Львівський національний університет імені Івана Франка

Факультет прикладної математики та інформатики

**Математичні основи криптології**

**Лабораторна робота №2**

**Шифр Тритеміуса**

Виконав:

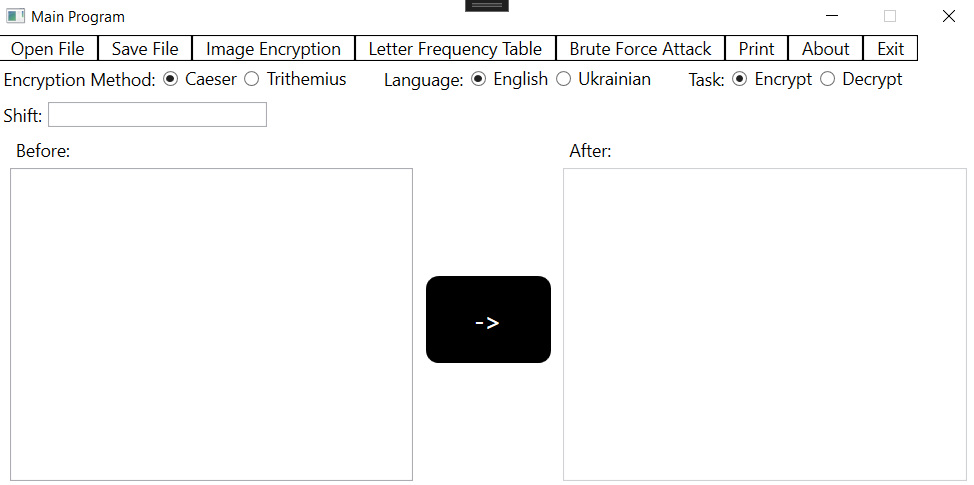
Студент групи ПМі-33

Тимчишин Ярема

Львів 2024

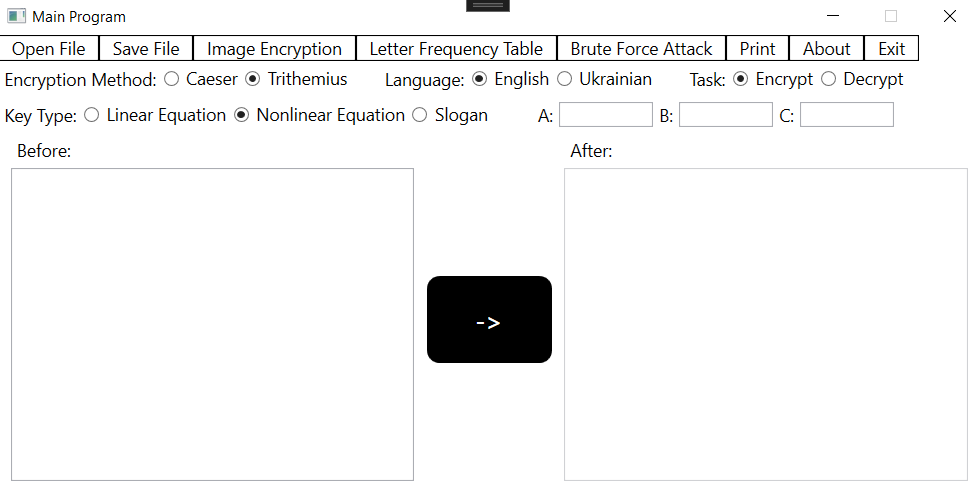
Інтерфейс криптографічної системи

* **Головне вікно:**



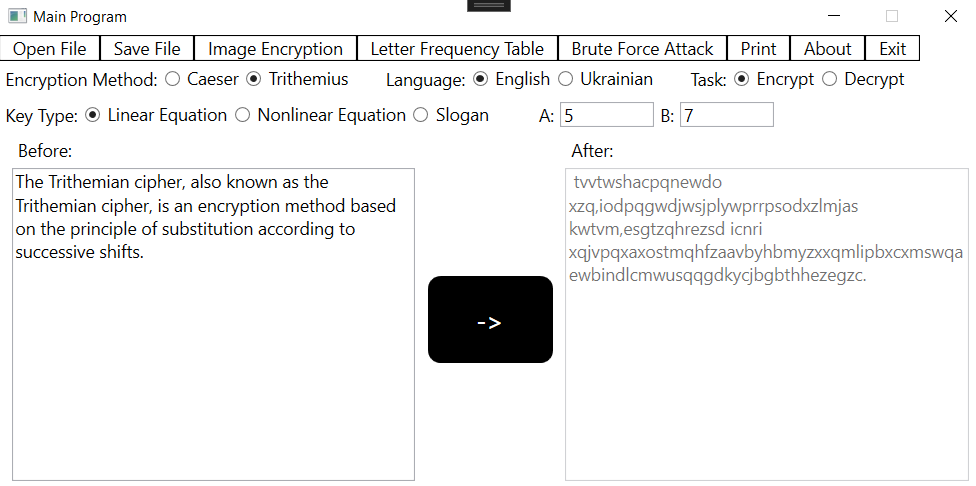
* + При вибору шифру Тритеміуса з’являються відповідні поля для цього методу: “Key Type”, в якому можна вибрати завдяки якому ключу буде відбуватися шифрування або дешифрування. Ключ може бути заданий лінійним рівнянням (k=Ap+B), нелінійним рівнянням (k=Ap2+Bp+C) та гаслом. І відповідно до вибраного подання ключа, будуть з’являтися відповідні комірки: “A”(поле для введення коефіцієнту А), “B”(поле для введення коефіцієнту B), “С”(поле для введення коефіцієнту C) та “Slogan”(поле для введення гасла). На кожному з цих полів стоїть відповідна валідація.



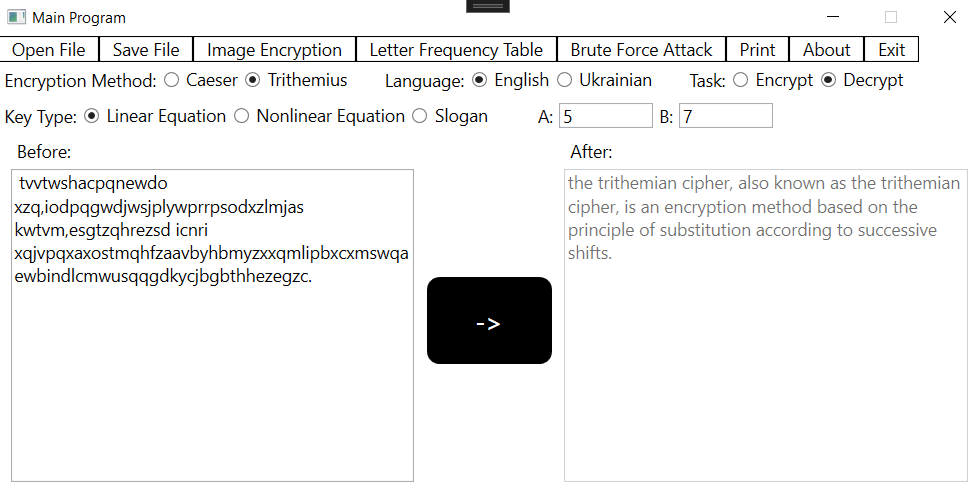




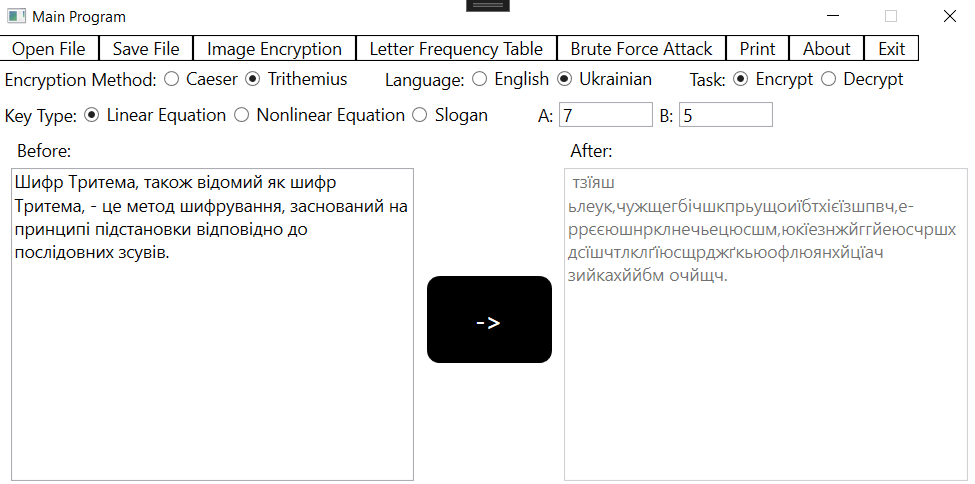
* **Лінійне шифрування англійською мовою:**



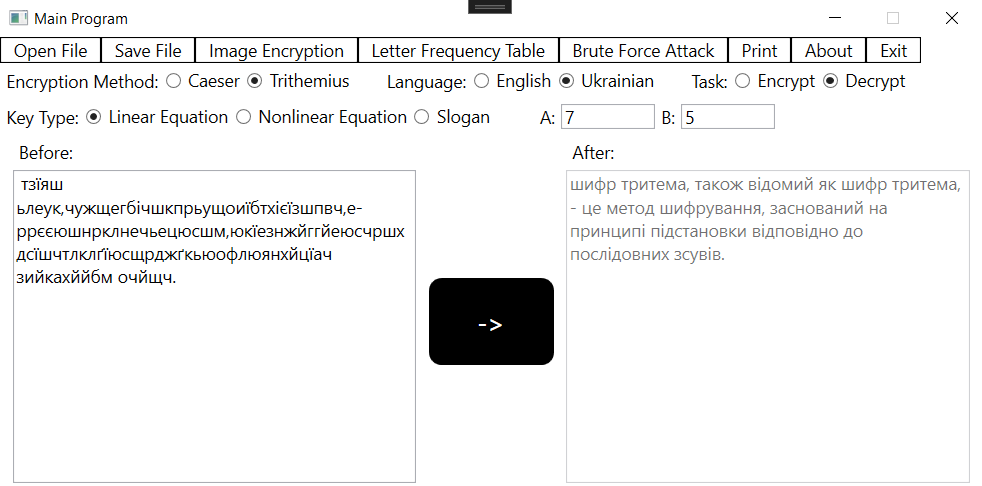
* **Лінійне дешифрування англійською мовою:**



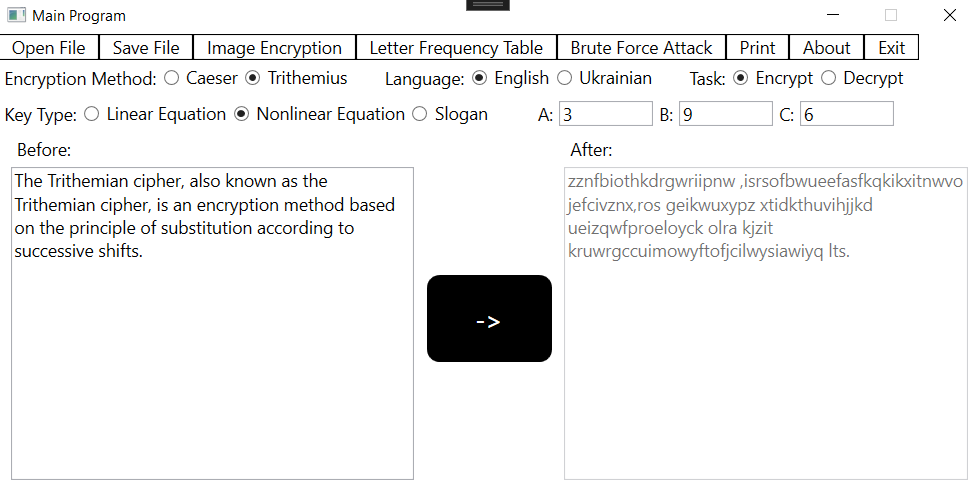
* **Лінійне шифрування українською мовою:**



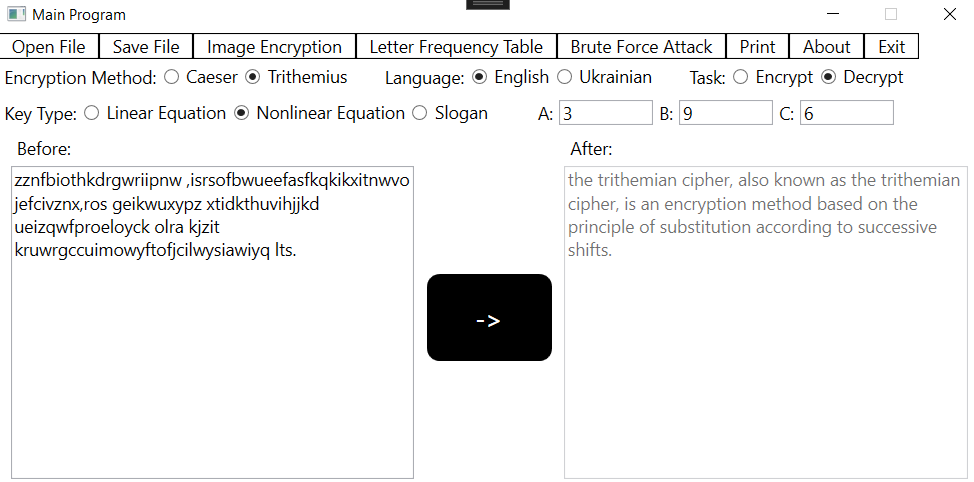
* **Лінійне дешифрування українською мовою:**



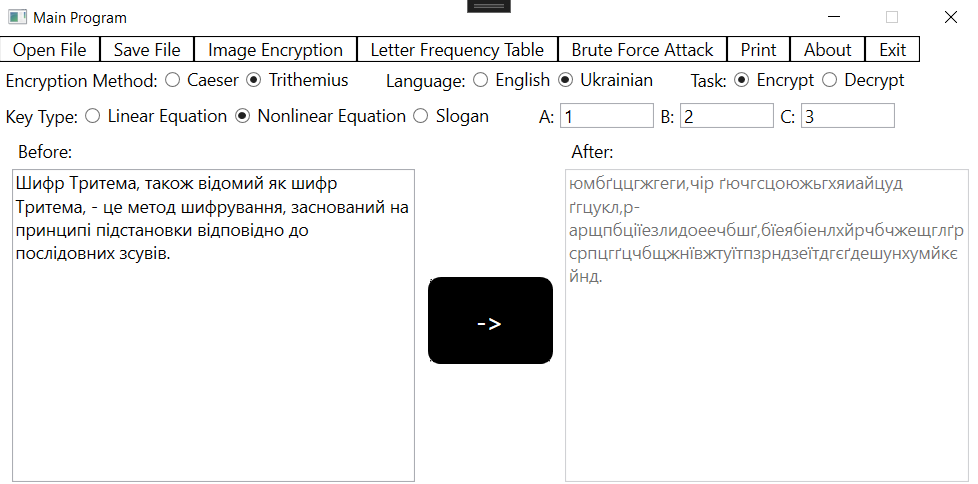
* **Нелінійне шифрування англійською мовою:**



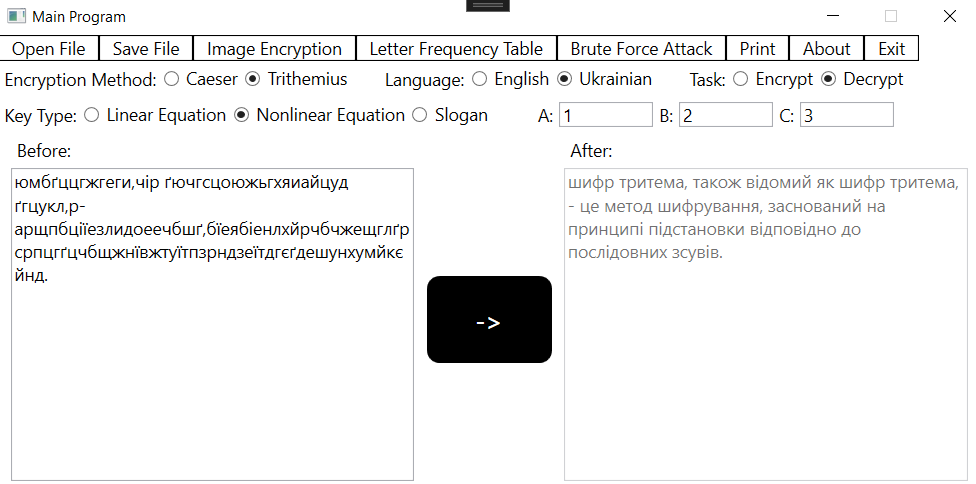
* **Нелінійне дешифрування англійською мовою:**



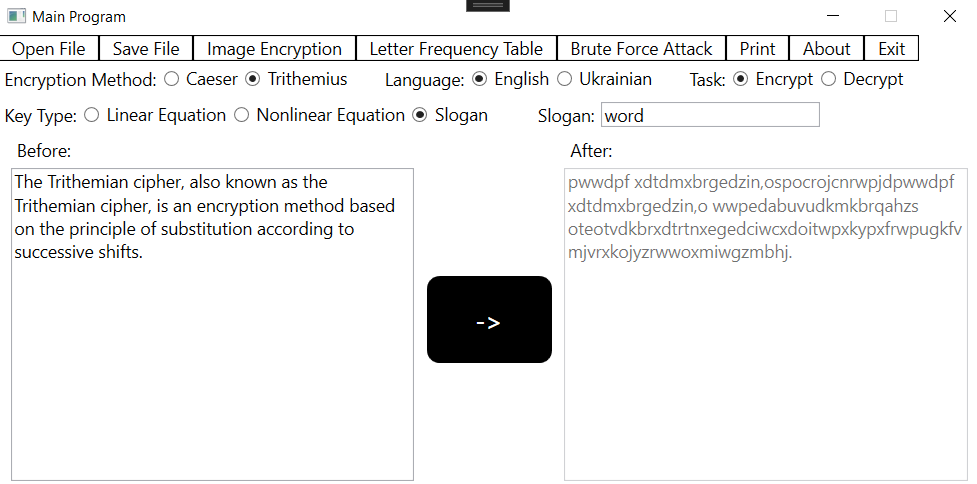
* **Нелінійне шифрування українською мовою:**



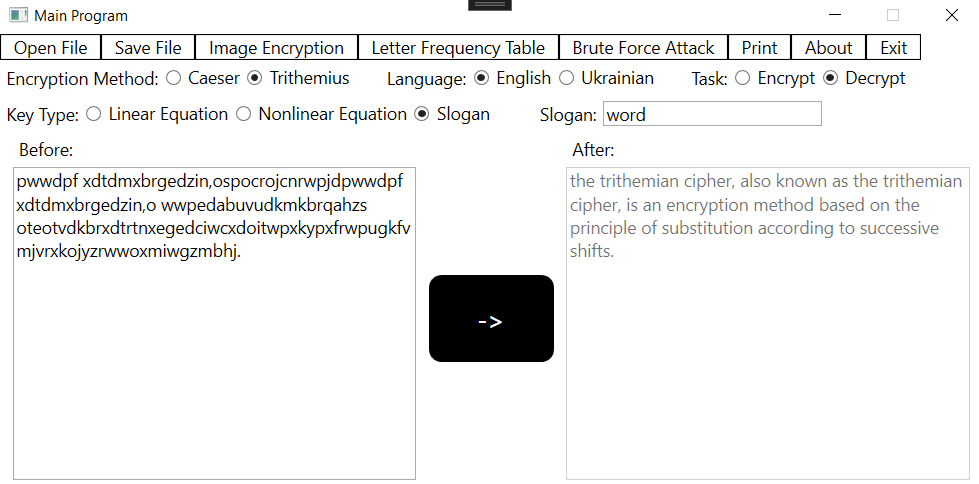
* **Нелінійне дешифрування українською мовою:**



* **Шифрування гаслом англійською мовою:**



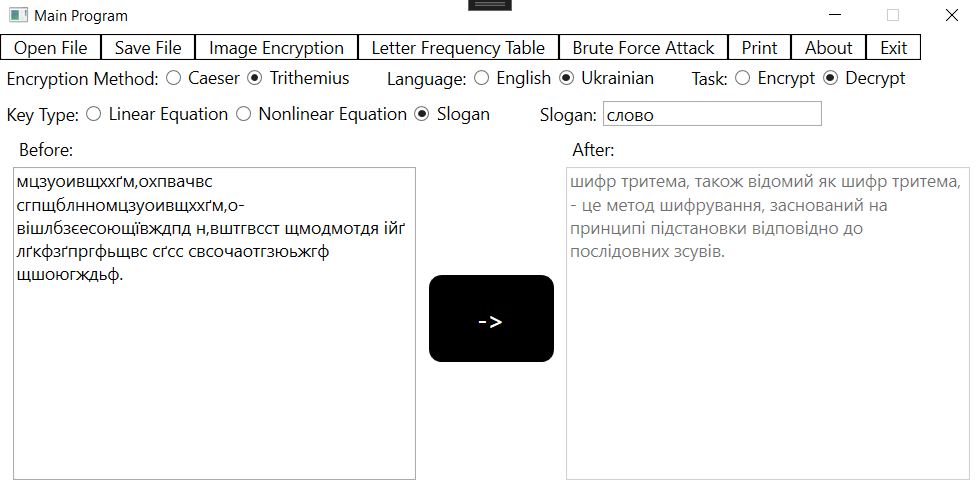
* **Дешифрування гаслом англійською мовою:**



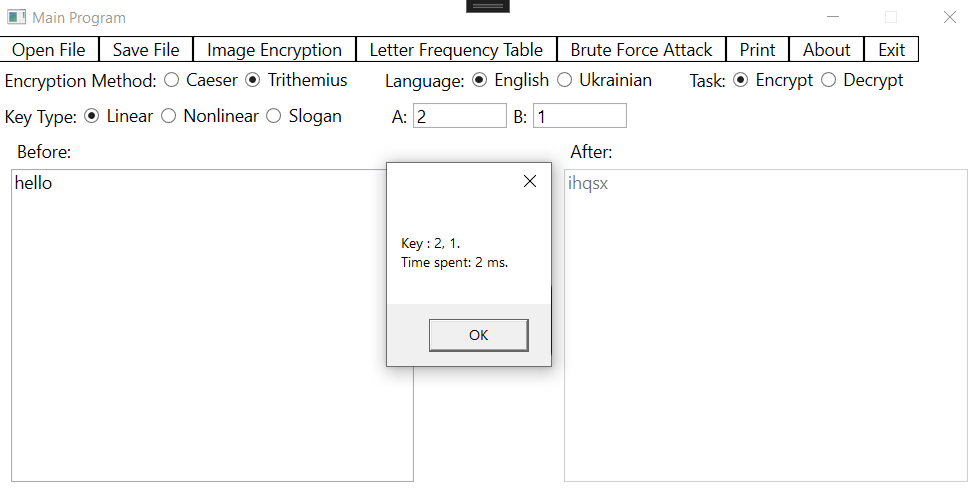
* **Шифрування гаслом українською мовою:**



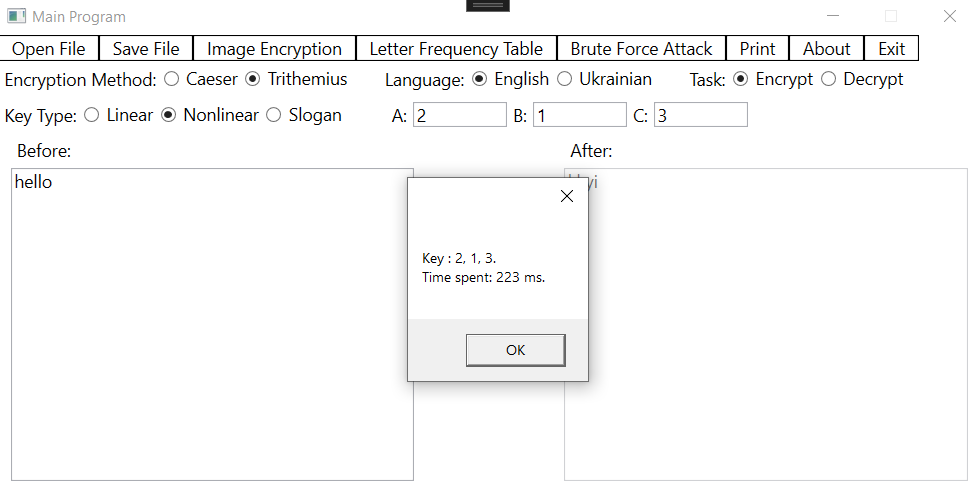
* **Дешифрування гаслом українською мовою:**



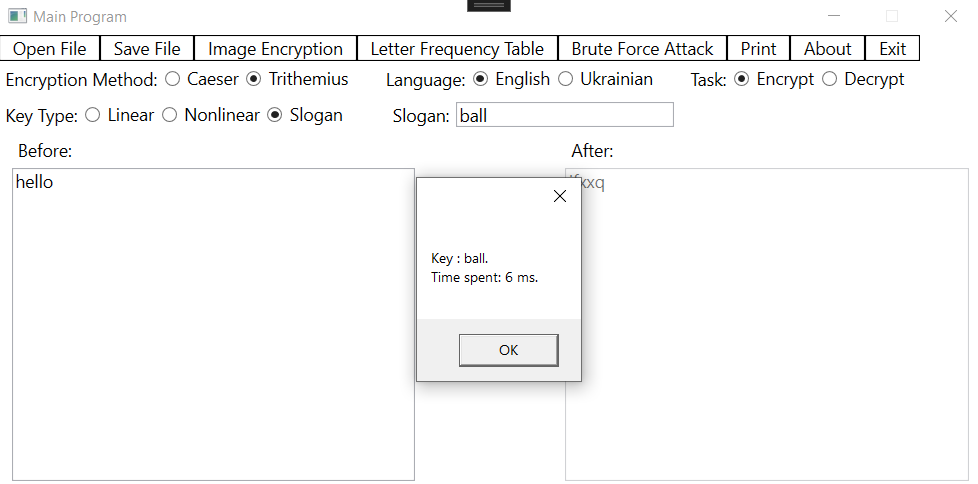
* **Лінійна атака англійською мовою:**



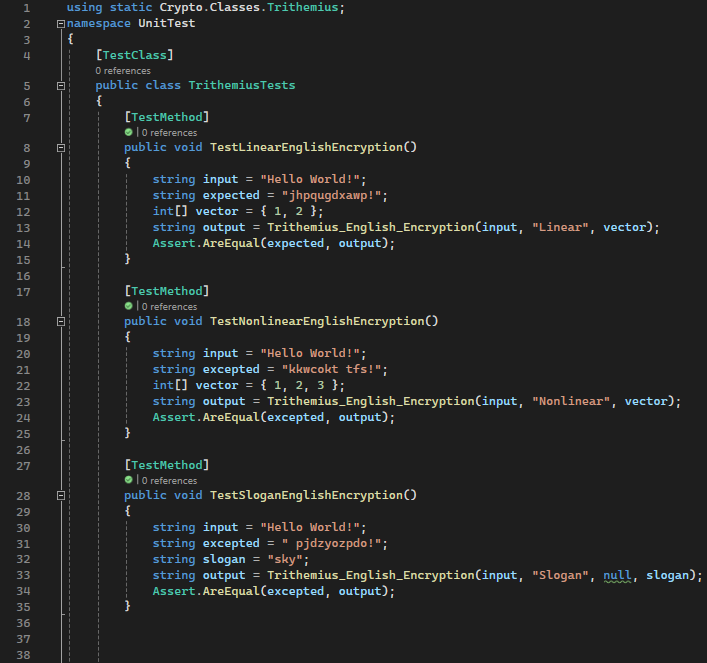
* **Нелінійна атака англійською мовою:**



* **Атака гаслом англійською мовою:**



Тестування програми

















Результати тестів

