Приложение для изучения отечественных криптопреобразований «ЛИТОРЕЯ», версия 0.1

Руководство пользователя

Санкт-Петербург

2023

Содержание

Введение

Представлен функционал предварительной версии приложения для самостоятельного изучения российских стандартов шифрования «Магма» и «Кузнечик».

Детали используемых преобразований описаны в виде подсказок, содержащих примеры расчётов.

Предусмотрена возможность пошагового выполнения преобразований для предъявления обучающемуся эталонных значений, с которыми можно сравнивать результаты расчетов, сделанных самостоятельно.

1. Запуск приложения

После завершения установки можно переместить запускаемый файл “LitoreR.exe” в удобное место и начинать работу с приложением, дважды кликнув по иконке. Начальный экран (рисунок 1.1) содержит меню основных функций приложения и окно ввода текста для зашифрования

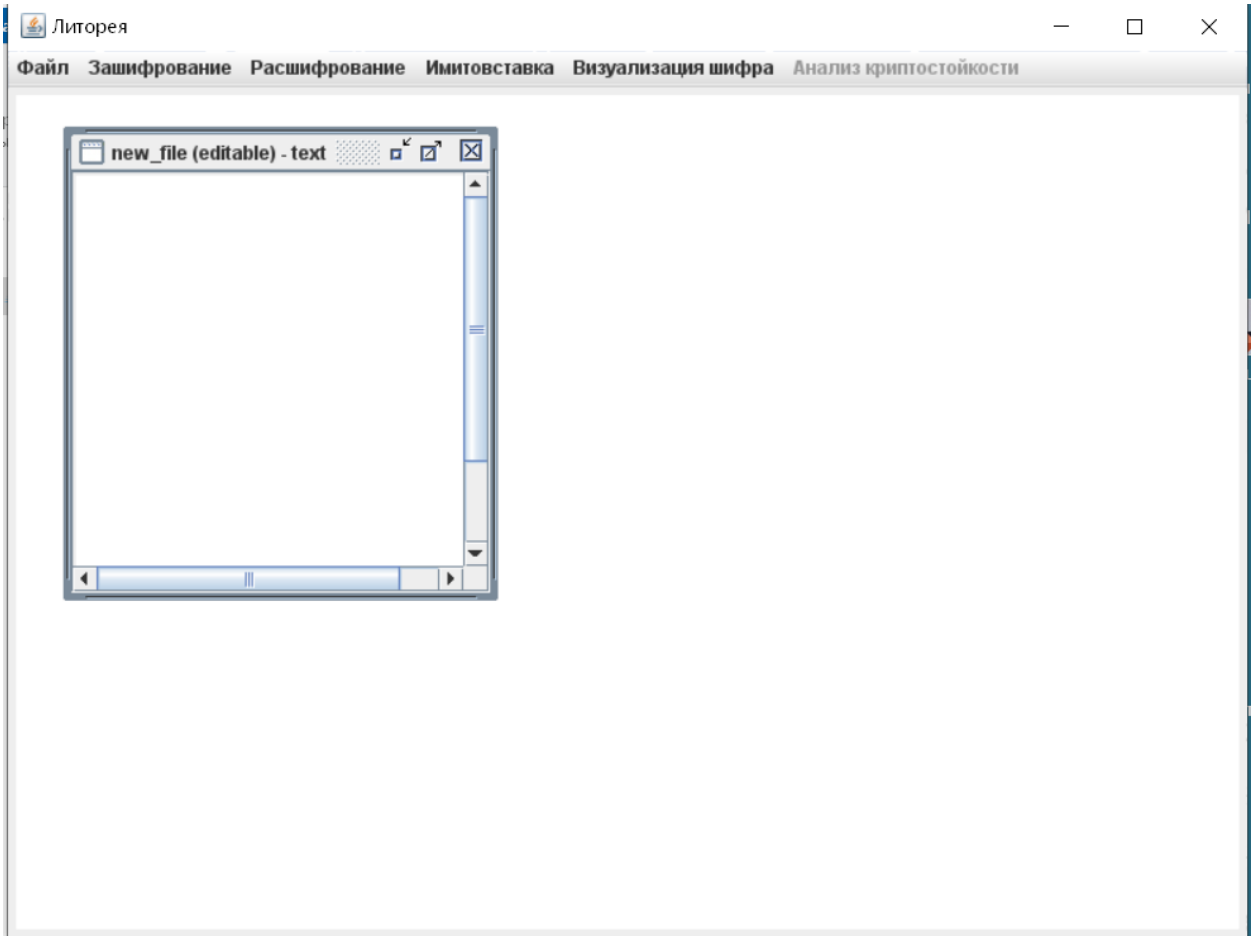


Рисунок 1.1 – Основное меню приложения

2. Меню функций

2.1. Файл: создание/открытие

Доступно две функции: создание файла и открытие ранее созданного файла на компьютере.

Создать можно файлы только двух типов: текстовый (.txt) и бинарный (.bin).

После того, как работа с созданным файлом закончена и требуется **сохранить** файл, необходимо: закрыть окно файла (пискограмма x), затем подтвердить сохранение (рисунок 2.1) и, наконец, назначить имя сохраняемому файлу, **его расширение в явном виде** (.txt/.bin), а также выбрать расположение сохраняемого файла (рисунок 2.2)

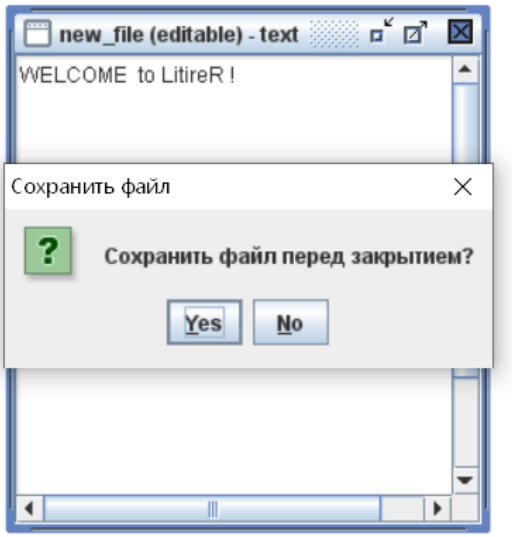


Рисунок 2.1 – Запрос на сохранение файла

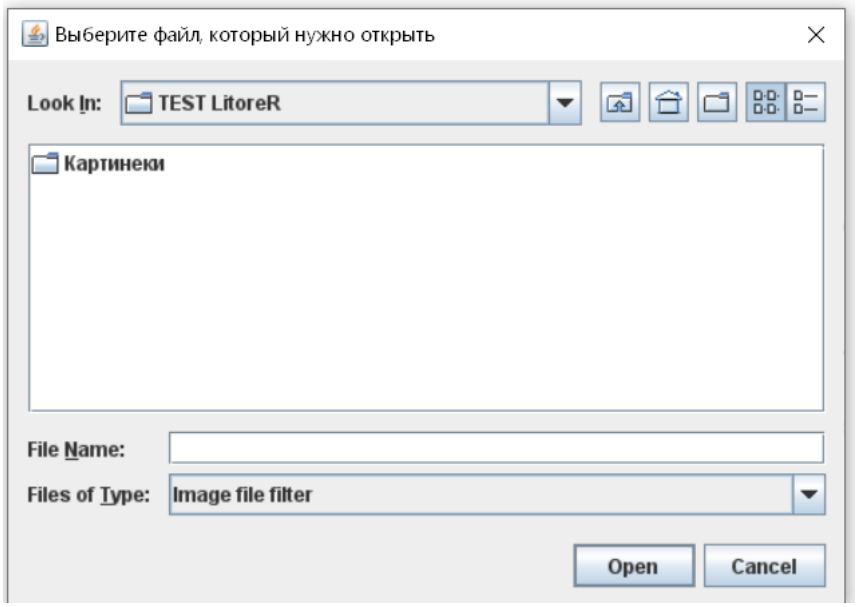


Рисунок 2.2 – Выбор месторасположения сохраняемого файла

Существует возможность (рисунок 2.3) открыть текстовый файл (txt), бинарный файл (bin) и файл с изображением (bmp, png, jpg, jpeg,)

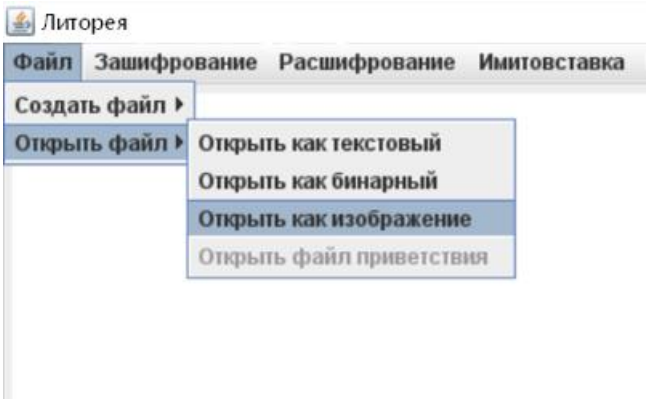


Рисунок 2.3

2.2. Зашифрование/расшифрование файла данных

Чтобы произвести зашифрование / расшифрование необходимо:

1. Открыть/создать файл данных (рисунок 2.4)

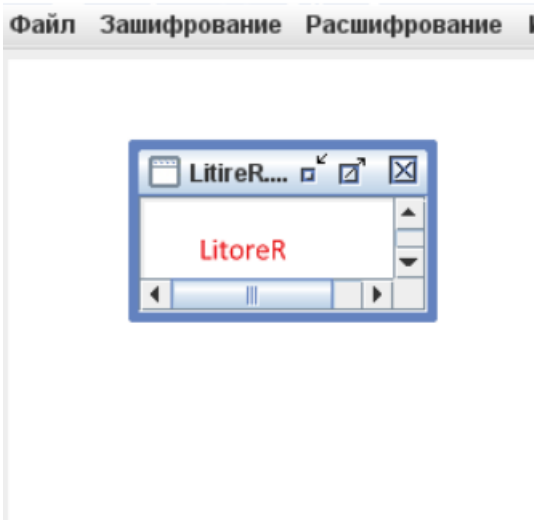


Рисунок 2.4 – Подготовленный файл данных для зашифрования/расшифрования

2. Выбрать процедуру (Зашифрование или Расшифрование)
3. Выбрать необходимый шифр и его режим работы (рисунок 2.5)

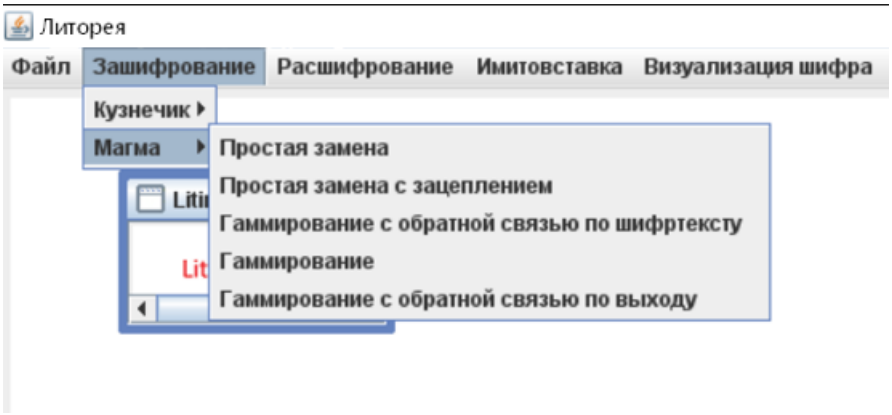


Рисунок 2.5 – Выбор шифра и его режима работы

4. Ввести, при необходимости секретный ключ, выбрать способ дополнения и ввести, при необходимости, синхропосылку (рисунок 2.6).

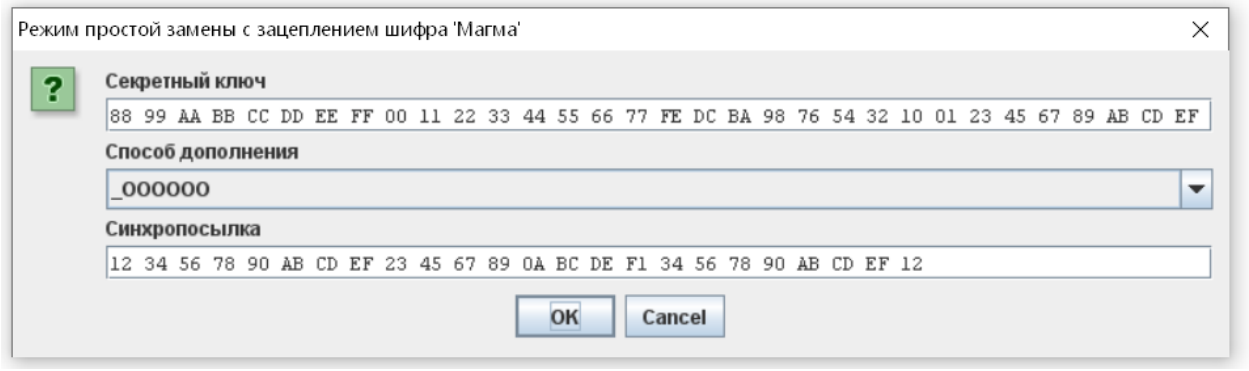


Рисунок 2.6 - Исходные параметры для зашифрования / расшифрования

При попытке выполнить процедуру без предварительного открытия целевого файла данных пользователю будет показано сообщение об ошибке (рисунок 2.7)

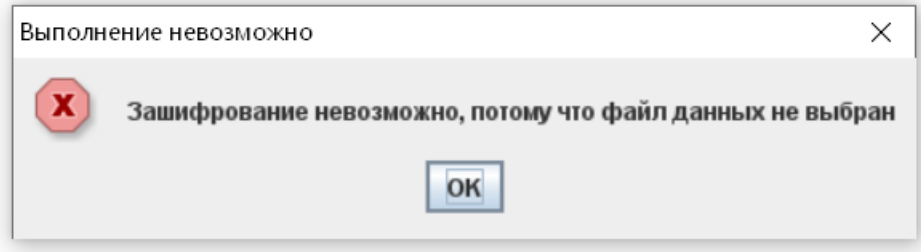


Рисунок 2.7 – Сообщение об отсутствии целевого файла

2.3. Выработка имитовставки

Для выработки (создания кода) имитовставки необходимо проделать шаги аналогичные описанным в п. 2.2

2.4. Визуализация криптопреобразований

Для запуска процедуры визуализации преобразований шифра необходимо:

.

1. Выбрать шифр и требуемое преобразование для визуализации (например, раундовые преобразования, процедура развертывания ключа). Целевой файл данных для работы процедуры визуализации создавать не нужно

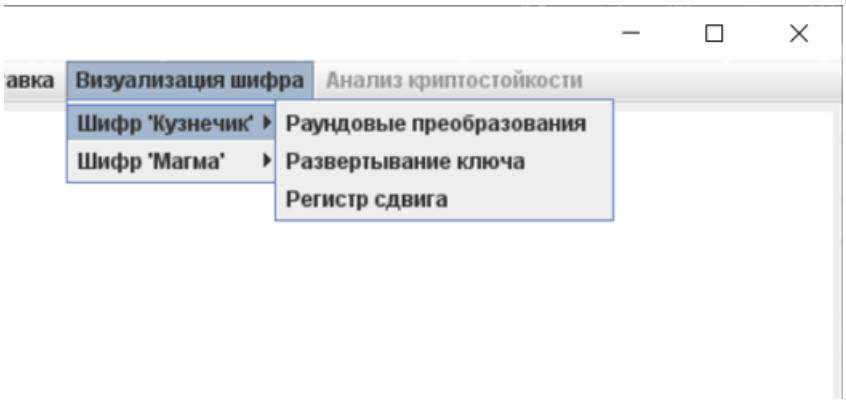


Рисунок 2.5 – Выбор преобразования для визуализации

2. Ввести входные параметры для процедуры визуализации (например, секретный ключ, способ дополнения последнего блока данных)

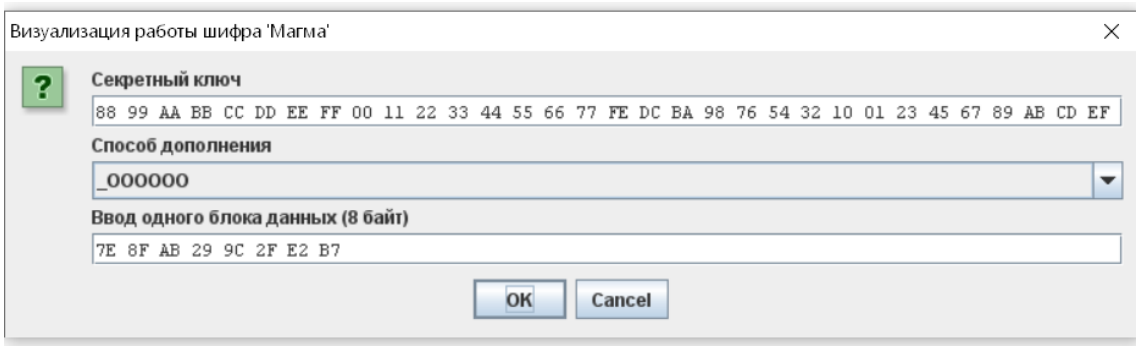
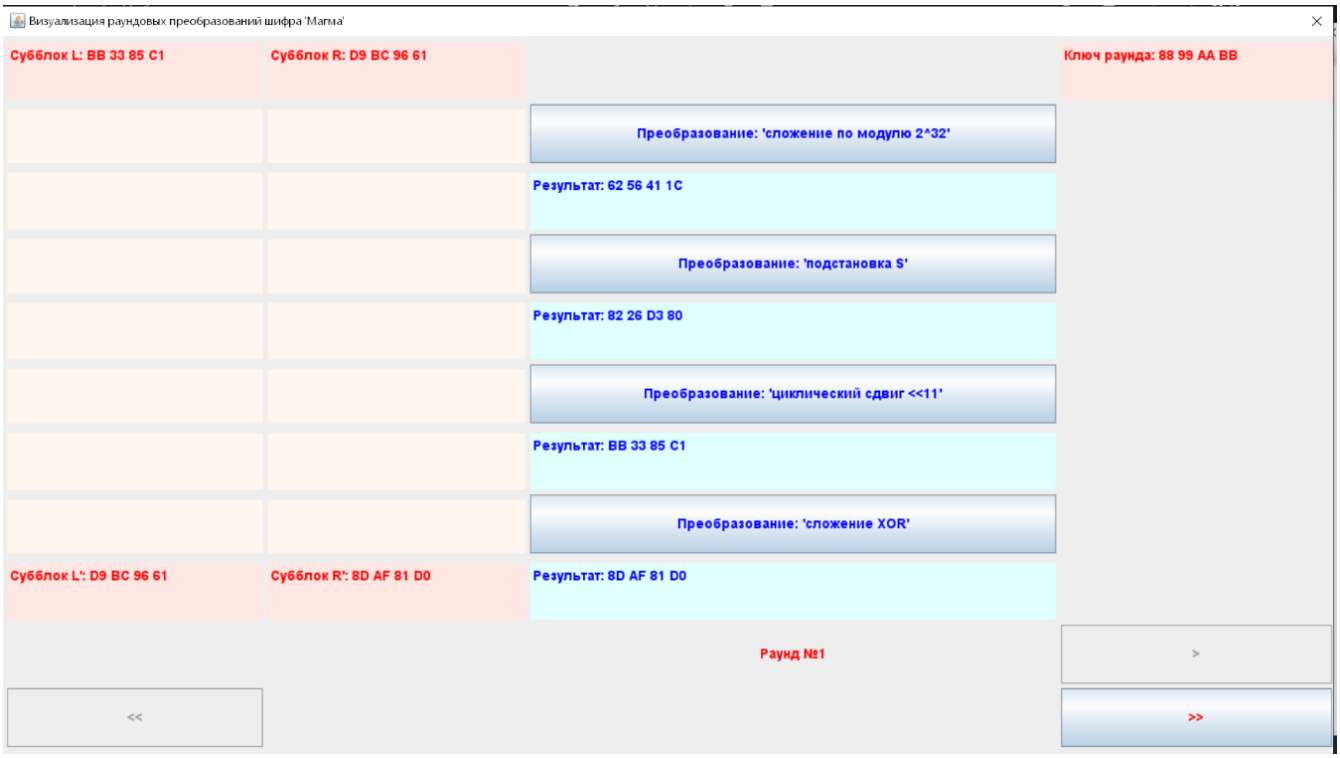


Рисунок 2.6 Ввод параметров для процедуры визуализации

3. В рабочем окне процедуры визуализации можно пошагово управлять выполнением криптопреобразований и просматривать результаты выполнения каждого шага



4. Управление визуализацией происходит посредством кнопок с надписями:

    a. Кнопки с надписями “>>” и “<<” для навигации по раундам
    b. Кнопки с надписями “>” и “<” для навигации по внутираундовым преобразованиям

5. Красным цветом в рабочем окне выделены данные, относящиеся к раундам, а синим – промежуточные результаты внутираундовых преобразований.

6. Подсказку по внутрираундовым преобразованиям можно получить щелчком «мыши» по кнопке с наименованием преобразования.

2.5. Имитация атаки «грубой силы»

Эта функция находится в процессе разработки