МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИЛЬВІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені ІВАНА ФРАНКА

**Звіт із**

**Протокол обміну ключами Діффі-Гелмана**

**Лабораторна робота №6**

з курсу «Математичні основи криптології»

Виконав:

Готюк Максим

Група Пмі-33

Оцінка \_\_\_

2025

# Звіт: Шифрування з відкритим ключем - Протокол Діффі-Хеллмана

## Тема

Шифрування з відкритим ключем. Протокол Діффі-Хеллмана для обміну ключами.

## Мета

Реалізувати протокол Діффі-Хеллмана для безпечного обміну ключами з використанням бінарного алгоритму піднесення до степеня за модулем.

## Постановка завдання

1. Відшукати в Інтернет-ресурсах чисельний приклад використання протоколу Діффі-Хеллмана з бінарним алгоритмом піднесення до степеня за модулем та опрацювати його.
2. Розробити інтерфейс для реалізації протоколу Діффі-Хеллмана з використанням бінарного алгоритму піднесення до степеня за модулем, передбачивши діалоги для:
   * Вибору/генерації спільних параметрів (просте число p та основа g)
   * Генерації приватних та публічних ключів для обох сторін
   * Формування спільного секретного ключа
3. Розробити методи, які б забезпечували: a. Генерацію приватних ключів для обох сторін. b. Обчислення публічних ключів на основі приватних. c. Обчислення спільного секретного ключа для безпечного зв'язку. d. Імплементацію бінарного алгоритму піднесення до степеня за модулем для ефективних обчислень.
4. Перевірити правильність роботи системи на основі використання даних з чисельного прикладу.

## Теоретичні відомості

Протокол Діффі-Хеллмана — це метод обміну криптографічними ключами, який дозволяє двом сторонам, які не мають попередніх знань одна про одну, спільно встановити спільний секретний ключ через незахищений канал зв'язку. Цей ключ може бути використаний для шифрування подальшого спілкування за допомогою симетричного шифрування.

Основні кроки протоколу:

1. Сторони А і В погоджуються на спільні параметри: просте число p та його первісний корінь g.
2. Сторона А генерує приватний ключ a і обчислює свій публічний ключ: A = g^a mod p.
3. Сторона В генерує приватний ключ b і обчислює свій публічний ключ: B = g^b mod p.
4. Сторони обмінюються публічними ключами через незахищений канал.
5. Сторона А обчислює спільний секретний ключ: K = B^a mod p.
6. Сторона В обчислює спільний секретний ключ: K = A^b mod p.

Обидві сторони отримують однакове значення K = g^(a\*b) mod p, яке є їхнім спільним секретним ключем.

Для ефективного піднесення до степеня використовується бінарний алгоритм піднесення до степеня за модулем.

## Програмна реалізація

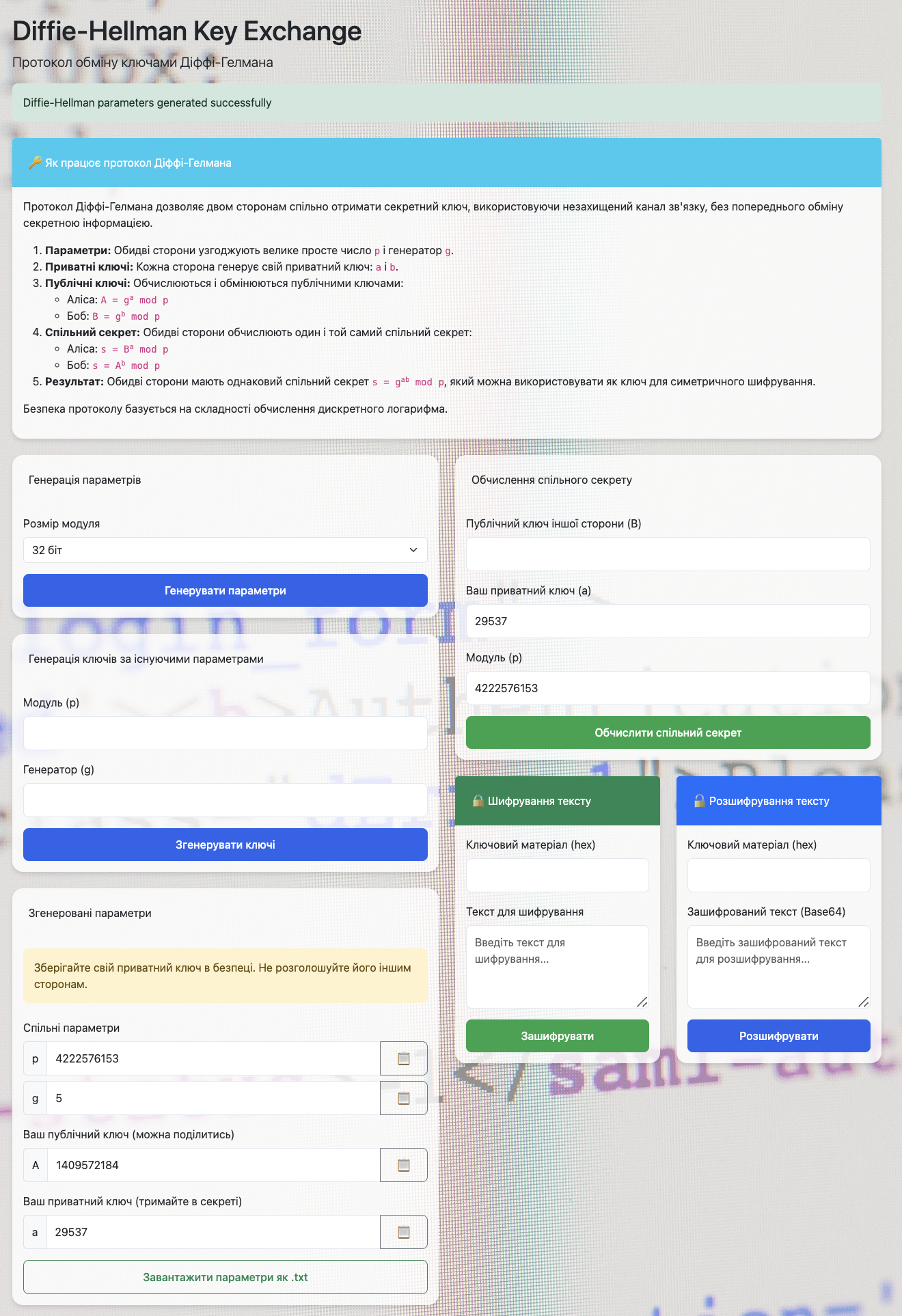
Для розробки інтерфейсу веб-застосунку було використано мову C# та фреймворк ASP.NET Core MVC 9.0.

Основні компоненти реалізації:

1. **Клас DiffieHellmanService**:
   * Містить методи для генерації простих чисел
   * Реалізує бінарний алгоритм піднесення до степеня за модулем
   * Забезпечує генерацію приватних ключів
   * Обчислює публічні та спільні секретні ключі
2. **Контролер DiffieHellmanController**:
   * Забезпечує взаємодію з користувачем
   * Відображає форми для введення параметрів
   * Демонструє результати обчислень
3. **Представлення (Views)**:
   * Форма для введення/генерації спільних параметрів p та g
   * Інтерфейс для обчислення та відображення публічних ключів
   * Сторінка для демонстрації обміну ключами та формування спільного секретного ключа

Інтерфейс програми дозволяє користувачам:

* Генерувати або вводити спільні параметри p і g
* Створювати приватні ключі для обох сторін
* Обчислювати та обмінюватись публічними ключами
* Демонструвати обчислення спільного секретного ключа
* Перевіряти коректність протоколу



## Висновок

У ході виконання лабораторної роботи було успішно реалізовано протокол Діффі-Хеллмана для безпечного обміну ключами з використанням бінарного алгоритму піднесення до степеня за модулем. Створений інтерфейс дозволяє користувачам легко працювати з протоколом, генерувати ключі та перевіряти коректність роботи системи.

Протокол Діффі-Хеллмана забезпечує безпечний обмін ключами навіть через незахищені канали зв'язку, оскільки приватні ключі ніколи не передаються, а обчислення спільного секретного ключа з публічних параметрів є обчислювально складним завданням для зловмисника через проблему дискретного логарифмування.

Розроблена реалізація демонструє основні принципи та переваги використання протоколу Діффі-Хеллмана в сучасних криптографічних системах.