Міністерство освіти і науки України Національний технічний університет України «Київський політехнічний інститут ім. І. Сікорського»

Кафедра інженерії програмного забезпечення в енергетиці

Комп`ютерний практикум №6

з курсу: «Безпека програмного забезпечення»

**Виконала:**

студентка 4-го курсу, групи ТВ-12

Піховкіна Катерина Вячеславівна

Посилання на GitHub репозиторій:

[https://github.com/EkaterinaPikhovkina/software-security-labs.git](https://github.com/EkaterinaPikhovkina/poetic-cipher.git)

**Перевірив:**

Гейко О.О.

Київ 2024/2025

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №6

Тема: Шифрування з відкритим ключем на основі алгоритму RSA

Мета: Ознайомитись з використанням криптопровайдерів .Net для побудови асиметричної криптосистеми

Хід виконання роботи:

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

**Завдання 1.**

Нехай відкрите повідомлення (plaintext) — це "HELLO". Візьмемо два простих числа: p = 17 і q = 19.

Обчислення n:

n = p \* q = 17 \* 19 = 323.

Обчислення φ(n):

φ(n) = (p - 1) \* (q - 1) = 16 \* 18 = 288.

Вибір відкритого ключа e:

e має бути взаємно простим із φ(n), і 1 < e < φ(n).

Виберемо e = 5 (оскільки gcd(5, 288) = 1).

Обчислення закритого ключа d:

d — це мультиплікативне обернене до e за модулем φ(n):

d \* e mod φ(n) = 1.

Використовуючи розширений алгоритм Евкліда, отримаємо d = 173.

Шифрування:

Для кожного символу M обчислюємо C = M^e mod n:

ASCII-коди повідомлення "HELLO" — це [72, 69, 76, 76, 79].

Результат шифрування:

C = [72^5 mod 323, 69^5 mod 323, 76^5 mod 323, 76^5 mod 323, 79^5 mod 323] = [249, 50, 129, 129, 22].

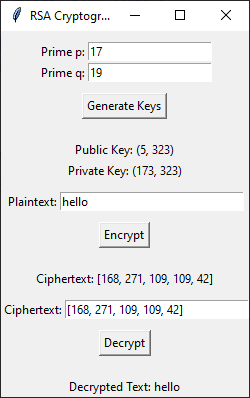
Розшифрування:

Для кожного C обчислюємо M = C^d mod n:

M = [249^173 mod 323, 50^173 mod 323, 129^173 mod 323, 129^173 mod 323, 22^173 mod 323].

Результат розшифрування: [72, 69, 76, 76, 79], що відповідає повідомленню "HELLO".

**Завдання 2-4.**



**Висновок**

У ході виконання комп’ютерного практикуму №6 було досягнуто мети роботи — ознайомлення з принципами асиметричної криптографії на основі алгоритму RSA та використання криптопровайдерів .Net для побудови криптосистеми.

В результаті виконання завдань:

* + - Було знайдено та опрацьовано числовий приклад використання алгоритму RSA. На його основі було розраховано:
      * + пару простих чисел p і q;
        + модуль n та функцію Ейлера φ(n);
        + відкритий та закритий ключі;
        + результати шифрування та розшифрування повідомлення.
    - Розроблено інтерфейс криптографічної системи з підтримкою діалогу для генерації відкритого ключа.
    - Реалізовано методи для:
      * + генерації пари «відкритий – закритий» ключі;
        + шифрування даних з використанням відкритого ключа;
        + розшифрування даних за допомогою закритого ключа.
    - Проведено тестування системи на основі знайденого числового прикладу, що підтвердило правильність реалізації алгоритму.

Дана лабораторна робота допомогла краще зрозуміти принципи роботи алгоритму RSA, а також засвоїти практичні аспекти його застосування для створення криптографічних систем.