

Разработка онлайн конвертера текста согласно алгоритмам шифрования “Cipher iT”

Воронин Андрей, 11 класс
Лицей НИУ ВШЭ 25.10.2018

Предпосылки

- Предметом исследования криптографии, в том числе, являются различные алгоритмы шифрования, как простые, так и сложные.
- Простые алгоритмы шифрования могут встречаться на соревнованиях по защите информации, в учебных проектах.
- Затраты времени на дешифрование вручную высоки, в связи с этим возникает необходимость в программном обеспечении.
- ПО может быть не всегда доступно, в таких случаях возможно использование удаленных сервисов, например веб-сайтов.

Актуальность и уникальность

Актуальность: применение сайта-конвертера уменьшает затраты времени на декодирование в условиях отсутствия программного обеспечения.

Уникальность: Отсутствие веб-сайтов с выбранными алгоритмами шифрования.

Выбранные алгоритмы шифрования: код Хемминга, код Элиаса, Сибирский шифр, табличные перестановки.

Цель и задачи проекта

Цель: создать веб-сайт, позволяющий шифровать и дешифровывать информацию согласно выбранным алгоритмам шифрования.

Задачи:

- создать удобный интерфейс;
- реализовать алгоритмы шифрования в обе стороны (возможность зашифровать и расшифровать текст).

Обзор алгоритмов шифрования

- **Шифр Элиаса:** алгоритм основан на переводе символов по таблице `ascii` в двоичный код и чередовании полученных чисел.
- **Шифр Хемминга:** алгоритм основан на группировке двоичного кода по ячейкам с проверкой истинности последовательности и переводе по таблице `ascii`
- **Сибирский Шифр:** алгоритм основан на вписывании текста в ступенчатый массив и считывании текста по его диагоналям
- **Табличные перестановки:** алгоритм основан на вписывании текста в таблицу и перестановку рядов и строк по некоторому ключу

Похожие проекты

Приведенные далее сайты связаны с кодированием информации, однако на представленных ресурсах отсутствуют алгоритмы шифрования, рассмотренные в нашем проекте

1. ASCII конвертер - <http://ascii.shadowservants.ru/>
2. Калькулятор шифра Цезаря - <https://planetcalc.ru/1434/>

ASCII конвертер

ASCII конвертер Made by JohnN@shadow servants.ru

Да! Это ASCII конвертер, который поддерживает вторую(русскую) половину таблицы ASCII. Можешь решать задачи сколько душа желает!

Вводи сюда данные для конвертирования

Введите числа через пробел

Input:

207 224 241 245 224 235 238 247 234 224

Как переводим ?

ASCII -> Строка

Output:

Сообщение

Основная функция данного сайта – конвертация ascii кода в текст и обратно. Несмотря на главную функцию, отличную от нашего проекта, присутствует сходство в интерфейсе (окна ввода, вывода, смена режима)

Калькулятор шифра цезаря

The screenshot shows the 'Шифр Цезаря' (Caesar Cipher) calculator on the PLANETCALC website. The interface includes a header with the site name and navigation links, a sidebar with social media icons, and a main content area. The main area has a large text input field for the 'Входной текст' (Input text) containing 'Чу, я слышу пушек гром!'. Below the input is a dropdown menu for 'Алфавит' (Alphabet) set to 'Русский'. A prominent orange 'РАССЧИТАТЬ' (Calculate) button is centered. Below the button, there is a table showing the 'Преобразованный текст' (Transformed text) for different shift values.

Преобразование	Преобразованный текст
ROT0	Чу, я слышу пушек гром!
ROT1	Шф. а тмьшф офшёл дспн!

Основная функция данного сайта – изменение текста по правилам шифра Цезаря. Несмотря на то, что эта задача связана с кодированием информации, алгоритмы шифрования нашего проекта и данного различны.

Средства реализации

- html + css
- JavaScript + JQuery

HTML



CSS



JS



Полученные результаты (Главная страница)

[Главная](#)[Хеминг](#)[Элиас](#)[Таблицы](#)[Сибирь](#)

CIPHER IT

На данном сайте собраны основные алгоритмы шифрования, изучаемые в "ЧУ ДО Школа Программистов", такие как шифр Хеминга, Элиаса, Сибирский шифр и табличные перестановки. Сайт создан для уменьшения затрат времени на дешифрование вручную. Алгоритмы шифрования работают в обе стороны - как дешифрование, так и шифрование. Приятного использования!

РЕЖИМЫ

[Хеминг](#)[Элиас](#)[Таблицы](#)[Сибирь](#)

Полученные результаты (Страница конвертера)

Главная

Хеминг

Элиас

Таблицы

Сибирь

Шифр Хеминга

Опция:

Расшифровать

Выполнить

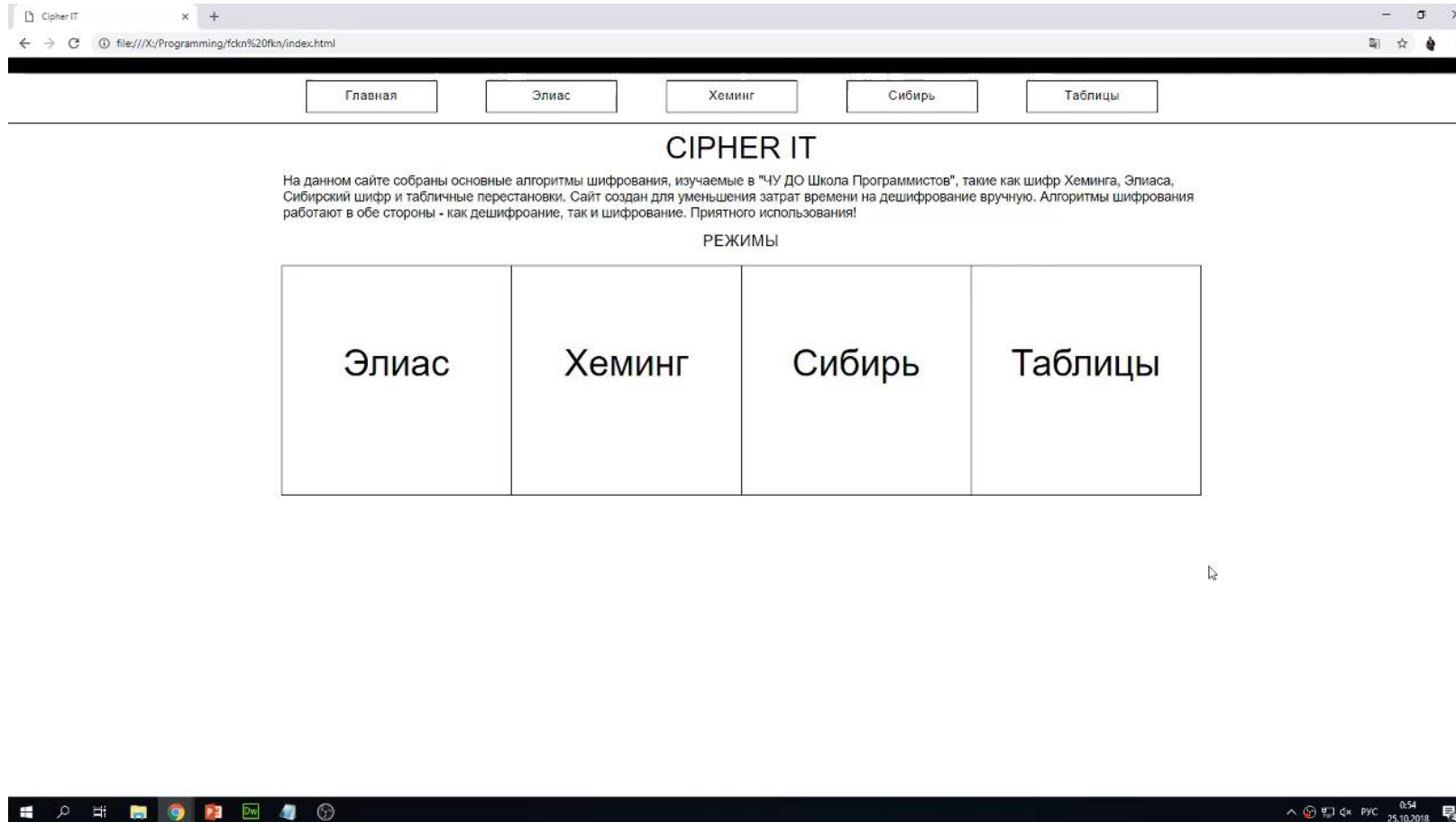
1010 0110 0010 0010 1001
0100 1001

Зы!

Описание:

Берём задачу:
1010 0110 0010 0010 1001 0100 1001
Первый знак - начало чередования. Отделяем и запоминаем его.
1 : 010 0110 0010 0010 1001 0100 1001
Остальное рабиваем на фрагменты Элиаса. Напоминаю: Количество нулей перед единицей=количеству цифр после единицы, принадлежащих данному сегменту.
010 011 0001000 1 010 010 1 00100 1
Убираем лишние нули:
10 11 1000 1 10 10 1 100 1

Полученные результаты (Видео)



Заключение

В рамках данного проекта удалось разработать веб-сайт с использованием четырех алгоритмов шифрования, реализующий поставленную задачу. На данном этапе работа завершена, но при необходимости возможно расширение функционала путем добавления новых шифров.

ИСТОЧНИКИ:

- <https://my.informatics.ru> – Школа Программистов
- <https://stackoverflow.com> – Stack Overflow
- <https://developer.mozilla.org/ru/> - MDN – Mozilla Developers Network
- <https://www.w3schools.com> – W3schools