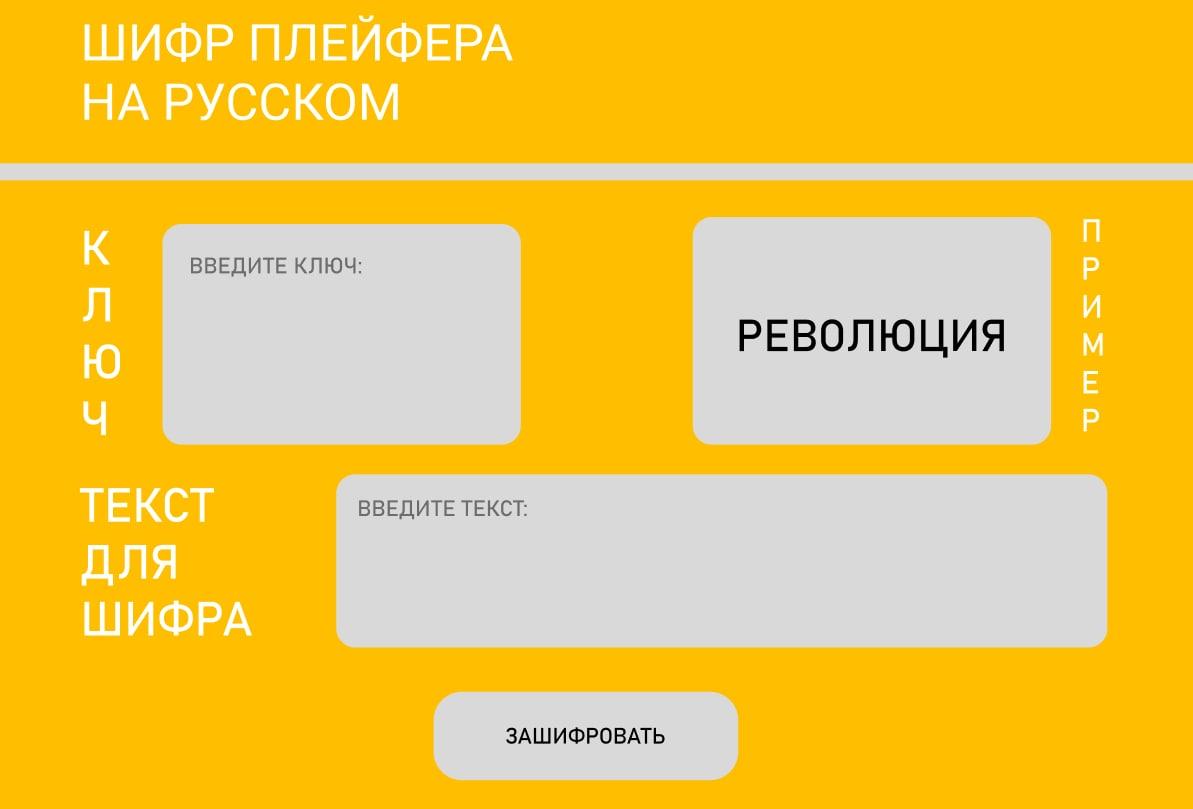
Создание сайта

Написание кода на языке Python

**Натурный эксперимент**

1. **Разработка сайта**

Первоначально был разработан эскиз сайта. Далее с помощью программы Figma, с учётом современных тенденций вида сайта, был разработан сам сайт.



Дизайн сайта (1)

1. **Разработка программы шифрования**

На основе изученного алгоритма шифрования методом Плейфера, был разработан алгоритм программы шифрования для сайта.

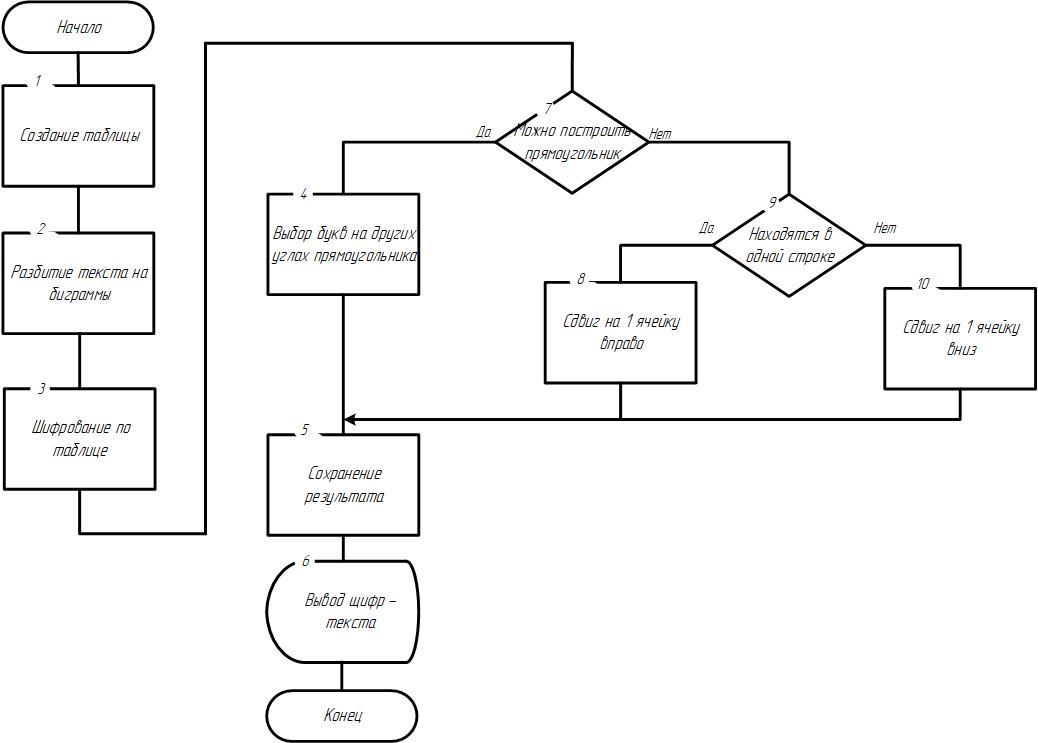
1. **Результаты**

Изучен шифр Плейфера. Готова HTML страница, а также код Python. Проведён натурный эксперимент с помощью одноклассников.

1. **Перспективы**

Дальнейшая работа над проектом должна включать поддержку разработанного сайта и доработку программного кода с позиции его эффективности. Кроме того, планируется добавить функцию по расшифровке зашифрованных сообщений.

1. **Схема алгоритма программы**



1. **Литература**

[1][https://stackoverflow.com](https://stackoverflow.com/)

* Автор: approximatenumber
* Название статьи: Применение CSS-свойств к элементам внутри определённого div.
* Ресурс: форум StackOverFlow
* Ссылка на статью: <https://ru.stackoverflow.com/questions/640691>

[2]<http://htmlbook.ru/samhtml/>

* Название статьи: Тег <div>.
* Ресурс: htmlbook
* Ссылка на статью: <http://htmlbook.ru/index.php/html/div>

[3] <https://qna.habr.com>

* Автор: WhiteNiBBa
* Название статьи: Как написать шифр Плейфера на python?
* Ресурс: форум qna.habr
* Ссылка на статью: <https://qna.habr.com/q/874071>