МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Звіт із**

**Шифрування з відкритим ключем на основі задачі рюкзака**

**Лабораторна робота №4**

з курсу «Математичні основи криптології»

Виконав:

Готюк Максим

Група Пмі-33

Оцінка \_\_\_

2025

Тема: Шифрування з відкритим ключем на основі задачі рюкзака

**Постановка завдання:**

1. ﻿﻿﻿Відшукайте в Інтернет-ресурсах чисельний приклад з використання «рюкзачного» алгоритму (наприклад, в Вікіпедії ) та опрацюйте його.
2. ﻿﻿﻿Розробіть інтерфейс криптографічної системи для шифрування з використанням задачі рюкзака, передбачивши окремий діалог для формування відкритого ключа.
3. ﻿﻿﻿Розробіть методи, які б забезпечували:

а. Генерацію пари «відкритий -закритий» ключі.

b. Шифрування з використанням відкритого ключа.

с. Розшифрування з використанням закритого ключа. При цьому

значення t-1 вважати відомим.

## **Програмна реалізація**

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

Додана можливість обрати шифр на основі задачі рюкзака.

A screen shot of a computer

AI-generated content may be incorrect.

Доступна можливіть генерації публічного та приватного ключів, енкрипції та декрипції.

Screens 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.

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