

“Разработка программы по шифрованию и дешифрованию осмысленного текста с ключом”

Кондратюк В.С.

Руководитель: Атурина В.А.

Цель

Создать программу по шифрованию и дешифрованию осмысленного текста при помощи шифра с ключом.

Задачи

1. Выбор средств шифрования
 - 1.1. Изучение алгоритмов
 - 1.2. Выбор оптимального варианта
2. Реализация
 - 2.1. Алгоритм шифрования сообщения
 - 2.2. Алгоритм дешифрования сообщения
 - 2.3. Проверка на корректность введенных данных

Обзор шифров

Были рассмотрены 4 шифра с ключом:

- Виженера
- Гронсфельда
- Плейфера
- Вернама

Выбор оптимального варианта

Для реализации задачи был выбран шифр Вернама.

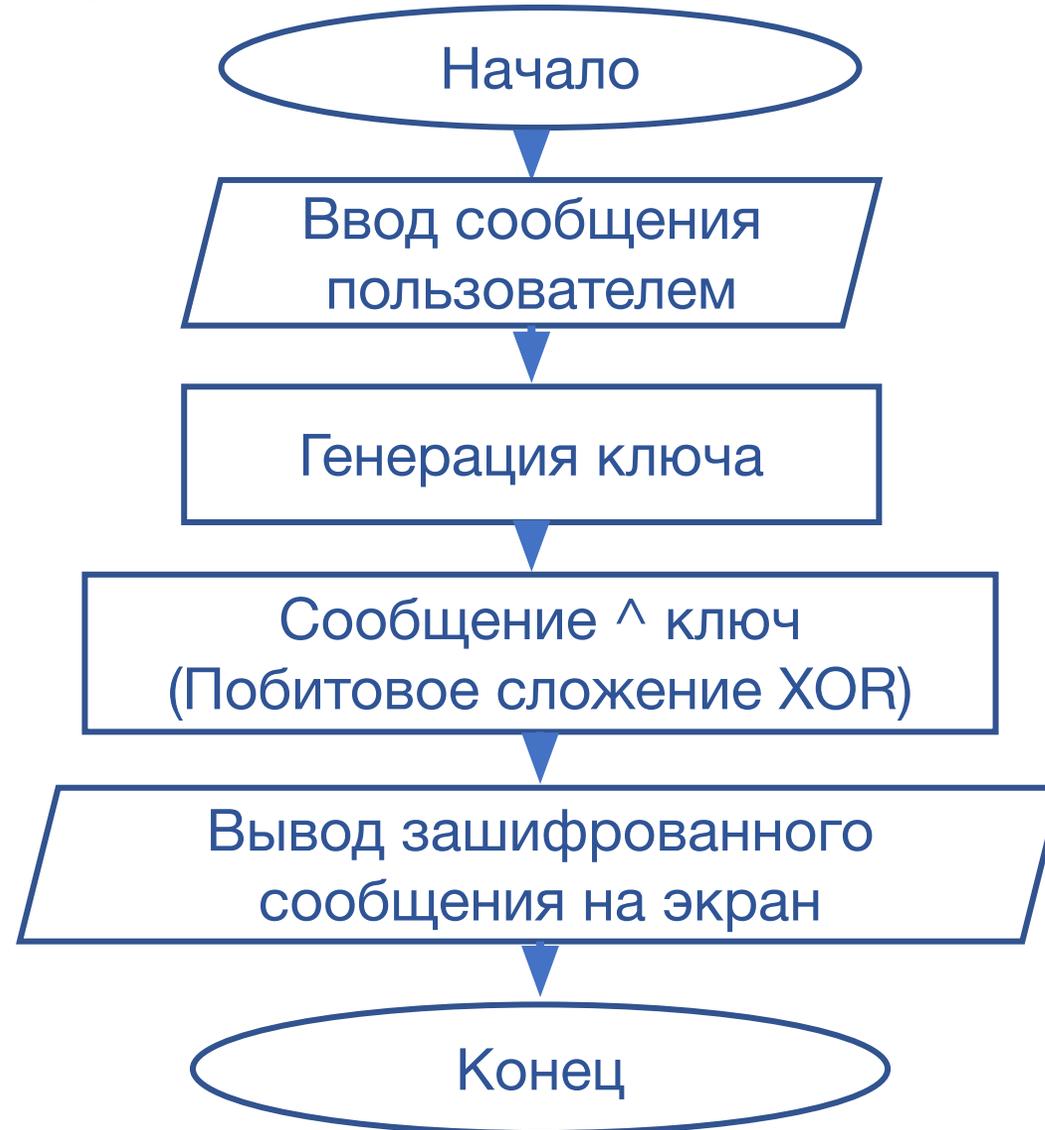
Плюсы шифра Вернама:

- не уходит много времени на процесс шифрования.
- обладает абсолютной безопасностью

Минусы шифра Вернама:

- длина ключа в шифре Вернама совпадает с длиной сообщения.
- ключ должен быть подобран абсолютно случайно.

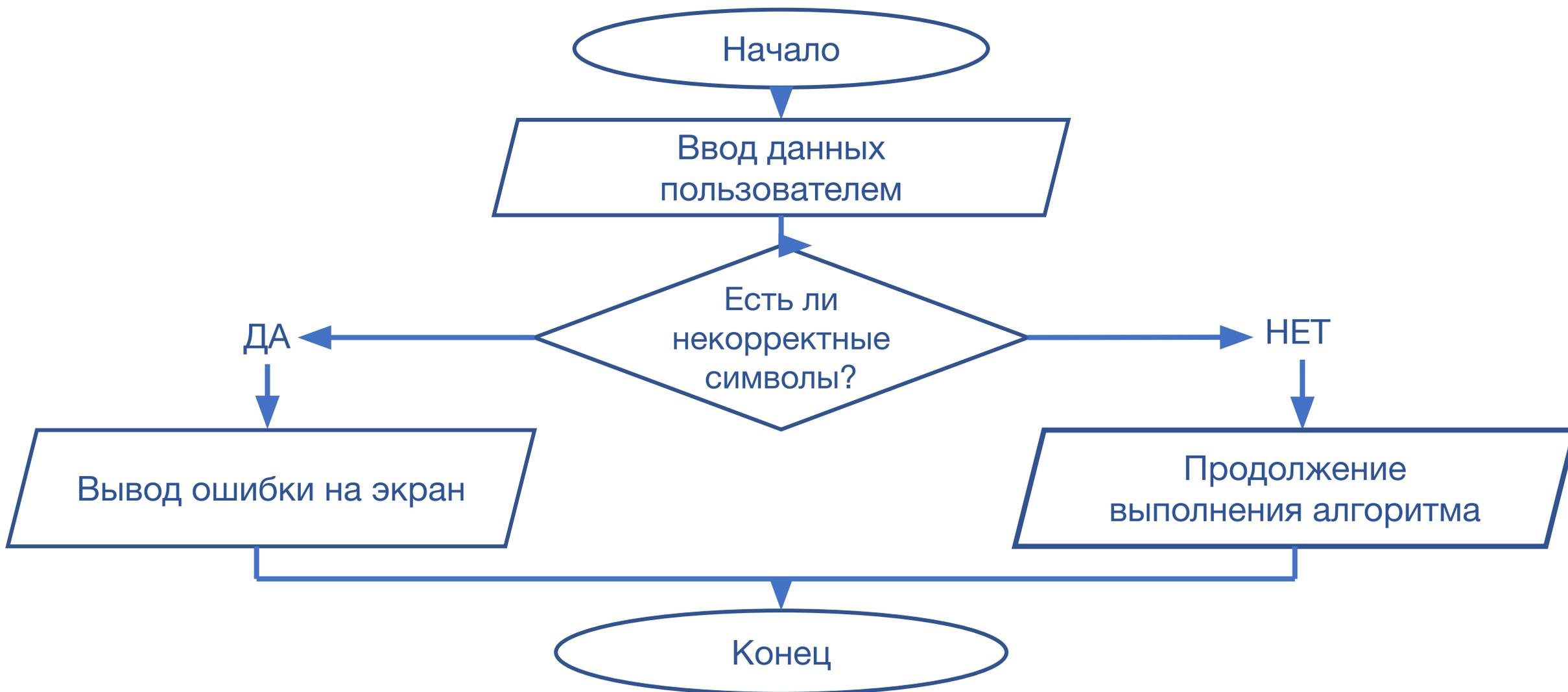
Алгоритм шифрования сообщения



Алгоритм дешифрования сообщения



Проверка на корректность введенных данных



Технические средства



HTML



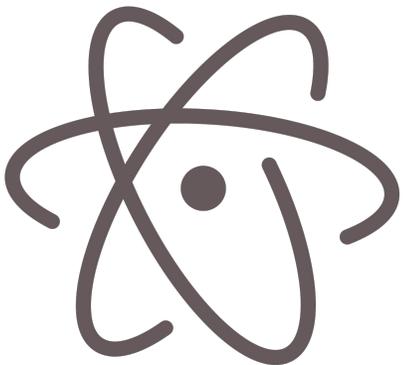
CSS



JS



Google Docs

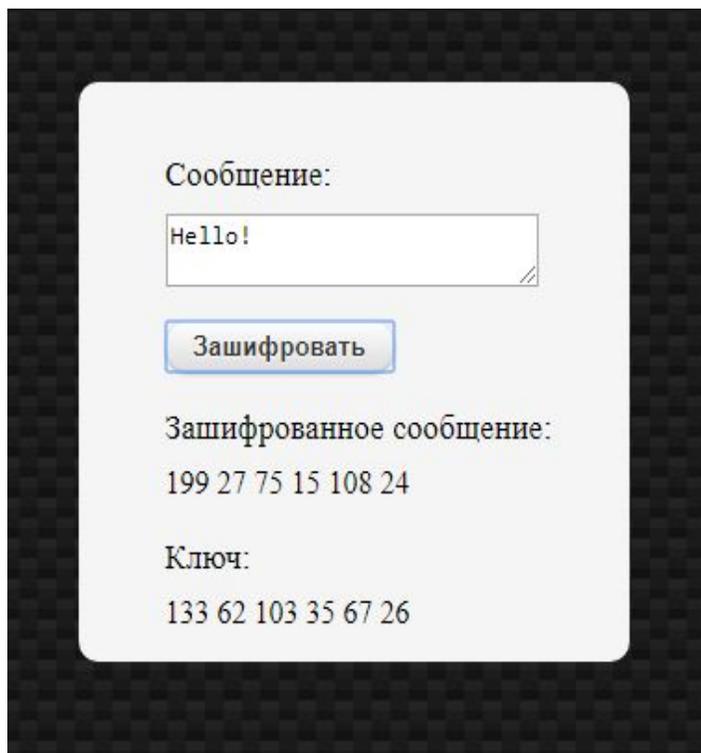


Google Drive

Итог

[Зашифровать сообщение](#)

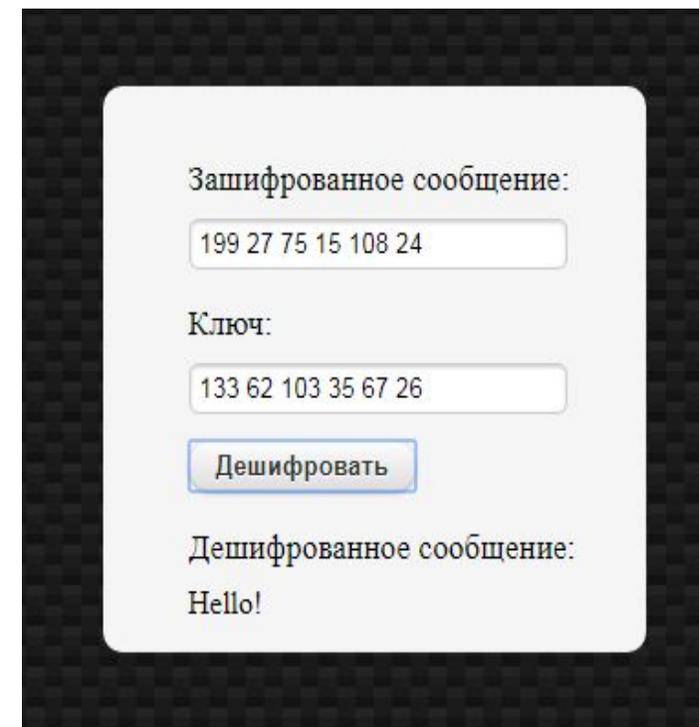
[Дешифровать сообщение](#)



Сообщение:

Зашифрованное сообщение:
199 27 75 15 108 24

Ключ:
133 62 103 35 67 26



Зашифрованное сообщение:

Ключ:

Дешифрованное сообщение:
Hello!



Спасибо за внимание!