Отчёт заказчику

Проект "Четыре алгоритма шифрования" выполнен с использованием передовых технологий в сфере Web-разработки. В процессе создания программного обеспечения были задействованы:

1. Веб-браузер Opera и Google Chrome для тестирования на кросс-браузерность и как основа для графического пользовательского интерфейса;
2. Высокоуровневый язык программирования общего назначения Python версии 3.6.2 для разработки прототипов программного обеспечения, реализующих методы шифрования согласно требуемым алгоритмам;
3. Сценарный мультипарадигменный язык программирования JavaScript для создания финальной версии программного обеспечения и графического пользовательского интерфейса;
4. Язык разметки XML, который в ходе дальнейшей разработки проекта было решено заменить на HTML5 в связи с недостаточностью встроенного функционала в XML;
5. Онлайн-сервис «Marvel» для проектирования прототипов графического пользовательского интерфейса;

В рамках проекта были предъявлены следующие функциональные требования:

1. Все требуемые алгоритмы шифрования должны быть реализованы и функционировать без возникновения системных ошибок;
2. Реализовать метод шифрования данных согласно алгоритму «Шифр Цезаря»;
3. Реализовать метод шифрования данных согласно алгоритму «XOR»;
4. Реализовать метод шифрования данных согласно алгоритму «Случайное перемешивание»;
5. Реализовать метод шифрования данных согласно алгоритму «Блочная перестановка»;
6. Возможность использования методов шифрования «XOR», «Шифр Цезаря» и «Блочная перестановка» поочерёдно, путём передачи получаемого результата одним из методов на вход другому. Последовательность методов выбирается пользователем вручную. В дальнейшем называется «Комбинированное шифрование»;
7. Реализована возможность удобного использования результата, полученного методом «Комбинированное шифрование», за пределами предоставленного программного обеспечения;
8. Валидация всех входных данных;
9. Финальная версия программного обеспечения должна иметь удобный, достаточный и отзывчивый графический пользовательский интерфейс;
10. При вводе пользователем не корректных данных уведомлять об этом пользователя;
11. При указании пользователем не корректных параметров необходимых для функционирования большинства методов шифрования – обеспечить устойчивость программного продукта к такому роду ошибок и уведомить об ошибке пользователя;
12. Написана инструкция пользователя;

Выполнено следующее:

1. Создан и спроектирован удобный, адаптивный и достаточный графический пользовательский интерфейс;
2. Создан метод шифрования данных алгоритмом «Шифр Цезаря»;
3. Создан метод шифрования данных алгоритмом «XOR»;
4. Создан метод шифрования данных алгоритмом «Случайное перемешивание»;
5. Создан метод шифрования данных алгоритмом «Блочная перестановка»;
6. Реализована возможность зашифровать данные методом «Комбинированное шифрование» использующий методы: «Шифр Цезаря», «XOR», «Блочная перестановка»;
7. Проведены тесты с использованием различных браузеров;
8. Все ошибки пользовательского ввода и ошибочного указания параметров, необходимых для работы большинства методов, адекватно обрабатываются и, при необходимости, происходит автоматическое информирование пользователя о соответствующей ошибке;

Описание используемых алгоритмов:

1. «Шифр Цезаря» - процесс шифрования данных заключается в том, что каждая буква заменяется на другую, расположенную, например, на три символа левее (при ключе равном трём). Ключом в шифре Цезаря является величина сдвига строки алфавита. Ссылка: <http://www.hi-edu.ru/e-books/xbook1019/01/info.pdf>;
2. «XOR» - процесс шифрования данных заключается в том, что необходимо ввести ключ, который представляет собой набор бит. Загружаем файл побитно. Проводим операцию A[i] XOR B[i]. Операция XOR является ничем иным как логической операцией «исключающего ИЛИ». Так как длина ключа B гораздо меньше длины шифруемого сообщения (файла) А, то после того, как будут использованы все байты ключа, необходимо начать использование ключа заново. Ссылка: <http://www.hi-edu.ru/e-books/xbook1019/01/info.pdf>;
3. «Случайное перемешивание» - процесс шифрования данных заключается в том, что на вход подаются текстовые данные. Символы полученного текста перемешиваются случайным образом и полученный результат подаётся на выход;
4. «Блочная перестановка» - процесс шифрования данных заключается в том, что входной поток исходного текста делится на блоки, в каждом из которых выполняется перестановка символов согласно заданному ключу. Ключом является указанная последовательность номеров   
   символов блока, которые меняются местами. Ссылка: <https://www.intuit.ru/studies/courses/691/547/lecture/12373?page=5>;