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

Кафедра інженерії програмного забезпечення в енергетиці

Комп`ютерний практикум №7

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

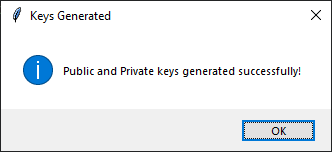
Тема: Електронно-цифровий підпис на основі алгоритму RSA

Мета: Ознайомитись з порядком утворення підпис на основі алгоритму RSA

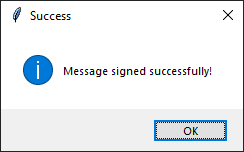
Хід виконання роботи:

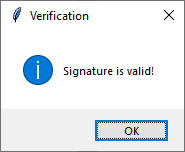
1. Розробіть інтерфейс системи формування і перевірки ЕЦП RSA, передбачивши окремий діалог для формування відкритого ключа.
2. Розробіть методи, які б забезпечували:
3. Генерацію пари «відкритий – закритий» ключі.
4. Підписування довільного повідомлення з використанням закритого ключа.
5. Перевірки ЕЦП з використанням відкритогоключа.
6. Перевірте правильність роботи системи.

**Завдання 1-3**









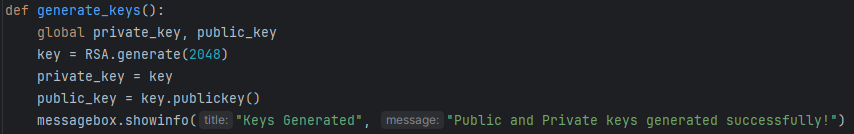
**Опис програмної реалізації**

Дана програма реалізує базову систему цифрового підпису на основі алгоритму RSA. Інтерфейс побудований за допомогою бібліотеки Tkinter, що дозволяє генерувати публічний і приватний ключі, підписувати повідомлення та перевіряти підпис.

**Основні компоненти коду**

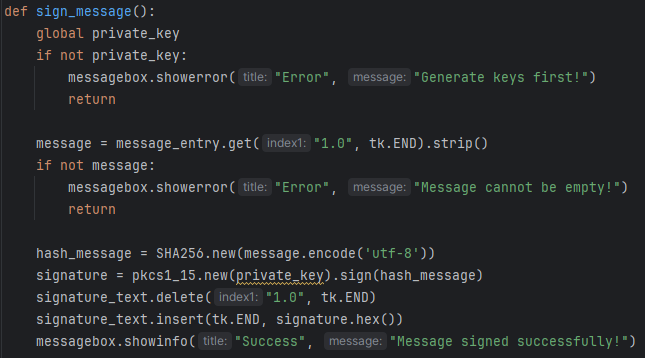
Генерація ключів (generate\_keys):

* Алгоритм RSA використовується для створення 2048-бітних ключів.
* Генерується пара ключів: приватний (для підпису) та публічний (для перевірки).
* Ключі зберігаються у глобальних змінних private\_key та public\_key.



Підписання повідомлення (sign\_message):

* Повідомлення вводиться користувачем через текстове поле.
* Хеш повідомлення обчислюється за допомогою алгоритму SHA-256.
* Підпис створюється з використанням приватного ключа та модуля pkcs1\_15.
* Результат підпису представлений у шістнадцятковому форматі.



Перевірка підпису (verify\_signature):

* Перевіряє введене повідомлення та його цифровий підпис.
* Обчислюється хеш повідомлення і перевіряється з використанням публічного ключа.
* Якщо підпис дійсний, відображається відповідне повідомлення, інакше — помилка.



**Висновок**

У ході виконання комп’ютерного практикуму №7 було досягнуто мети роботи — Ознайомитись з порядком утворення підпис на основі алгоритму RSA.

В результаті виконання завдань було написано програму, яка демонструє базову реалізацію системи цифрового підпису за допомогою RSA. Вона надає фундаментальне уявлення про процеси генерації ключів, підписання та перевірки повідомлень. Для розширення функціональності можна додати збереження ключів у файл, підтримку різних форматів повідомлень або підвищити безпеку перевірок.