МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №4:**

по дисциплине «Криптографические методы защиты информации»

Тема «ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

Ход работы

Приложение было разработано на NodeJS. В своем приложении согласно варианту 13 я использовала алфавит английского языка, а так же два способа шифрования: шифр на основе аффинной системы подстановок Цезаря, где a = 6, b = 7 и таблица Трисемуса, где ключевое слово – security.

Здание №1

В данном задании я разработала шифр на основе аффинной системы подстановок Цезаря, где a = 6, b = 7. Данный алгоритм проходится по каждой букве строки, запоминает ее значение и индекс, после чего, он вычисляет новую позицию по формуле: . После вычисления новой позиции, мы находим букву в алфавите соответствующую этому индексу и заменяем ей старую букву.



Рисунок 1 — реализация шифра на основе аффинной системы подстановок Цезаря

Задание №2

Здесь я разработала дешифратор для шифра на основе аффинной системы подстановок Цезаря. Для дешифратора я использовала формулу, представленную в учебнике: . Для нахождения числа, обратного числу *a* по модулю *N* я использовала расширенный алгоритм Евклида. Код представлен на рисунках 2 и 3.

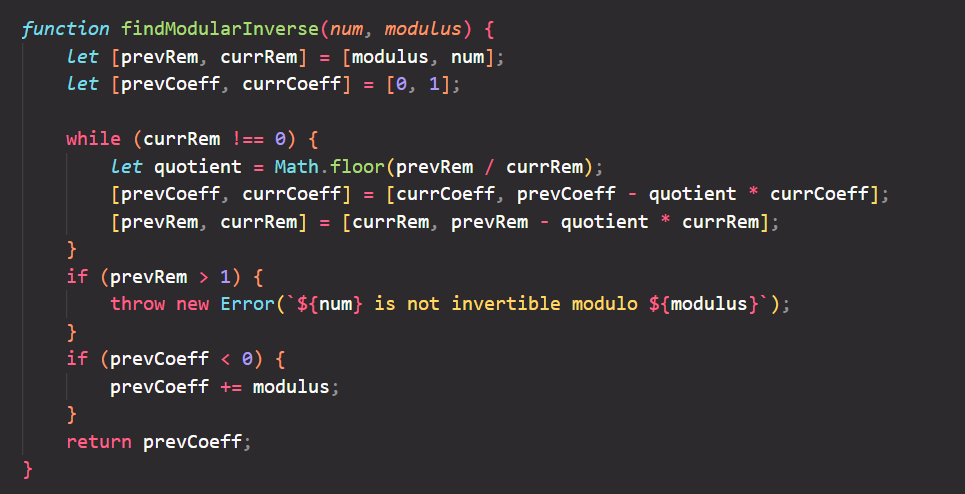


Рисунок 2 — нахождение числа, обратного числу num по модулю moduls

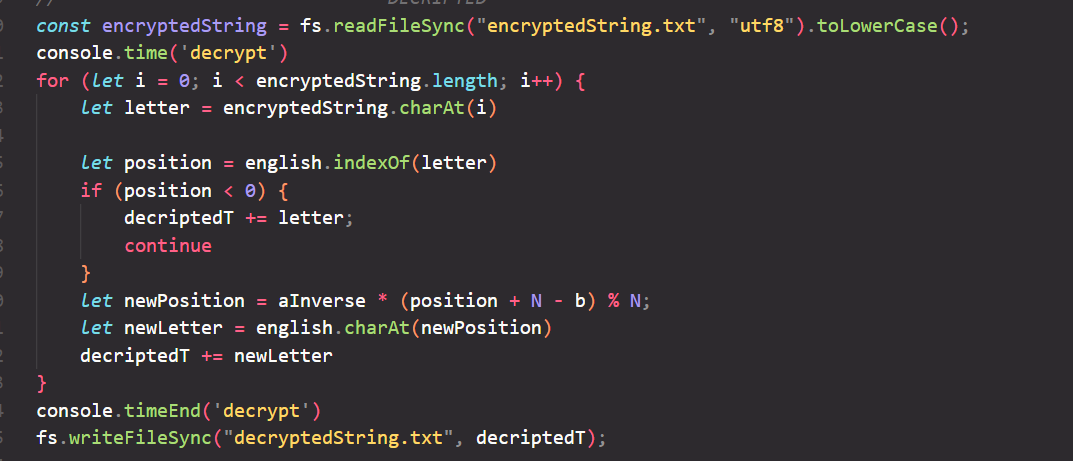
****

Рисунок 3 — дешифратор для шифра на основе аффинной системы подстановок Цезаря

Задание №3

В данном задании я разработала шифр на основе таблицы Трисемуса, ключевое слово – security. Для реализации данного алгоритма надо было разработать код для создания таблицы Трисемуса с ключевым словом security. Данный код приведен на рисунке 4.



Рисунок 4 — код для создания таблицы Трисемуса с ключевым словом security

Полученная таблица представлена на рисунке 5.

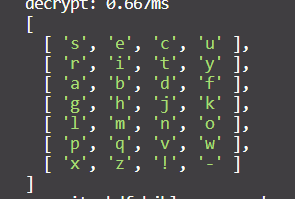


Рисунок 5 — таблица Трисемуса с ключевым словом security

Далее я разработала код для шифрования, который представлен на рисунке 6.

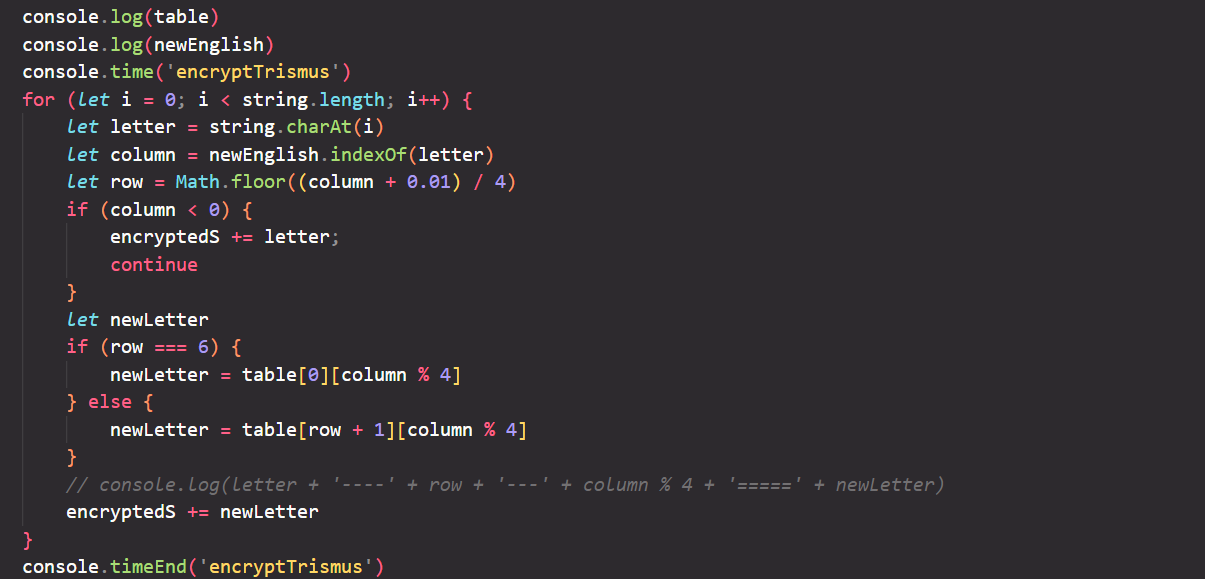


Рисунок 6 — реализация шифрования по таблице Трисемуса

Задание №4

В этом задании я разработала дешифратор, в котором также использовала таблицу Трисемуса, полученную в предыдущем задании. Код представлен на рисунке 7.



Рисунок 7 — реализация дешифратора по таблице Трисемуса

Далее был произведен анализ гистограмм. Сами гистограммы представлены на рисунках 8-11. Гистограммы соответствующие частоте появления букв при шифровании и дешифровании текста с помощью аффинной системы подстановок Цезаря представлены на рисунках 8, 9.

Рисунок 8 — Частота появления букв при шифровании

Рисунок 9 — Частота появления букв при дешифровании

Гистограммы соответствующие частоте появления букв при шифровании и дешифровании текста с таблицей Трисемуса, ключевое слово – security представлены на рисунках 10, 11 соответственно.

Рисунок 10 — Частота появления букв при шифровании

Рисунок 11 — Частота появления букв при дешифровании

Далее будет приведен график зависимостей количества символов от времени при разном способе шифрования и дешифрования. График представлен на рисунке 12.

В данном графике линия оранжевого и серого цвета соответствуют способу шифрования и дешифрования с помощью шифра на основе аффинной системы подстановок Цезаря. А линии синего и желтого цвета – способу шифрования и дешифрования с помощью таблицы Трисемуса соответственно.

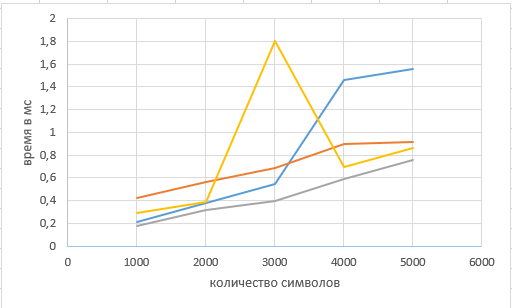


Рисунок 12 — График зависимостей:

Оранжевый – шифрование шифра на основе аффинной системы подстановок Цезаря;

Синий – шифрование с помощью таблицы Трисемуса;

Серый – дешифрование на основе аффинной системы подстановок Цезаря;

Желтый – дешифрование с помощью таблицы Трисемуса.