МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Звіт із**

**Шифрування RSA**

**Лабораторна робота №5**

з курсу «Математичні основи криптології»

Виконав:

Готюк Максим

Група Пмі-33

Оцінка \_\_\_

2025

Тема: Шифрування з відкритим ключем.

Мета: Реалізувати криптосистему RSA з використанням бінарного алгоритму піднесення до степеня за модулем

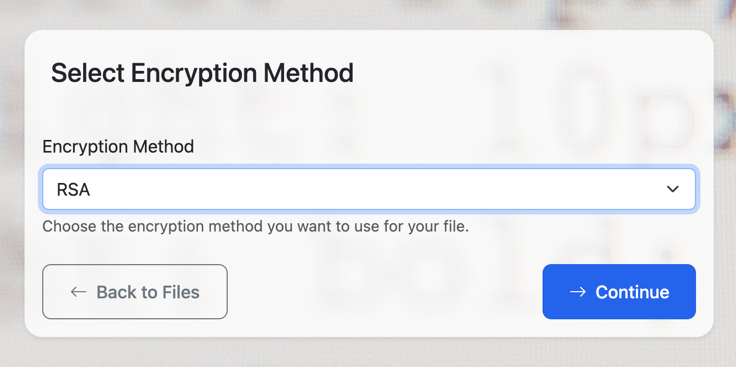
**Постановка завдання:**

1. Відшукайте в Інтернет-ресурсах чисельний приклад з використання бінарного алгоритму піднесення до степеня за модулем (наприклад, в Вікіпедії ) та опрацюйте його.
2. Розробіть інтерфейс криптографічної системи RSA для шифрування з використанням бінарного алгоритму піднесення до степеня за модулем, передбачивши окремий діалог для формування відкритого ключа.
3. Розробіть методи, які б забезпечували:
   1. Генерацію пари «відкритий –закритий» ключі.
   2. Шифрування з використанням відкритого ключа.
   3. Розшифрування з використанням закритого ключа.
4. Перевірте правильність роботи системи на основі використання даних з чисельного прикладу.

## **Програмна реалізація**

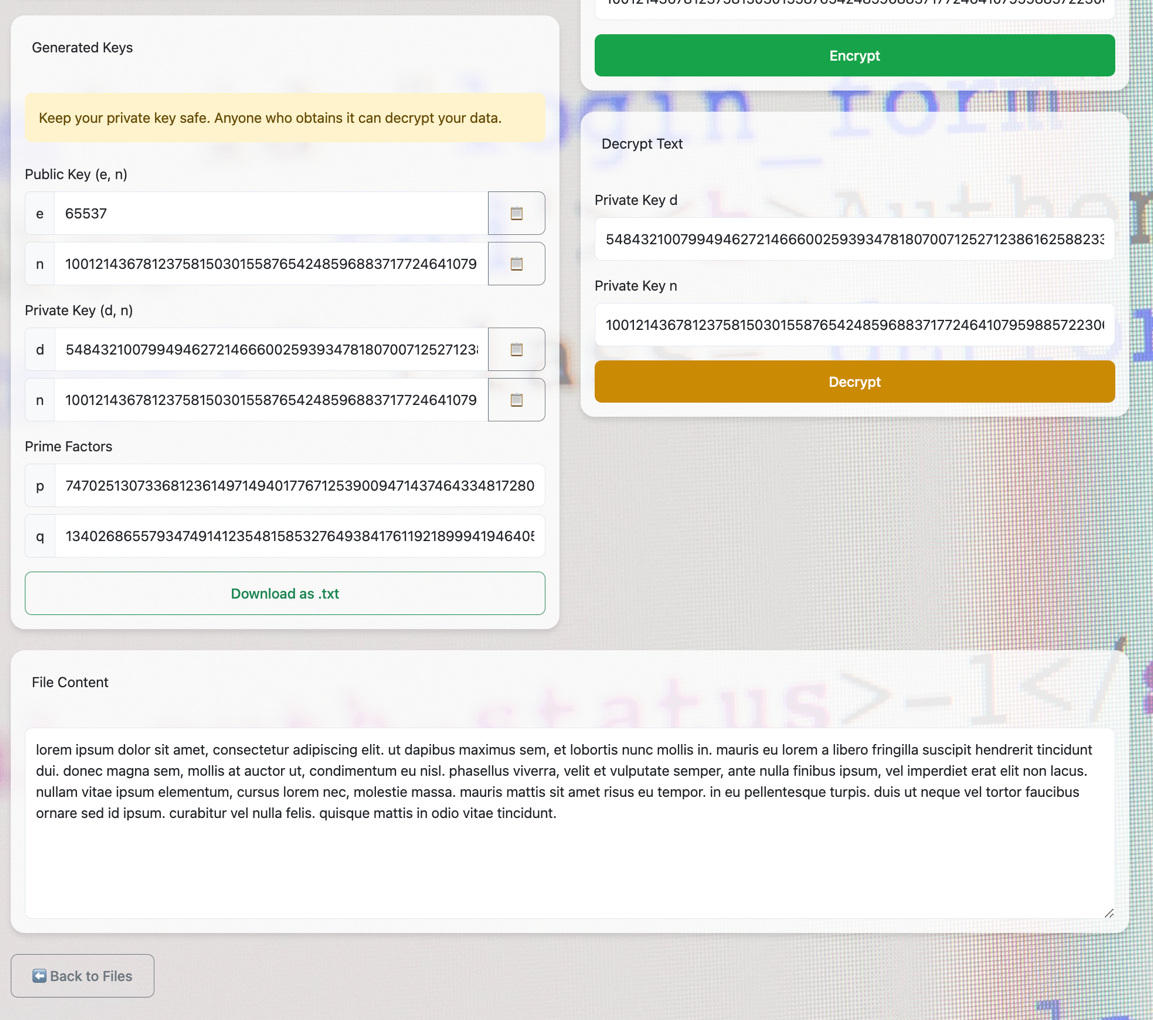
Для розробки інтерфейсу веб-застосунку я скористався мовою C# та фреймворком ASP.NET Core MVC 9.0.

Додана можливість обрати шифр на основі задачі рюкзака.



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

A screenshot of a computer

AI-generated content may be incorrect.  


**Висновок**  
У ході виконання лабораторної роботи було реалізовано криптосистему RSA з використанням бінарного алгоритму піднесення до степеня за модулем. Основним завданням було створення інтерфейсу для генерації ключової пари, шифрування та розшифрування даних з використанням відкритого та закритого ключів.