МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Звіт із**

**Теорія імовірності та математичної статистики**

**Лабораторна робота №2**

з курсу «Математичні основи криптології»

Виконав:

Готюк Максим

Група Пмі-33

Оцінка \_\_\_

2025

Тема: Шифр Тритеміуса

Мета: Розробити криптосистему на основі шифру Тритеміуса

**Постановка завдання:**

1. Модифікуйте інтерфейс криптографічної системи симетричного шифрування з лабораторної роботи №1, забезпечивши можливість використання в якості ключа:

1. 2-вимірного вектору для зберігання коефіцієнтів лінійного рівняння шифрування,
2. 3-вимірного вектору для зберігання коефіцієнтів нелінійного рівняння шифрування, c. Текстового рядка (гасла).

2. Доповніть 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. Виконайте тестування роботи системи.

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

5. Доповніть систему модулем активної атаки на шифр Тритеміуса, який би забезпечував знаходження ключа шифрування у випадку, коли зловмиснику вдалось отримати пару повідомлень «незашифроване – зашифроване».

## **Програмна реалізація**

Для розробки інтерфейсу веб-застосунку я скористався мовою C# та фреймворком ASP.NET Core MVC 9.0.

Додана можливість обрати шифр Тритеміуса.

A screen shot of a computer

AI-generated content may be incorrect.

Доступна можливіть енкрипції та декрипції з лінійним, нелінійним ключами та гаслом.

A screenshot of a computer

AI-generated content may be incorrect.

Атака реалізована для знаходження ключа за фрагментом розшифрованого тексту:  
A screenshot of a computer

AI-generated content may be incorrect.

Для кожного файлу доступні частотні таблиці:  
A screenshot of a computer

AI-generated content may be incorrect.

**Тестування системи:**Написані такі Юніт тести:

**A screenshot of a computer

AI-generated content may be incorrect.**

* **Index\_ReturnsViewWithFileContent**:
  + **Час виконання**: 0.0 мс.
  + **Опис**: Перевіряє, чи повертається представлення з вмістом файлу при виклику методу Index.
* **Index\_ReturnsNotFound\_WhenFileDoesNotExist**:
  + **Час виконання**: 0.0 мс.
  + **Опис**: Перевіряє, чи повертається статус "Не знайдено" (404), коли файл не існує.
* **EncryptLinear\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 2.0 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після шифрування лінійним методом.
* **EncryptQuadratic\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 3.0 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після шифрування квадратичним методом.
* **EncryptKeyword\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 4.0 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після шифрування з використанням ключового слова.
* **DecryptLinear\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 5.0 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після розшифрування лінійним методом.
* **DecryptQuadratic\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 2.0 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після розшифрування квадратичним методом.
* **DecryptKeyword\_UpdatesFileContent\_AndReturnsView**:
  + **Час виконання**: 93 мс.
  + **Опис**: Перевіряє, чи оновлюється вміст файлу та повертається представлення після розшифрування з використанням ключового слова.
* **Attack\_ReturnsViewWithKey\_WhenSuccessful**:
  + **Час виконання**: 79 мс.
  + **Опис**: Перевіряє, чи повертається представлення з ключем, коли атака на шифр успішна.
* **Attack\_ReturnsViewWithError\_WhenKeyNotFound**:
  + **Час виконання**: 2.0 мс.
  + **Опис**: Перевіряє, чи повертається представлення з повідомленням про помилку, коли ключ не знайдено під час атаки.

Ці тести перевіряють різні аспекти функціональності, включаючи шифрування, розшифрування та атаку на шифр.

**Висновок**  
У ході виконання лабораторної роботи було розроблено криптографічну систему на основі шифру Тритеміуса, яка підтримує шифрування та розшифрування текстових українською та англійською мовами. Система включає інтерфейс для зручного управління файлами, функції шифрування/розшифрування, активну, а також побудову частотних таблиць для аналізу текстів.