|  |  |
| --- | --- |
|  | **МИНОБРНАУКИ РОССИИ**  Федеральное государственное бюджетное образовательное учреждение высшего образования  **«Национальный исследовательский университет «МЭИ»** |

**Расчетное задание**

По дисциплине «Криптографические методы защиты информации»

**«**Программная реализация шифра Плейфера**»**

|  |  |
| --- | --- |
| Студент А-13а-20 | Зайцева И.А. |
| Преподаватель | Хорев П.Б. |

Москва 2024

Содержание

[Введение 3](#_Toc165288248)

[Описание шифра 4](#_Toc165288249)

[Описание программы 5](#_Toc165288250)

[Заключение 6](#_Toc165288251)

[Список использованных источников 7](#_Toc165288252)

[Приложение 8](#_Toc165288253)

# Введение

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.

Шифр Плейфера также может быть легко взломан, если имеется достаточный объём текста. Получение ключа является относительно простым, если известны шифрованный и обычный текст. Когда известен только зашифрованный текст, можно провести частотный анализ, но не для 26 возможных символов латинского алфавита, а для 25 ⋅ 24 = 600 возможных биграмм (одна из букв и биграммы из двух одинаковых букв исключаются). Криптоаналитики анализируют соответствие между частотой появления биграмм в зашифрованном тексте и известной частотой появления биграмм в языке, на котором написано сообщение [1].

Данный шифр стал первым буквенным биграммным шифром. Он был предназначен для обеспечения секретности телеграфной связи и применялся британскими войсками в Англо-бурской и Первой мировой войнах. Им пользовалась также австралийская служба береговой охраны островов во время Второй мировой войны[2].

# Описание шифра

Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила.

Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку).

Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице.

Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».
2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении [1].

# Описание программы

В выполненной программной реализации шифра Плейфера используются два алфавита – латинский и кириллический. Пользователь может выбрать язык, с которым будет работать, используя специальный переключатель. В качестве служебных символов используются символы «\*» и «$». Символ «\*» служит для отделения одинаковых символов в исходном слове, а символ «$» используется как разделитель между словами.

Разработанная программа позволяет шифровать и расшифровывать сообщения, введенные пользователем непосредственно в поле для ввода. Также имеется возможность зашифровать или расшифровать текстовые данные, загруженные из файла, и сохранить результат на компьютер.

Для выбора режима шифрования необходимо выбрать нужный режим в раскрывающемся списке в главном окне программы. Кроме обычных режимов шифрования и расшифрования доступны режимы шифрования и расшифрования с добавлением и проверкой сигнатуры соответственно. Данный режим позволяет проверить правильность введенной парольной фразы. В противном случае оценка правильности расшифровки устанавливается пользователем.

В качестве демонстрации, в программе добавлена возможность просмотреть матрицу шифрования, которая была сформирована на основе парольной фразы и используемого алфавита. Для отображения необходимо после проведения процедуры шифрования или расшифрования щелкнуть соответствующую галочку «Отобразить матрицу шифрования». Интерфейс программы можно посмотреть в приложении.

**Примечание**: в тексте сообщения и парольной фразы могут быть использованы только заглавные буквы и пробелы. Строчные буквы будут автоматически переведены в верхний регистр, а все остальные символы будут проигнорированы. Данные ограничения появляются из-за особенностей шифра. Экспериментально получен вывод о том, что, если мощность алфавита слишком велика (при попытке объединения в одну таблицу символы латинского и кириллического алфавитов, обеих регистров, а также знаков препинания и других символов), возникает проблема того, что шифр становится нечувствительным к правильности парольной фразы. Например, секрет «африка», может быть подменен секретом «африка1», из-за незначительного смещения символов таблицы.

# Заключение

Шифр Плейфера позволяет шифровать текстовые сообщения. Его особенностью является использование матрицы алфавита, с помощью которой преобразуются биграммы исходного текста. Достаточно прост в реализации, более устойчив к криптоанализу, чем шифр простой замены, однако все ещё уязвим для криптоатак. В годы первой и второй мировых войн использовался некоторыми спецслужбами, однако в настоящее время используется как инструмент скрытия некоторой информации от непрофессионалов. Например, в уличных квестах, в которых необходимо разгадывать загадки [2].

# Список использованных источников

1. Шифр Плейфера [Электронный ресурс]: Википедия. Свободная энциклопедия. – URL: <https://ru.wikipedia.org/wiki/Шифр_Плейфера> (дата обращения: 28.04.2024)

2. Шифр Плейфера [Электронный ресурс]: NightQuests Сайт о субкультуре городских квестов. – URL: https://nightquests.ru/knowledgebases/shifr-playfair-chestnaya-igra/ (дата обращения: 28.04.2024)

# Приложение

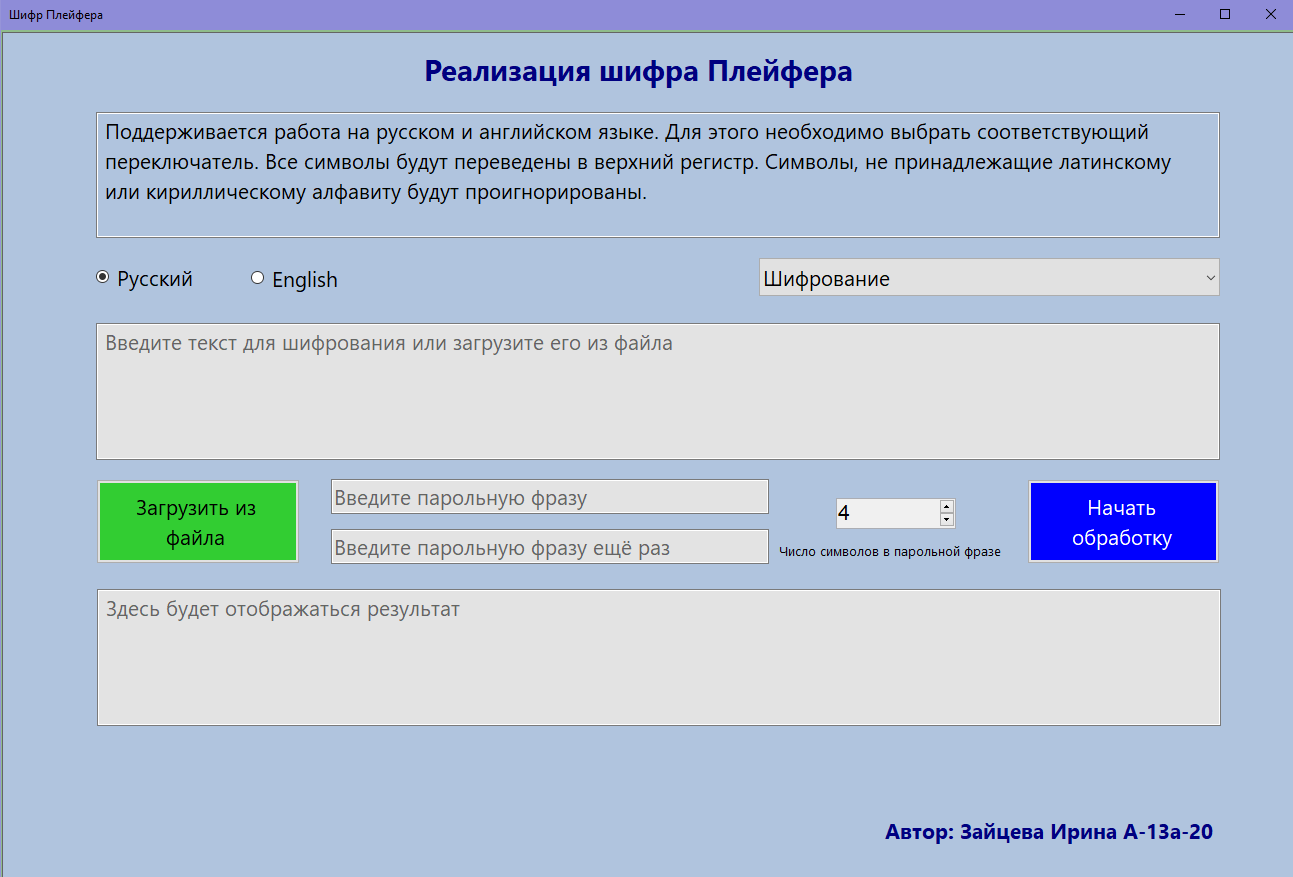
****

Рисунок 1 Главное окно приложения

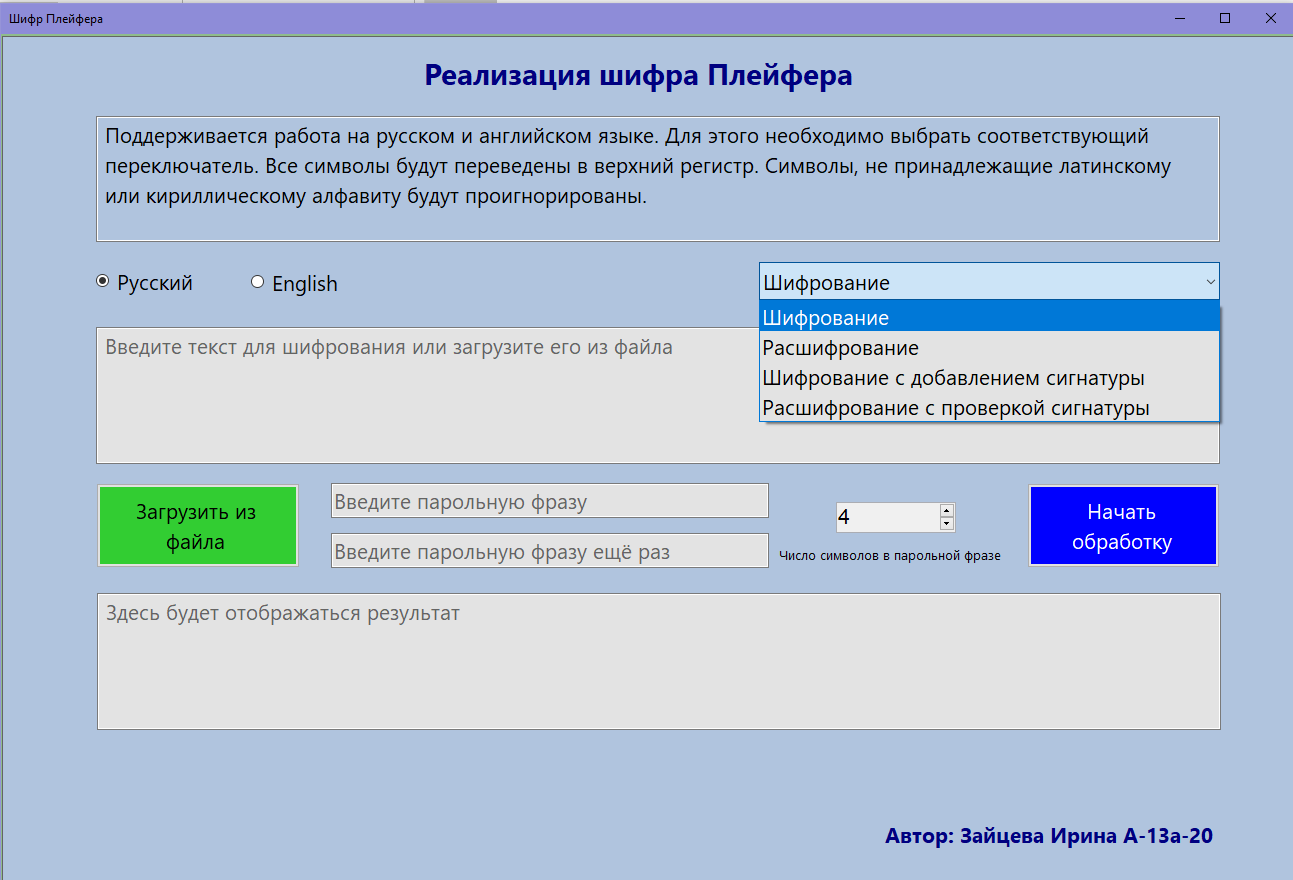


Рисунок 2 Демонстрация выбора режимов

Кнопка «Отправить результат на расшифрование» автоматически перенесет результат в поле для ввода исходного текста.

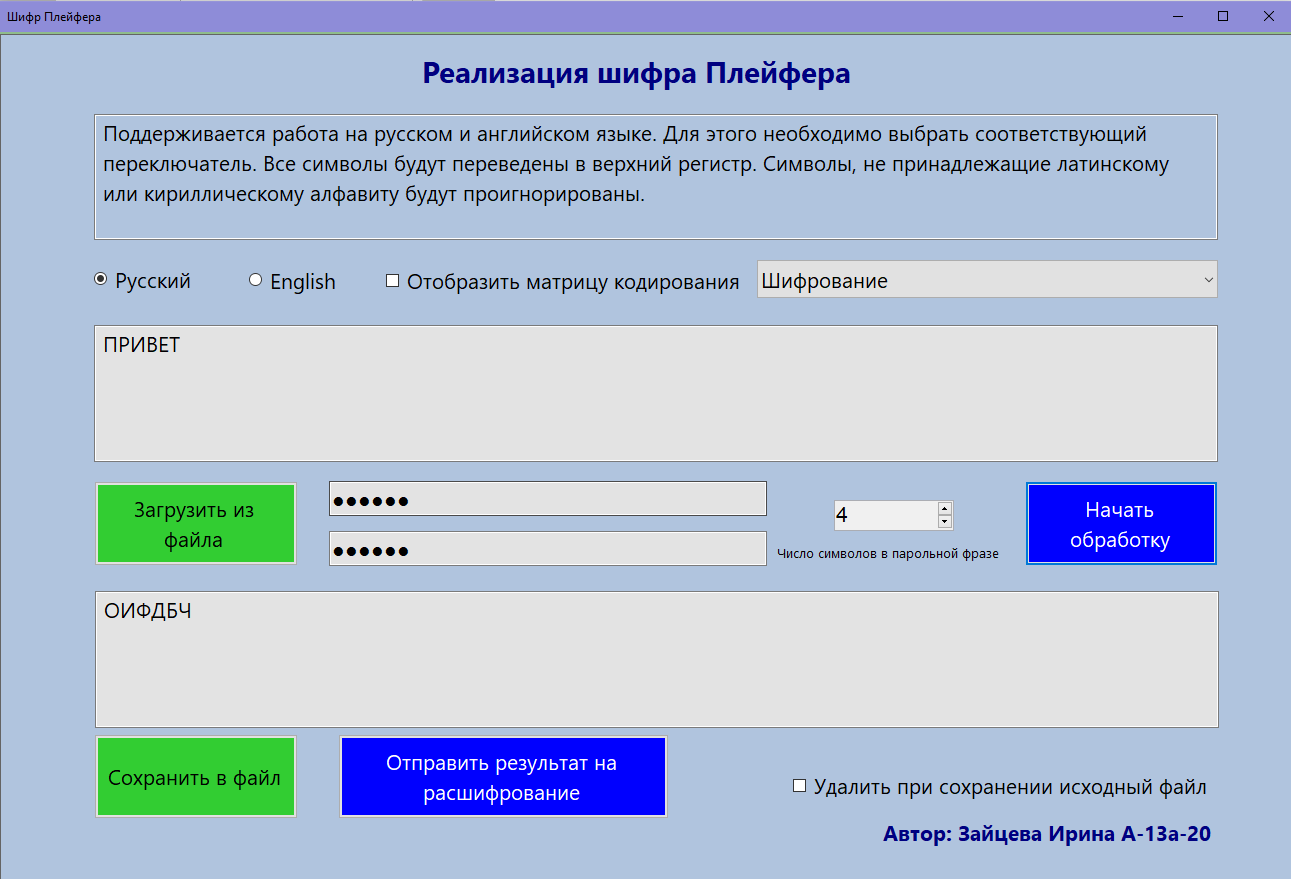


Рисунок 3 Пример работы программы

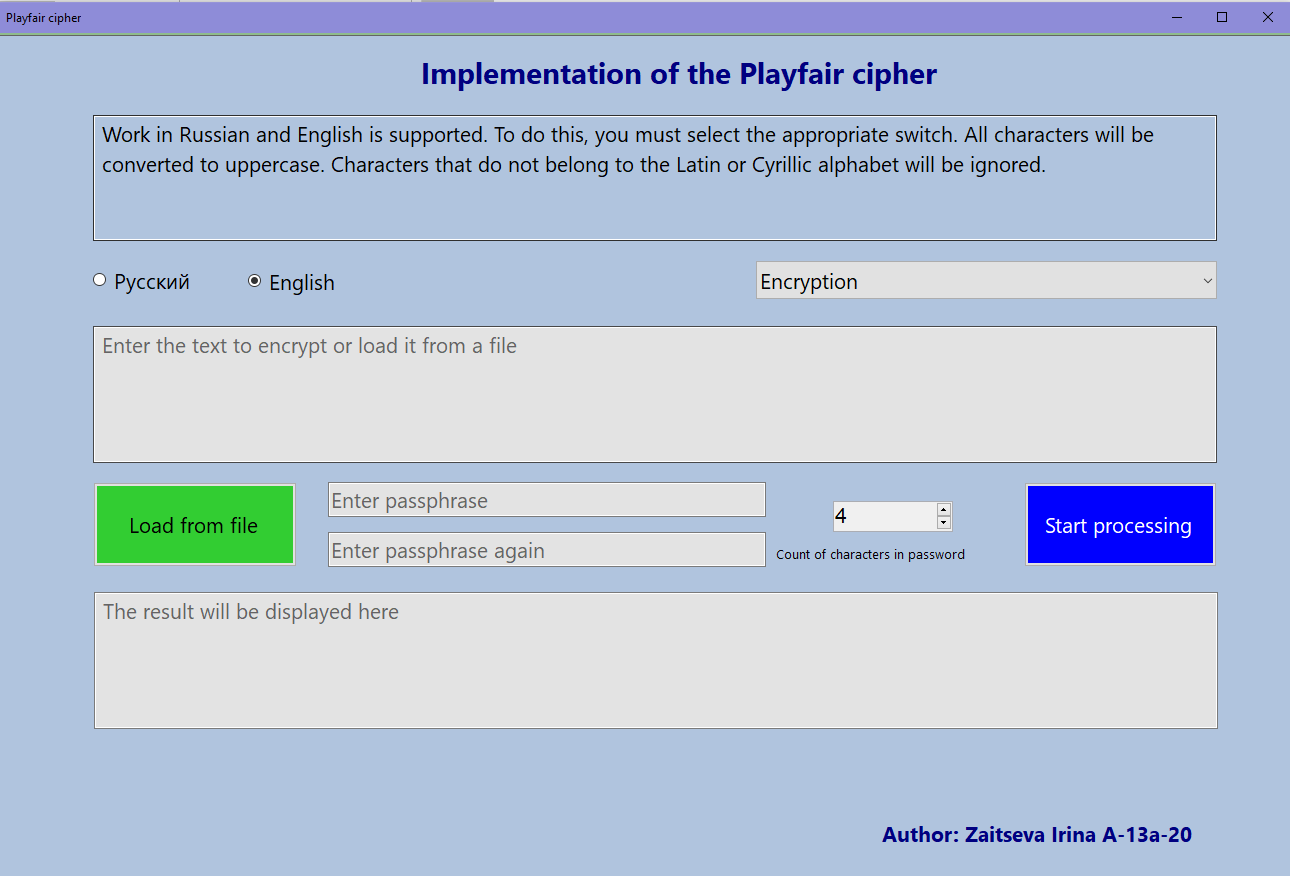
Также работа программы поддерживается на английском языке. 

Рисунок 4 Программа с интерфейсом на английском языке