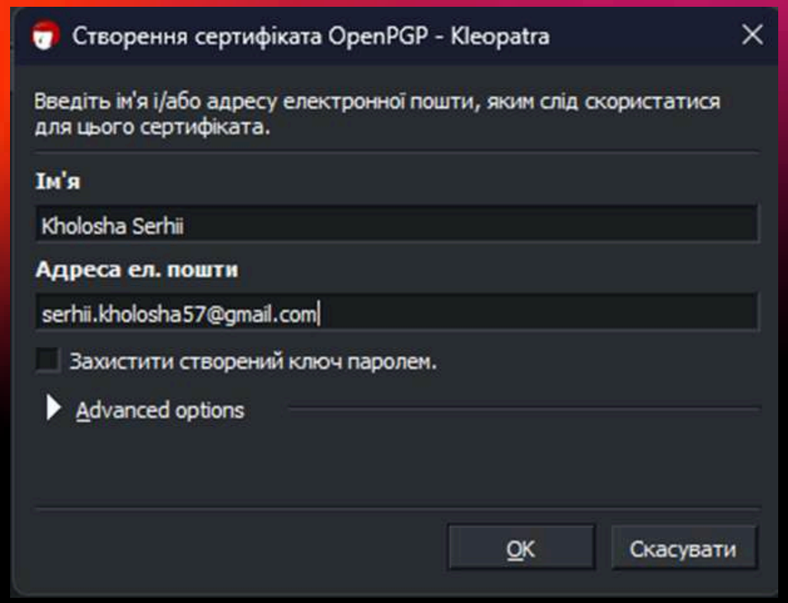
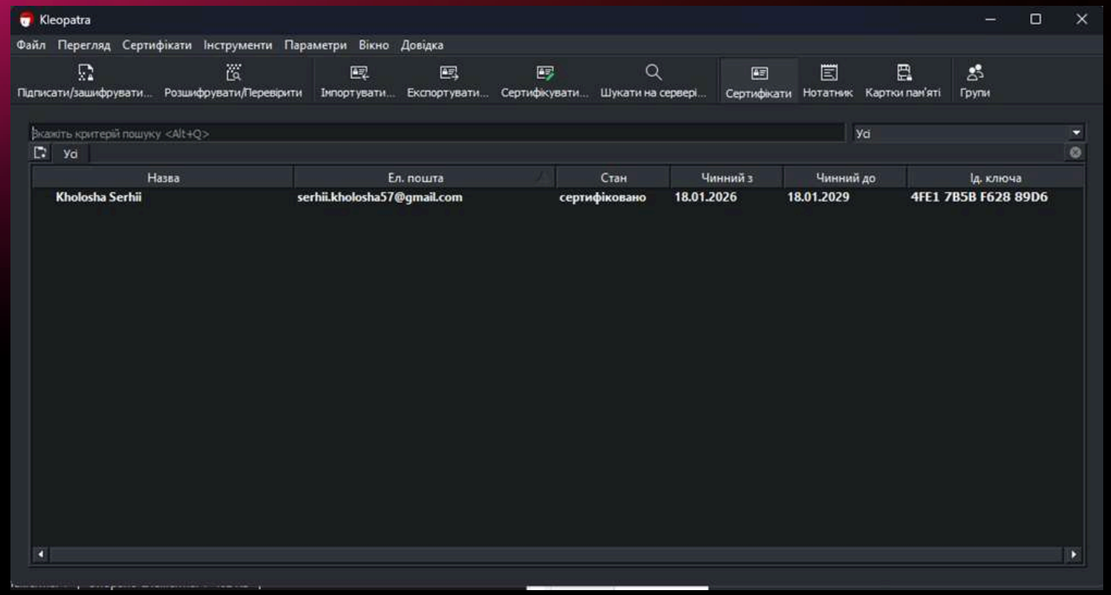
ЛАБОРАТОРНА РОБОТА 4

Особистий цифровий підпис

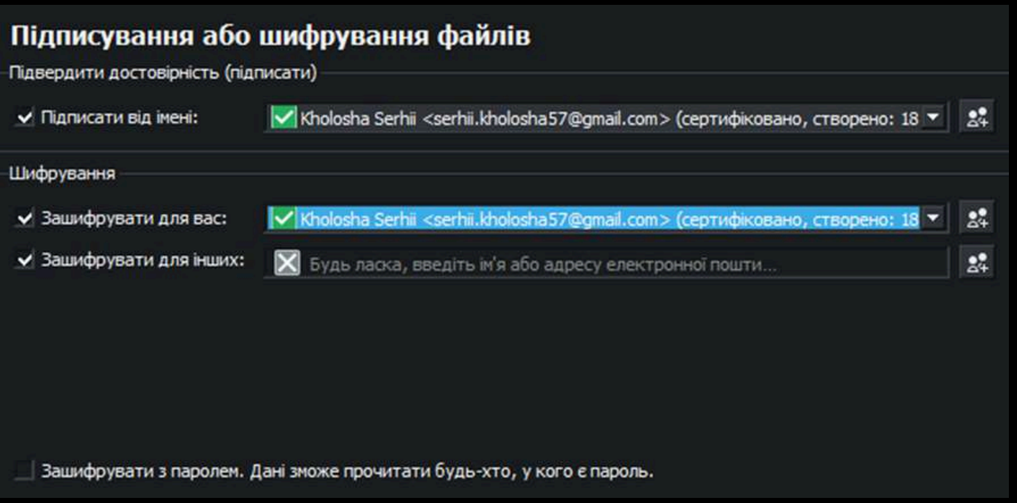
Виконав Холоша Сергій

Дослідження готових інструментів цифрового підпису


Створення сертифіката OpenPGP - Kleopatra
Введіть ім'я і/або адресу електронної пошти, яким слід скористатися для цього сертифіката.
Ім'я
Kholosha Serhii
Адреса ел. пошти
serhii.kholosha57@gmail.com
Захистити створений ключ паролем.
Advanced options
OK
Скасувати


Kleopatra
Файл Перегляд Сертифікати Інструменти Параметри Вікно Довідка
Підписати/зашифрувати... Розшифрувати/Перевірити Імпортувати... Експортувати... Сертифікувати... Шукати на сервері... Сертифікати Нотатник Картки пам'яті Групи
Назва Ел. пошта Стан Чинний з Чинний до Ід. ключа
Kholosha Serhii serhii.kholosha57@gmail.com сертифіковано 18.01.2026 18.01.2029 4FE1 7B5B F628 89D6


документ.docx

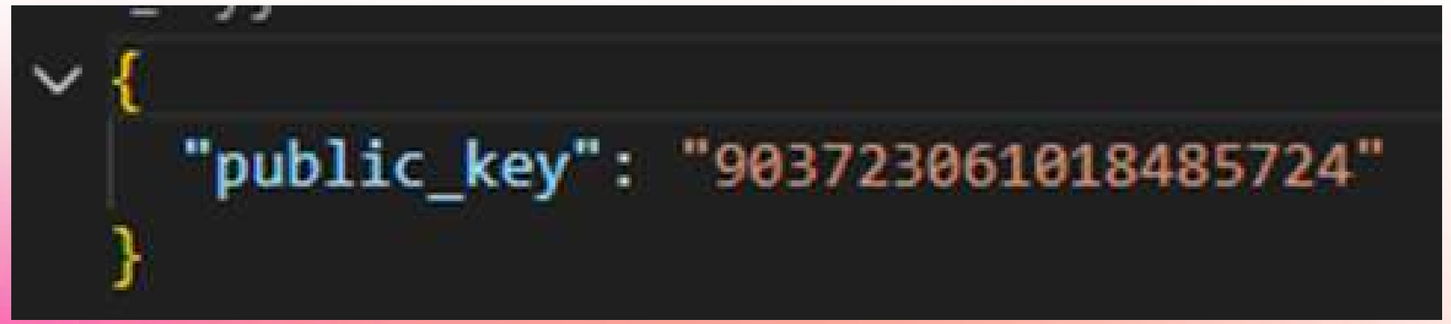

Підписування або шифрування файлів
Підвердити достовірність (підписати)
Підписати від імені:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Шифрування
Зашифрувати для вас:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Зашифрувати для інших:
Будь ласка, введіть ім'я або адресу електронної пошти...
Зашифрувати з паролем. Дані зможе прочитати будь-хто, у кого є пароль.


документ.docx.gpg

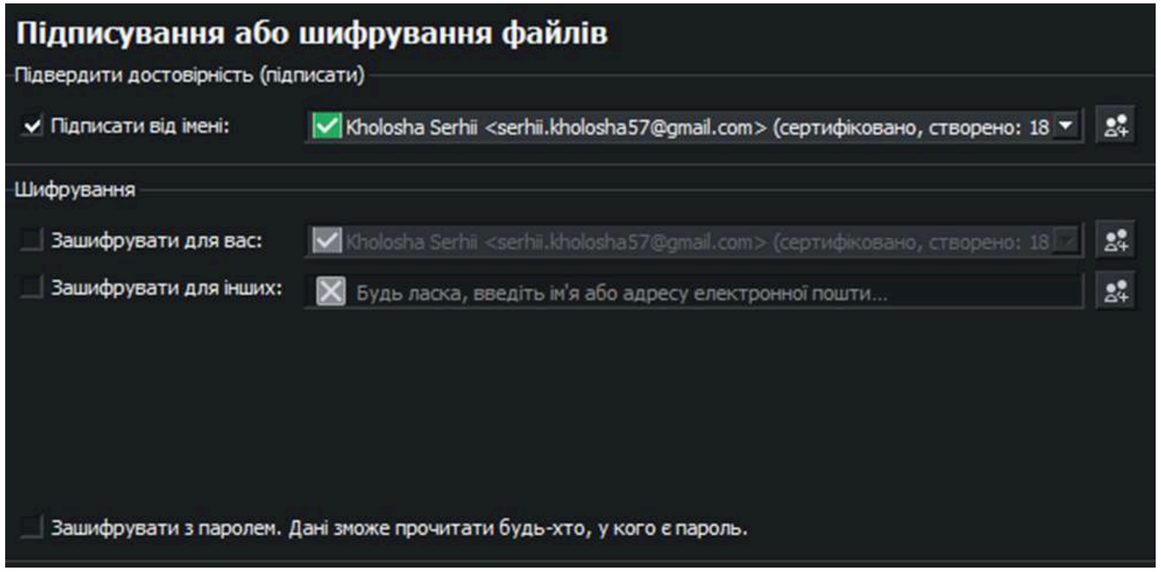

документ.docx.gpg → документ.docx:
Чинний підпис serhii.kholosha57@gmail.com
Отримувач: Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, OpenPGP, створено: 18.01.2026)
Підпис створено 18 січня 2026 р. 15:22:34
Із сертифікатом:
Kholosha Serhii <serhii.kholosha57@gmail.com> (4FE1 7B5B F628 89D6)
Підпис є чинним, а надійності сертифіката можна необмежено довіряти.

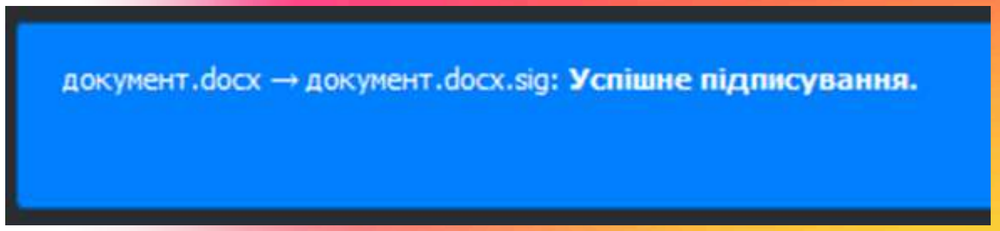
Створення власної пари ключів

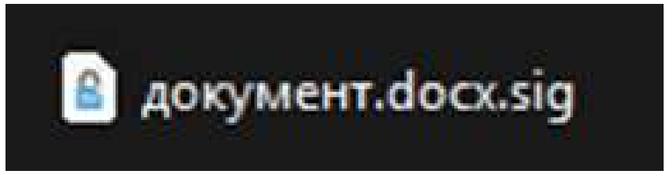
```
Введіть ім'я: Сергій
Введіть дату народження (ДД.ММ.РРРР): 14.08.2004
Введіть секретне слово: Холоша

Приватний ключ: 0774afce37de127bf9e6cfec082406869a4f5e9da6e5ba87c5a1b8cf4ef49a4b
Публічний ключ: 9037230610184857 24

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

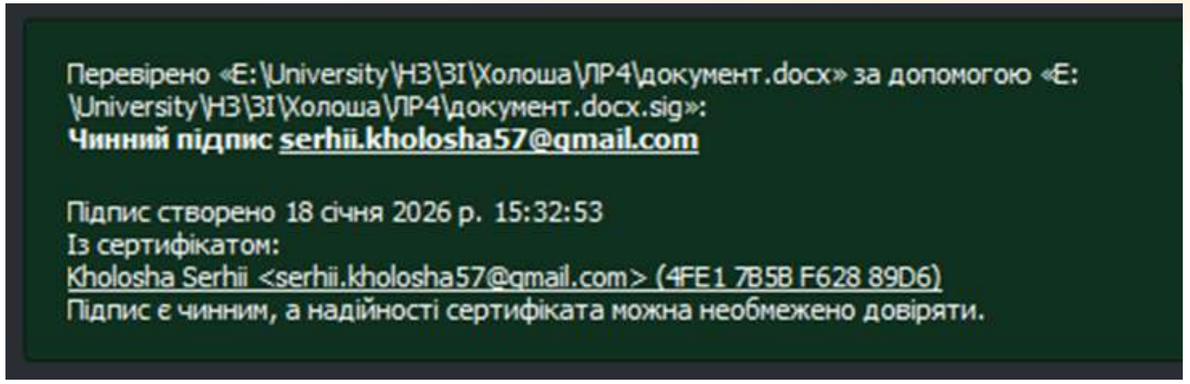


Підписання власних документів

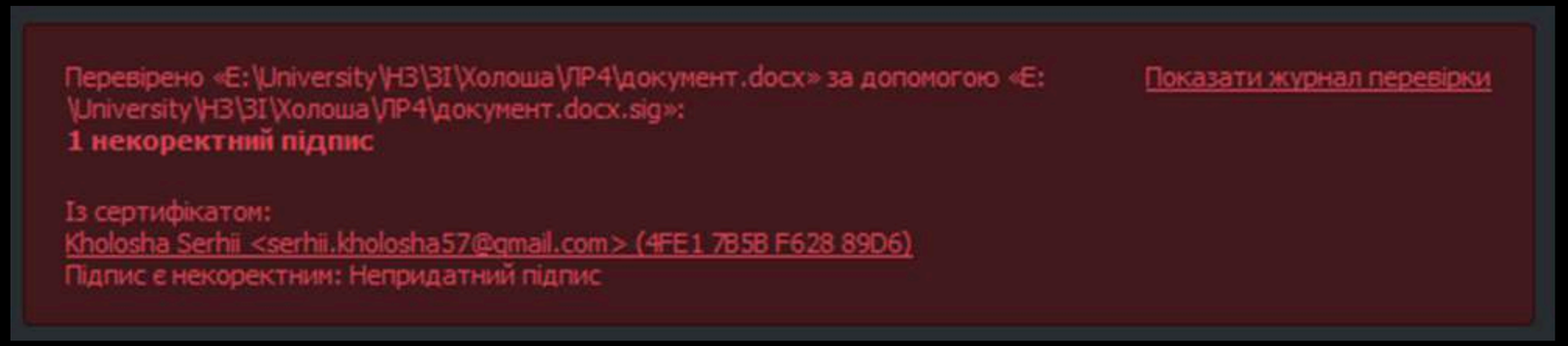

Підписування або шифрування файлів
Підвердити достовірність (підписати)
Підписати від імені:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Шифрування
Зашифрувати для вас:
Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, створено: 18
Зашифрувати для інших:
Будь ласка, введіть ім'я або адресу електронної пошти...
Зашифрувати з паролем. Дані зможе прочитати будь-хто, у кого є пароль.


документ.docx → документ.docx.sig: Успішне підписування.


документ.docx.sig

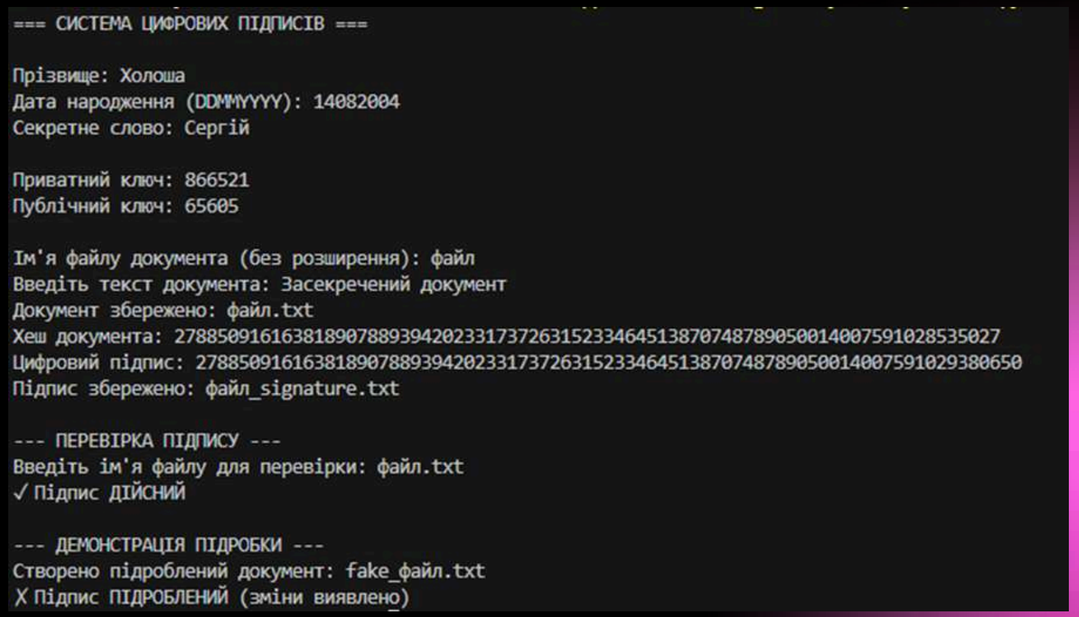

Перевірено «E:\University\НЗ\ЗІ\Холоша\ЛР4\документ.docx» за допомогою «E:\University\НЗ\ЗІ\Холоша\ЛР4\документ.docx.sig»:
Чинний підпис serhii.kholosha57@gmail.com
Підпис створено 18 січня 2026 р. 15:32:53
Із сертифікатом:
Kholosha Serhii <serhii.kholosha57@gmail.com> (4FE1 7B5B F628 89D6)
Підпис є чинним, а надійності сертифіката можна необмежено довіряти.

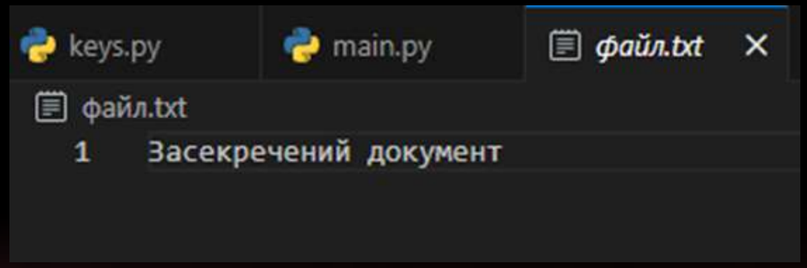
Тестування підробки підписів

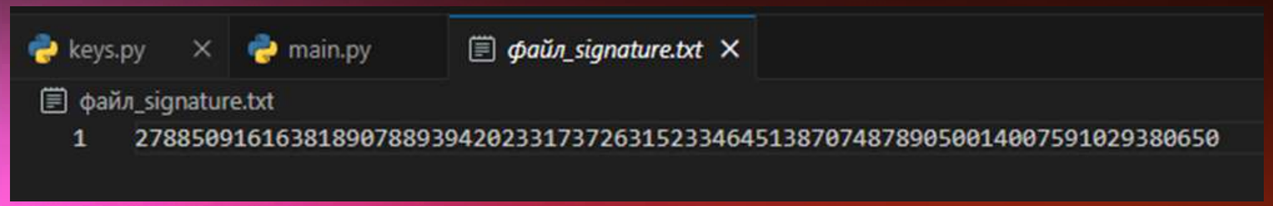


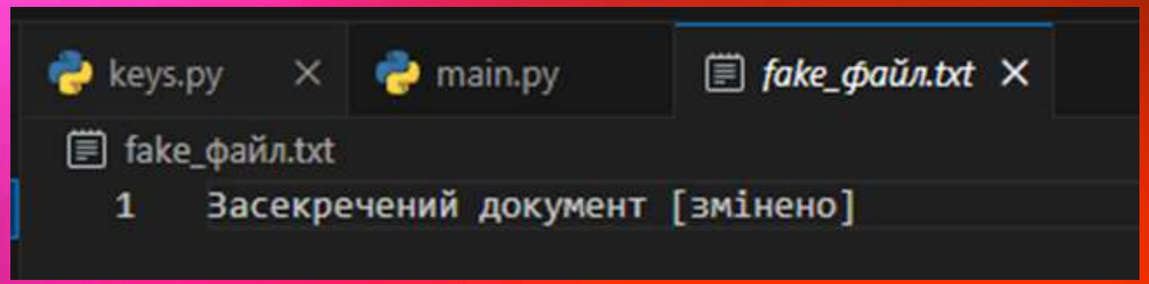
Після редакції документа

Технічне завдання


=== 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: 278850916163818907889394202331737263152334645138707487890500140075910293806 50
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)


keys.py
main.py
файл.txt
файл.txt
1 Засекречений документ


keys.py
main.py
файл_signature.txt
файл_signature.txt
1 27885091616381890788939420233173726315233464513870748789050014007591029380650


keys.py
main.py
fake_файл.txt
fake_файл.txt
1 Засекречений документ [змінено]

Дякую за увагу!

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