МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНИ СЕМЕНА КУЗНЕЦЯ

ЗВІТ
о виконанні лабораторної роботи №4
з дисципліни «Захист інформації»
за темою «Особистий цифровий підпис»

Виконав:
Студент 4 курсу
групи 6.04.122.010.22.1
факультету ІТ
Холоша Сергій

Перевірив:
Професор кафедри
кібербезпеки та ІТ
Тютюнник В. В.

Харків – 2025

Порядок виконання практичної частини

Крок 1. Дослідження готових інструментів цифрового підпису

1) Завантажити та встановити GPG4Win або GPG Suite для Mac;

2) Спробувати згенерувати тестову пару ключів (публічний та приватний);

3) Підписати тестовий файл та перевірити підпис;

4) Зрозуміти принципи роботи асимметричних підписів та різницю між хешуванням і підписанням.

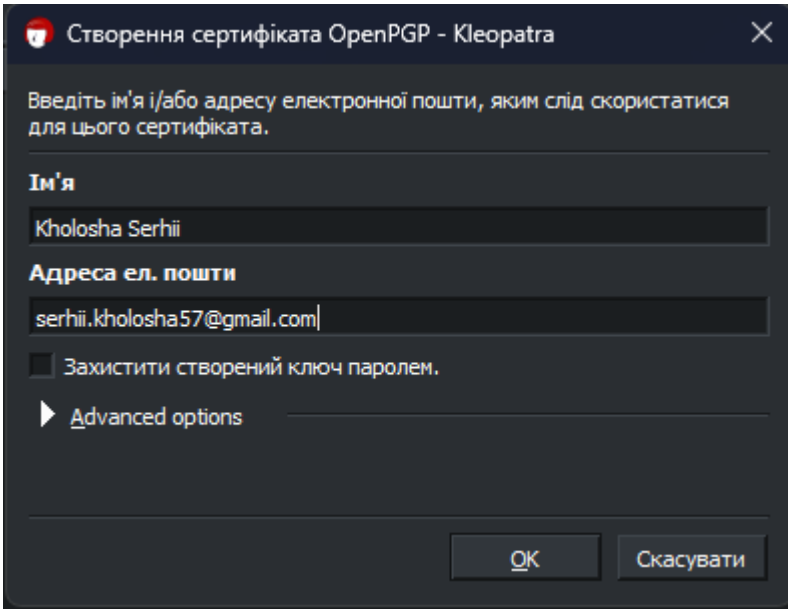

Рис. 1 Вікно створення ключів

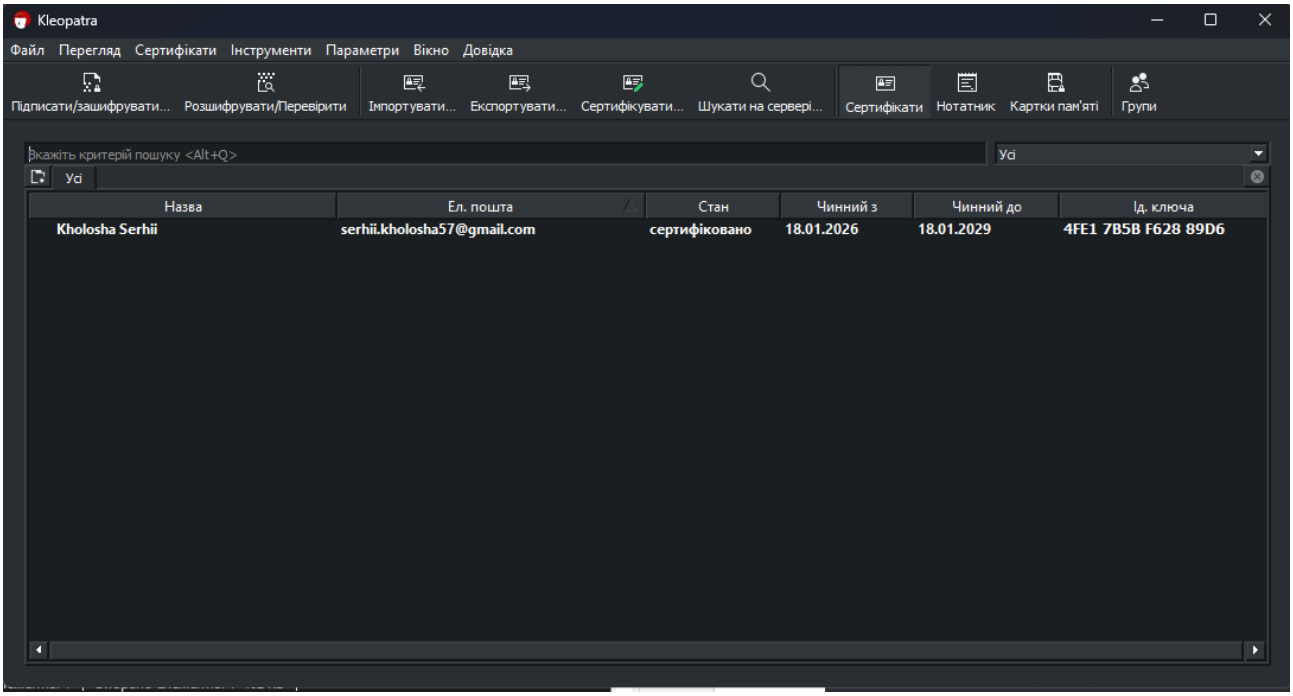

Рис. 2 Успішно створена пара ключів

Рис. 3 Створений файл для тестування

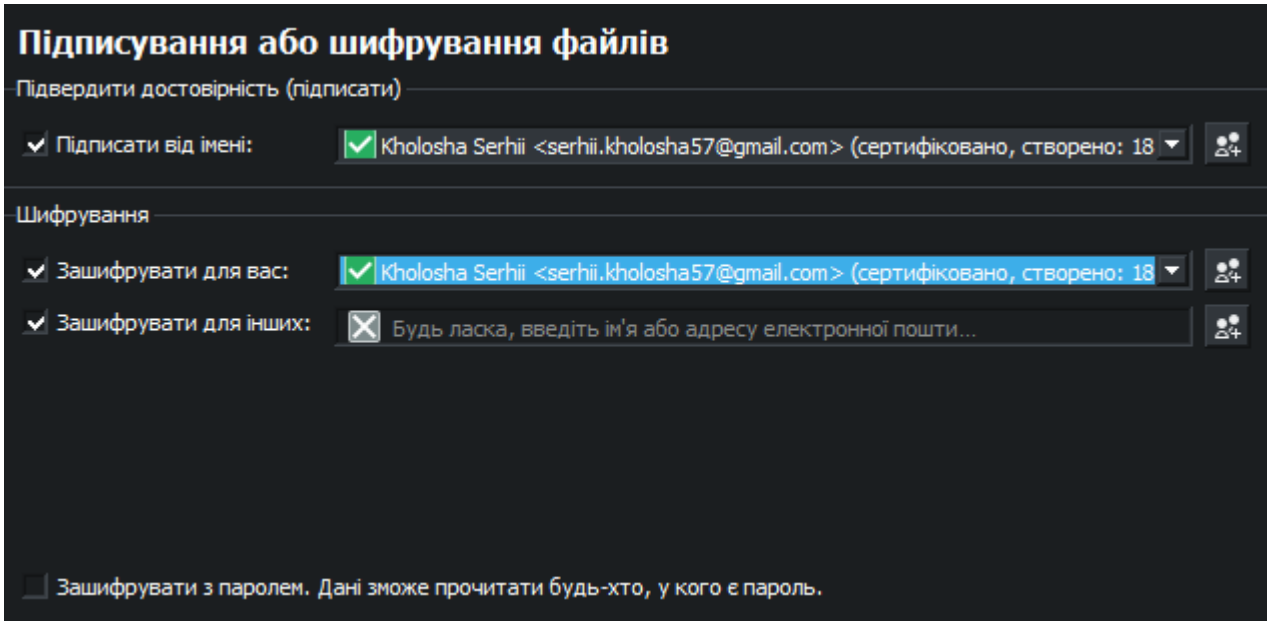

Рис. 4 Підписання та шифрування тестового файлу

Рис. 5 Створений файл

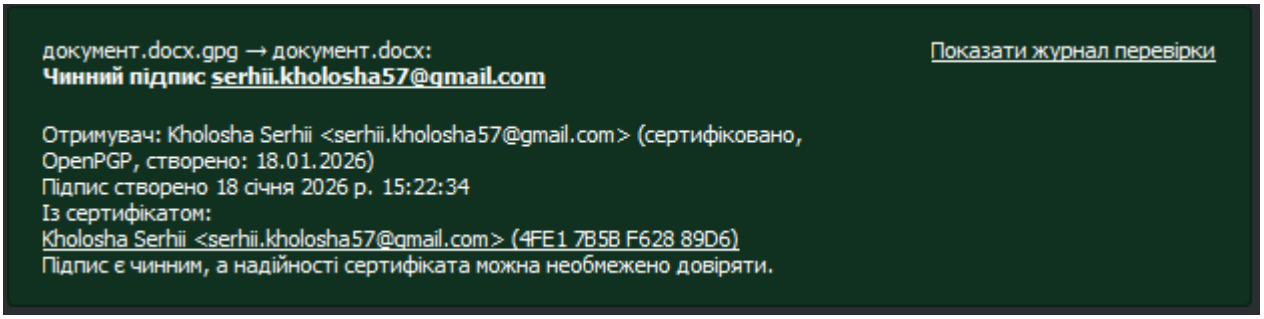

Рис. 6 Перевірка підпису

Крок 2. Створення власної пари ключів

1) Згенерувати просту пару ключів на основі персональних даних (не криптографічно стійку, а для демонстрації);

2) “Приватний ключ”: хеш від (ім’я + дата народження + секретне слово);

3) “Публічний ключ”: математично пов’язана з приватним ключем величина;

4) Зберегти ключі в окремих файлах.

```
Введіть ім'я: Сергій
Введіть дату народження (ДД.ММ.РРРР): 14.08.2004
Введіть секретне слово: Холоша

Приватний ключ: 0774afce37de127bf9e6cfec082406869a4f5e9da6e5ba87c5a1b8cf4ef49a4b
Публічний ключ: 903723061018485724

Ключі збережено у файли private_key.json та public_key.json
```

Рис. 7 Створені ключі


```
{
  "private_key": "0774afce37de127bf9e6cfec082406869a4f5e9da6e5ba87c5a1b8cf4ef49a4b"
}
```


Рис. 8 Приватний ключ


```
{
  "public_key": "903723061018485724"
}
```


Рис. 9 Публічний ключ

Крок 3. Підписання власних документів

1) Створити хеш документа (SHA–256);

2) “Підписати” хеш за допомогою приватного ключа (шифрування хешу);

3) Зберегти підпис в окремому файлі;

4) Перевірити підпис за допомогою публічного ключа.

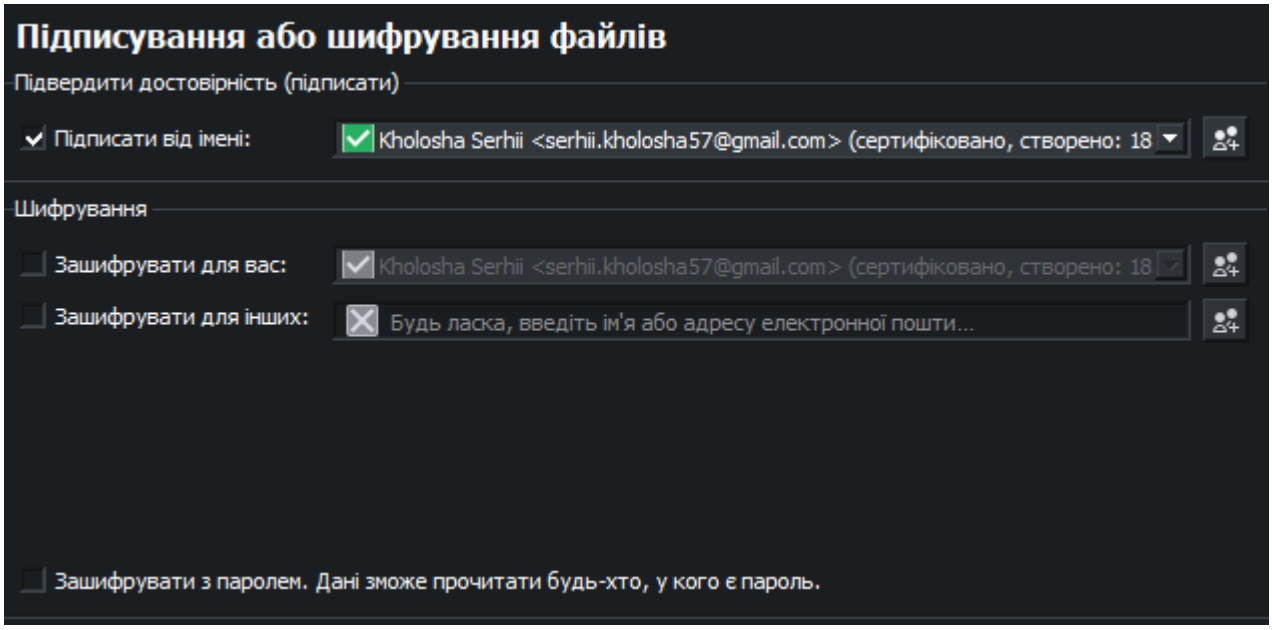

Рис. 10 Підписання документу

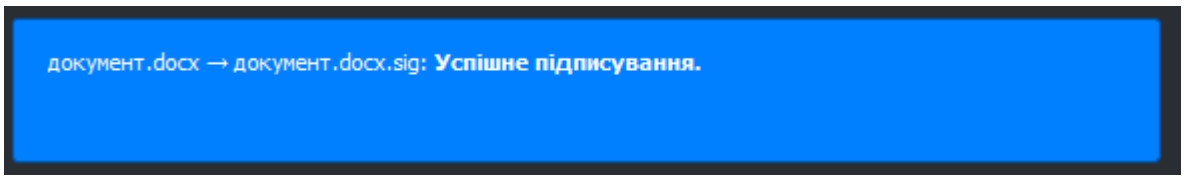

Рис. 11 Успішне підписання

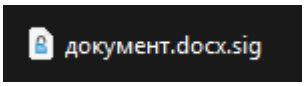

Рис. 12 Створений файл .sig

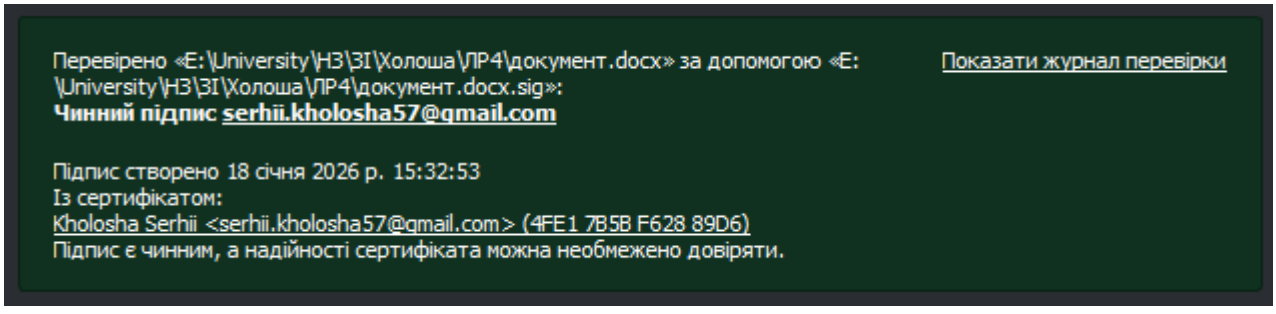

Рис. 13 Успішний підпис

Крок 4. Тестування підробки підписів

1) Спробувати модифікувати підписаний документ;

2) Перевірити, чи виявляє система зміни в документі;

3) Спробувати підробити підпис та переконатися, що це неможливо без приватного ключа.

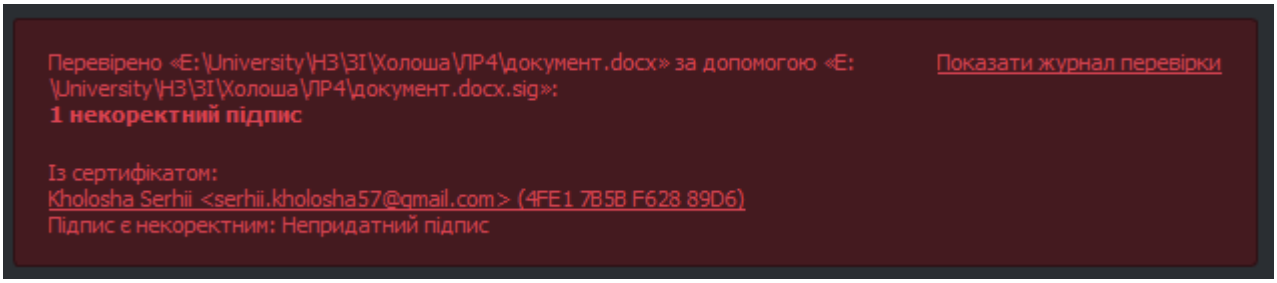

Рис. 14 Перевірка підпису після редагування документа

Технічне завдання

Завдання: Реалізувати спрощену систему цифрових підписів з демонстрацією принципів асимметричного шифрування.

```
=== СИСТЕМА ЦИФРОВИХ ПІДПИСІВ ===

Прізвище: Холоша
Дата народження (DDMMYYYY): 14082004
Секретне слово: Сергій

Приватний ключ: 866521
Публічний ключ: 65605

Ім'я файлу документа (без розширення): файл
Введіть текст документа: Засекречений документ
Документ збережено: файл.txt
Хеш документа: 27885091616381890788939420233173726315233464513870748789050014007591028535027
Цифровий підпис: 27885091616381890788939420233173726315233464513870748789050014007591029380650
Підпис збережено: файл_signature.txt

--- ПЕРЕВІРКА ПІДПИСУ ---
Введіть ім'я файлу для перевірки: файл.txt
✓ Підпис ДІЙСНИЙ

--- ДЕМОНСТРАЦІЯ ПІДРОБКИ ---
Створено підроблений документ: fake_файл.txt
✗ Підпис ПІДРОБЛЕНИЙ (зміни виявлено)
```

Рис. 15 Робота програми

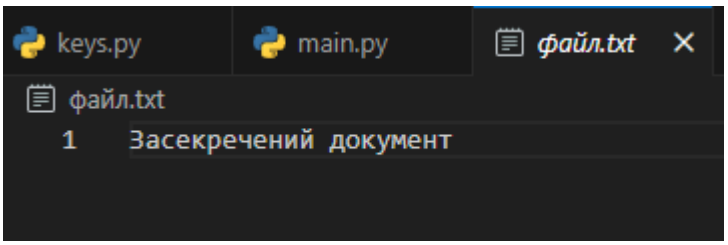

Рис. 16 Створений файл

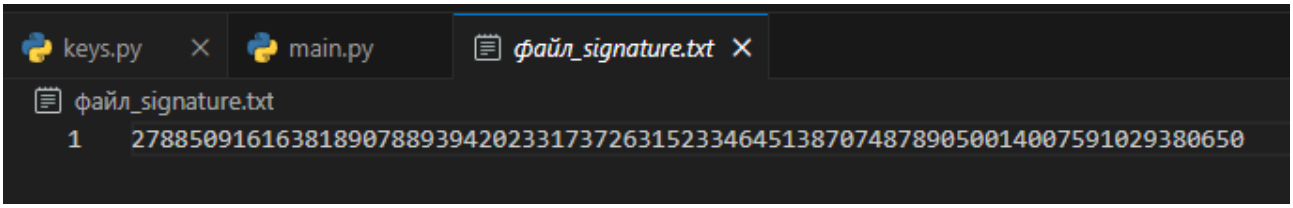

Рис. 17 Створений підпис

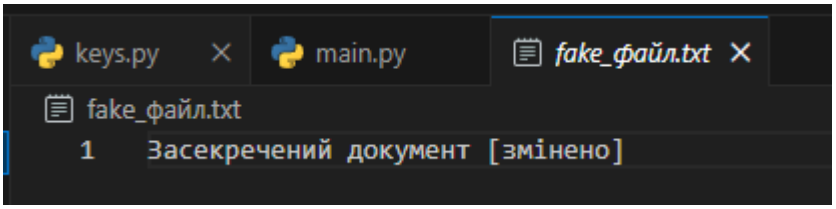

Рис. 18 Файл зі зміною для перевірки

Посилання на GitHub: [zahist-informaciji/lab4 at main · serhiikholosha57/zahist-informaciji]

Висновок: в ході лабораторної роботи було створено власну систему цифрових підписів для забезпечення автентичності та цілісності документів