Лабораторна робота №2

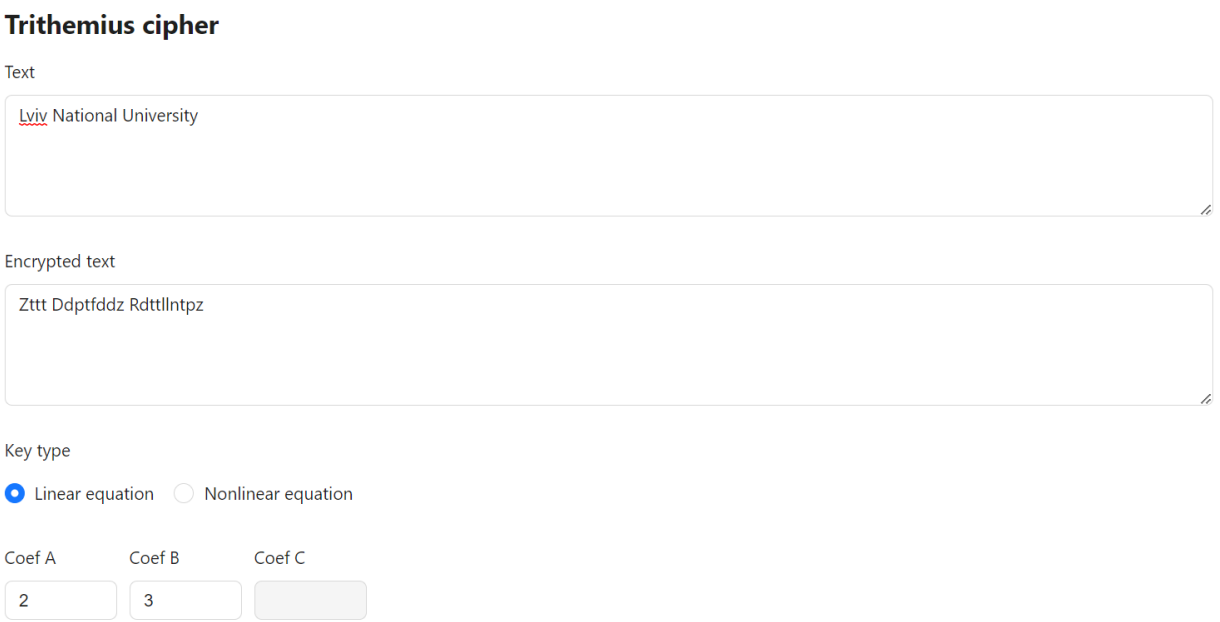
Виконав: Вавринович Михайло ПМІ-33

Тема: Шифр Тритеміуса

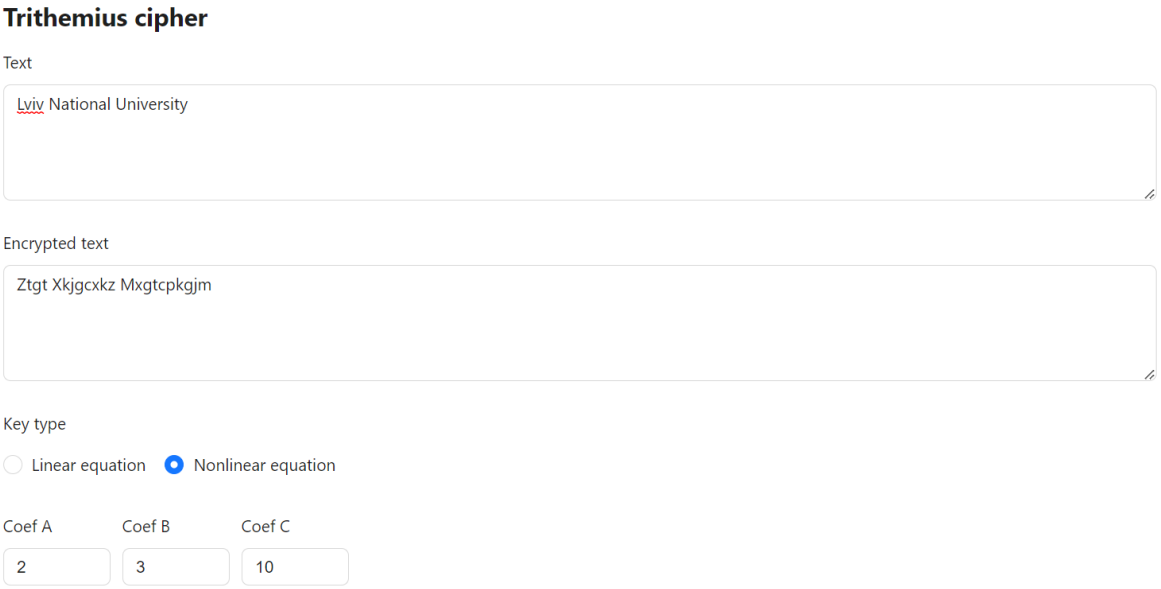
Мета: Розробити криптосистему на основі шифру Тритеміуса

Хід роботи

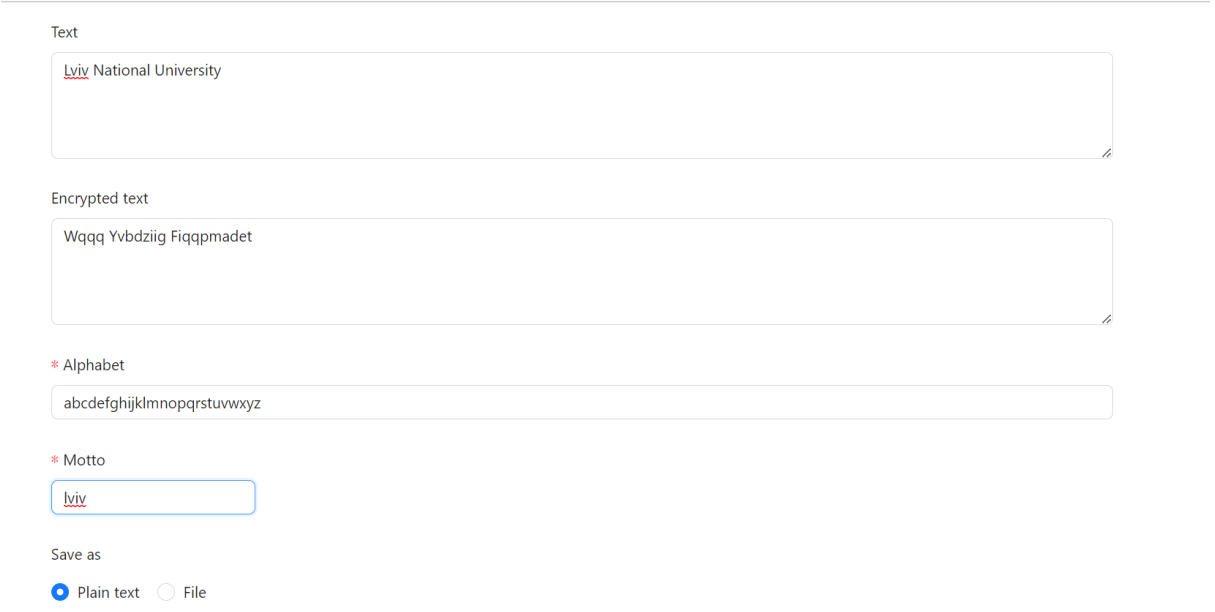
1. Модифікував інтерфейс криптографічної системи симетричного шифрування з лабораторної роботи №1, забезпечивши можливість використання в якості ключа:
    a. 2-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування



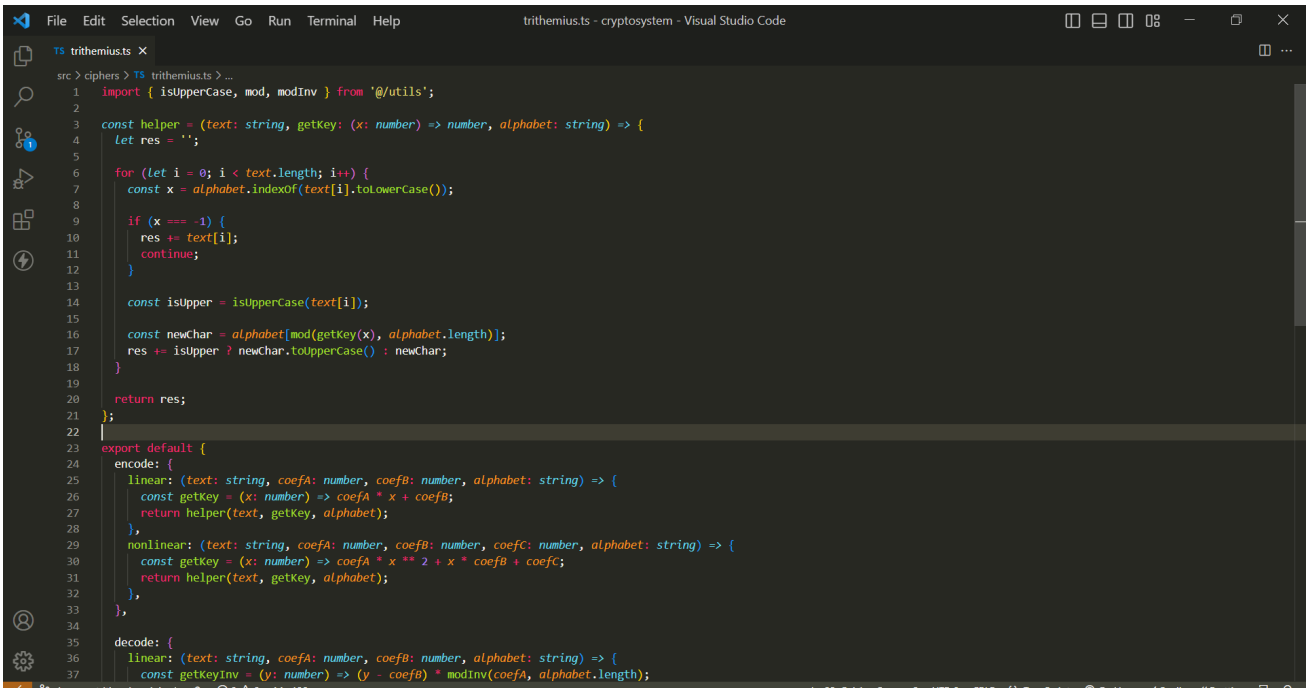
b. 3-вимірного вектору для зберігання коефіцієнтів нелінійного рівняння шифрування

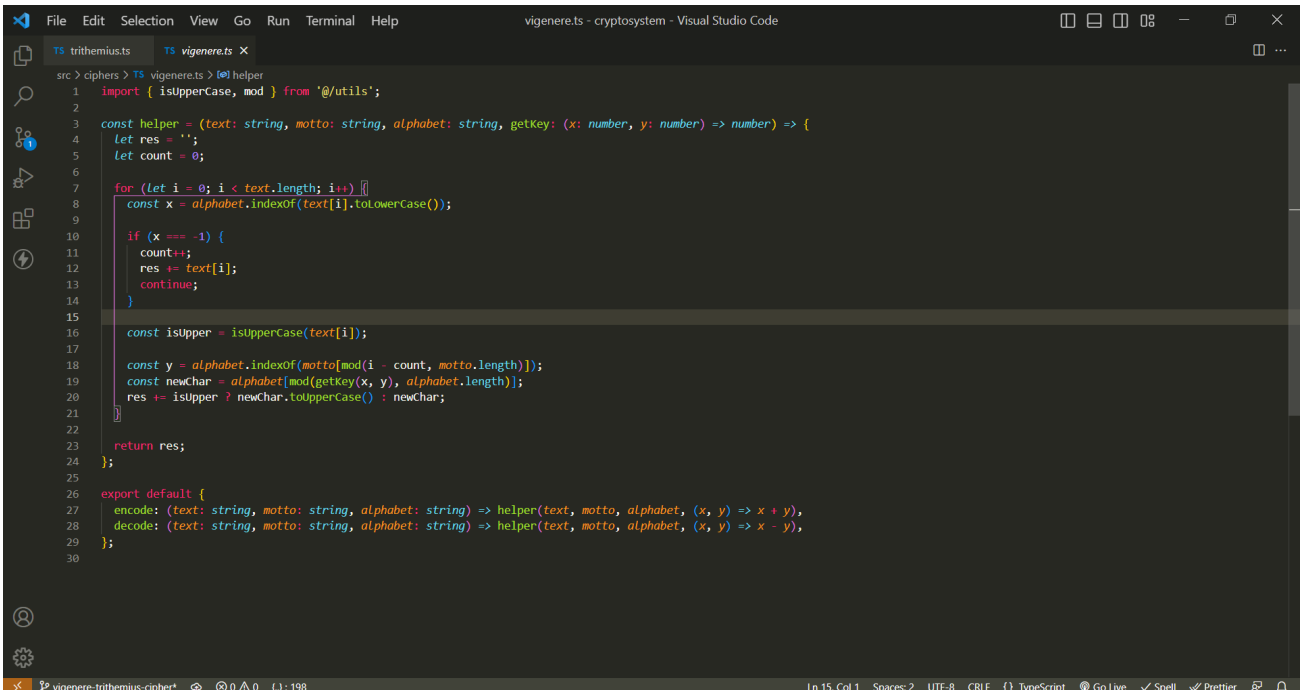


c. Текстового рядка (гасла)

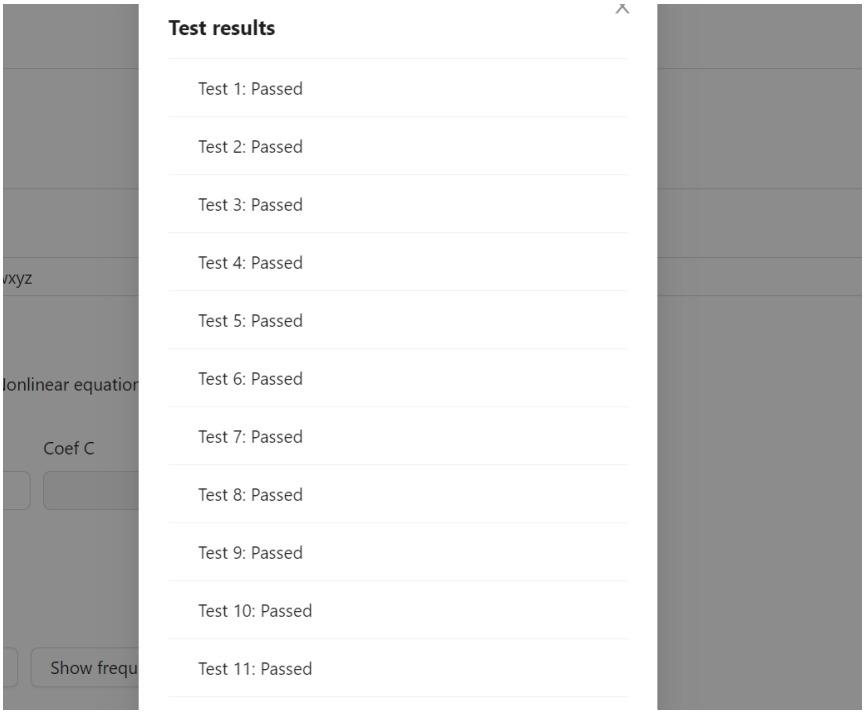


2. Доповнив систему класів з лабораторної роботи №1 класами та методами, необхідними для реалізації симетричного шифрування методом Тритеміуса, передбачивши в них методи валідації ключа, валідації шифрування і розшифрування даних.

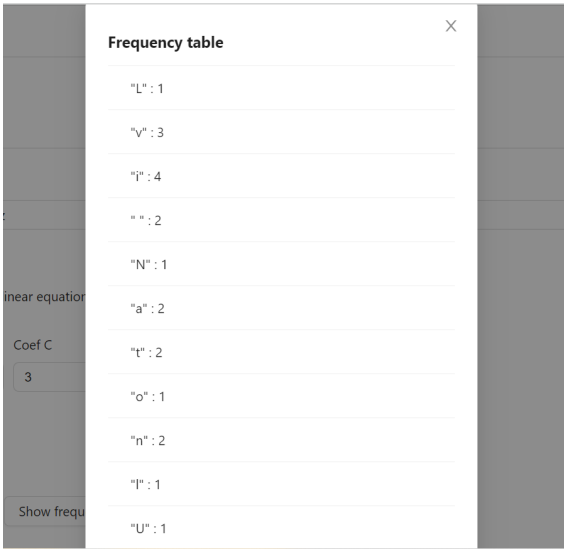




3. Виконав тестування роботи системи.



4. Застосував частотні таблиці для української та англійської мов для атаки.



Висновок: я розробив криптосистему на основі шифру Тритеміуса.