****

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Рівненський фаховий коледж інформаційних технологій**

**Звіт**

**Про виконання лабораторної роботи №4**

**Практичне застосування симетричного та асиметричного шифрування. Цифровий підпис.**

**Виконав**

**Студент 3 курсу групи КН-3/1**

**Валерій ФОРМАНЮК**

**07.10.2025 р.**

**м.Рівне**

**Лабораторна робота №4**

# **Тема:** Практичне застосування симетричного та асиметричного шифрування. Цифровий підпис.

# **1. Мета роботи:**

* Засвоїти основи створення, використання та управління криптографічними ключами.
* Навчитися виконувати шифрування і дешифрування файлів симетричними та асиметричними методами.
* Опанувати створення та перевірку цифрового підпису за допомогою інструменту **GnuPG (gng)**. Алгоритми шифрування, що використовують два ключі, називаються асиметричними алгоритмами шифрування.

# **2. Теоретичні відомості:**

* **Симетричне шифрування** - це криптографічний метод, де один і той самий ключ використовується і для шифрування, і для дешифрування даних.
* **Асиметричне шифрування** - це алгоритми шифрування які використовують два ключі: **публічний ключ** - для шифрування або перевірки підпису та **приватний ключ** - для дешифрування або створення підпису.
* **Цифровий підпис** - це спосіб підтвердження авторства та цілісності файлу за допомогою приватного ключа.
* **GPG (GNU Privacy Guard)** - використовується для шифрування та розшифрування даних, а також для створення та перевірки електронних підписів, електронних листів та файлів.

# **3. Хід виконання роботи:**

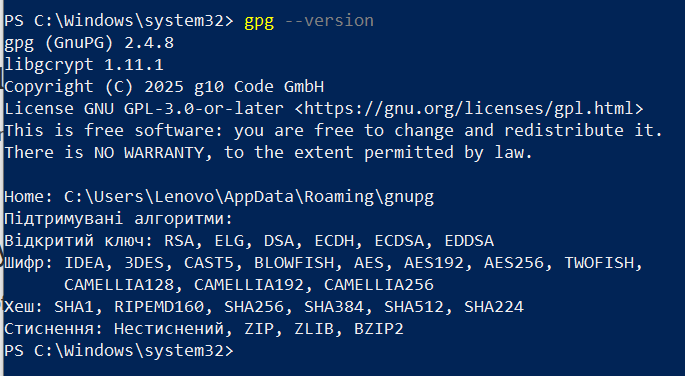
## **Частина 1. Створення ключів**

Встановив Gpg4win

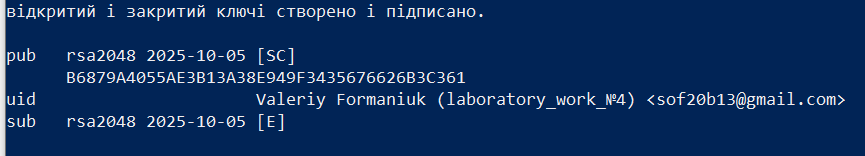
Виконав команди:

gpg --full-generate-key

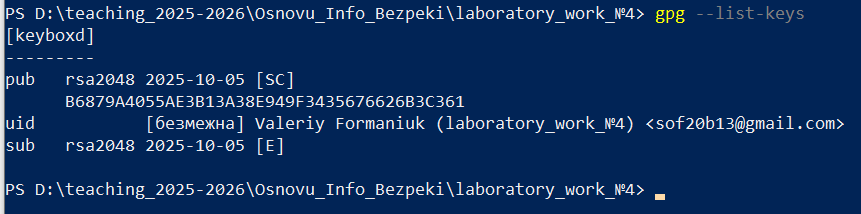
gpg --list-keys



Скріншот 1: Встановлення GnuPG



Скріншот 2: Результат створення ключа



Скріншот 3: Відображення ключів у списку

Висновок: Успішно створено пару ключів RSA, які будуть використані для шифрування та підпису файлів.

## **Частина 2. Шифрування/дешифрування**

* Створив файл: secret.txt

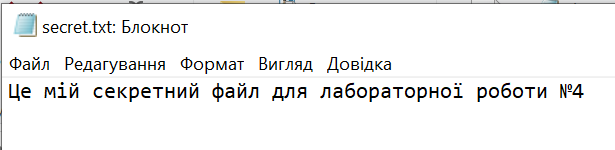
Ввів команди:

шифрування файлу

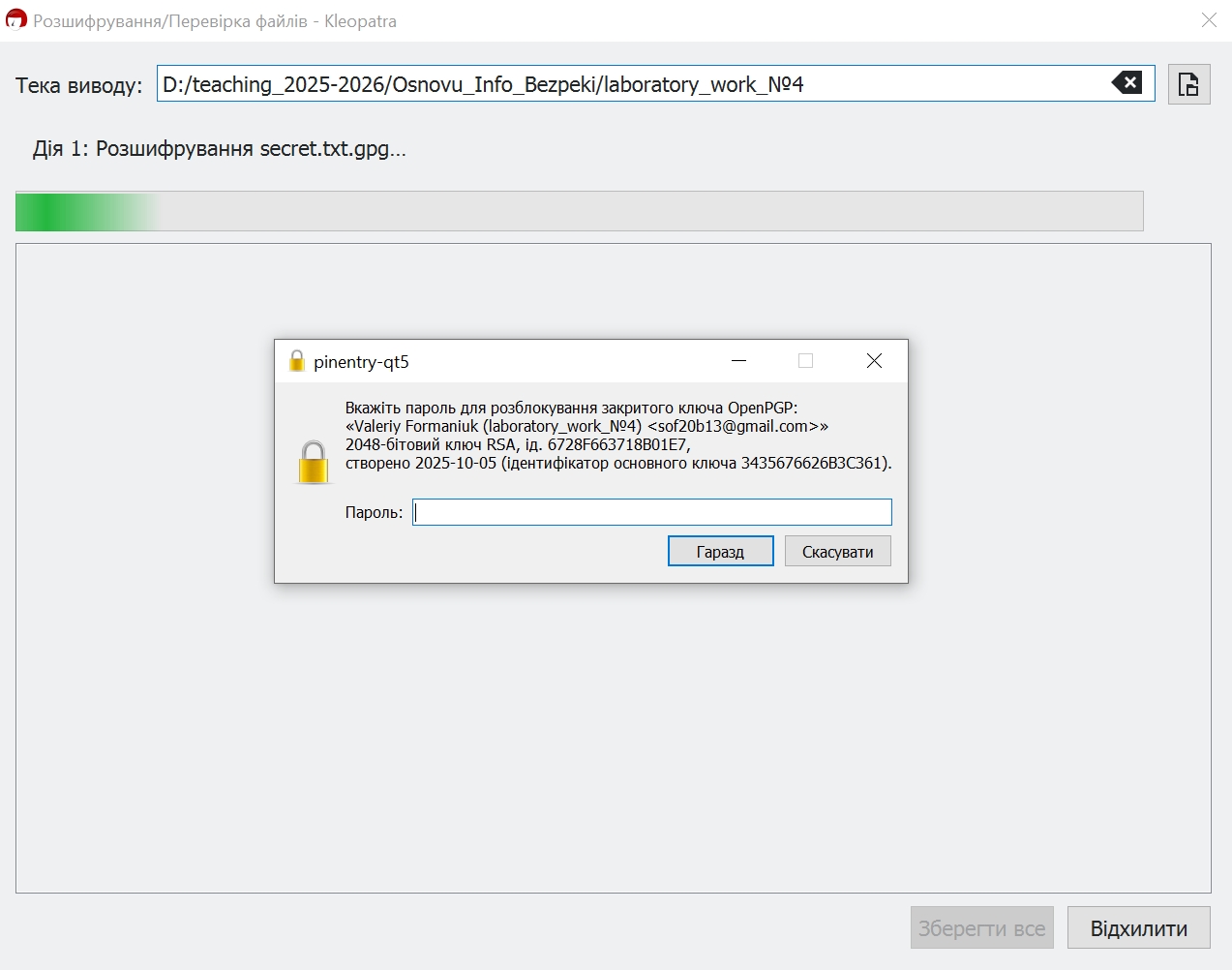
gpg -e -r “Valeriy Formaniuk” secret.txt

дешифрування файлу

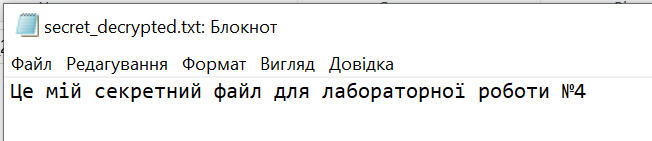
gpg -d .\secret.txt.gpg > .\secret\_decrypted.txt



Скріншот 4: Файл secret.txt

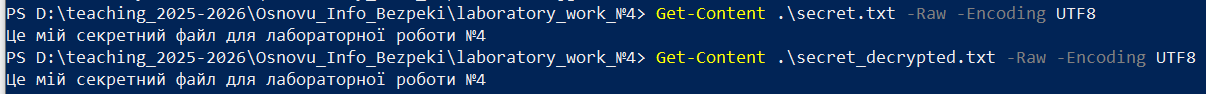


Скріншот 5: Шифрування файлу secret.txt



Скріншот 6: Розшифрування файлу secret.txt.gpg

Порівняння оригіналу та дешифрованого файлу:



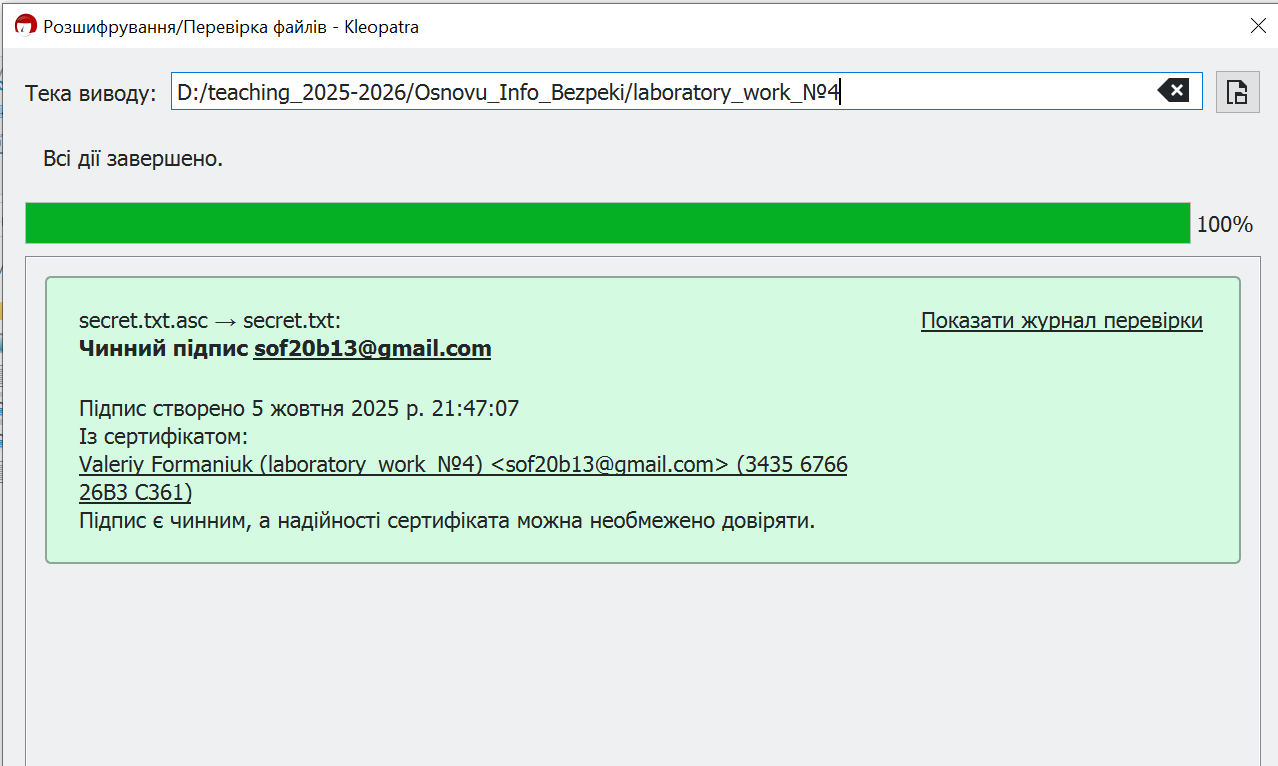
Скріншот 7: Порівняння файлів

## **Частина 3. Цифровий підпис**

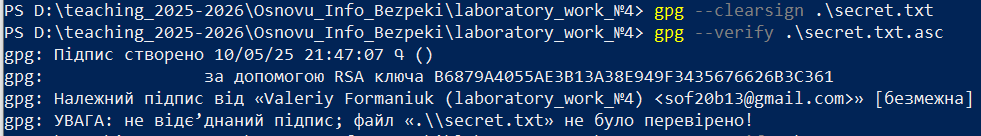
Ввів команди:

gpg clearsign secret.txt

gpg --verify secret.txt.asc



Скріншот 8: Цифровий підпис



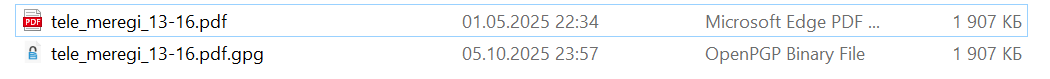
Скріншот 9: Результат перевірки

## **Частина 4. Індивідуальний варіант**

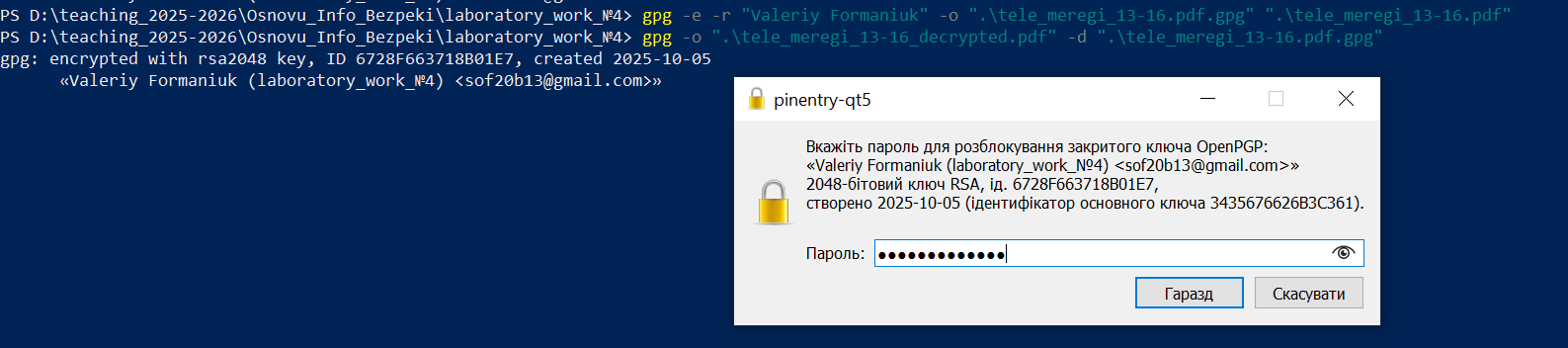
* Виконати шифрування PDF-документа

gpg -e -r "Valeriy Formaniuk" -o ".\tele\_meregi\_13-16.pdf.gpg" ".\tele\_meregi\_13-16.pdf"

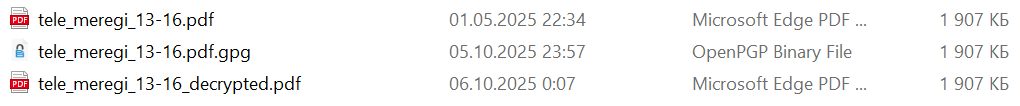
gpg -o ".\tele\_meregi\_13-16\_decrypted.pdf" -d ".\tele\_meregi\_13-16.pdf.gpg"



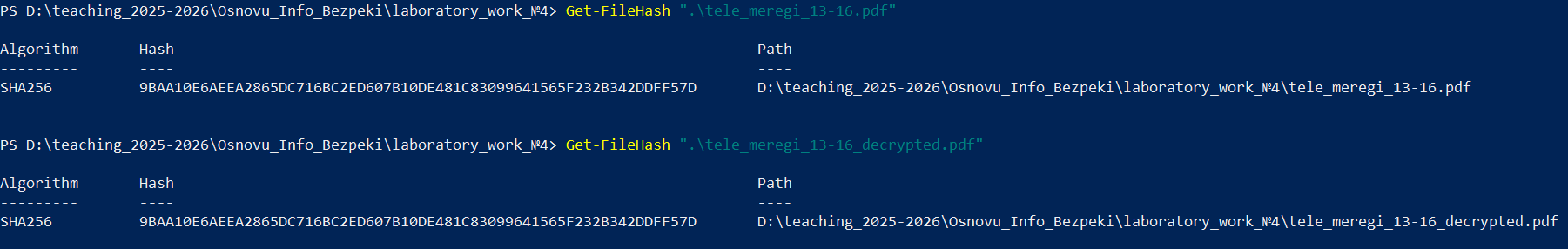
Скріншот 10: Шифрування pdf файлу



Скріншот 11: Розшифрування pdf файлу



Скріншот 12: Розшифрування pdf файлу



Скріншот 13: Порівняння hash pdf

**Висновок:** PDF файл успішно зашифровано асиметричним методом для мого публічного ключа та відновлено приватним ключем. Перевірка на збіг хешів підтвердилась, конфіденційність забезпечено. Розшифрувати файл зможе власник приватного ключа.

## **Частина 5. Контрольні питання**

1. **У чому відмінність між симетричним та асиметричним шифруванням?**

Симетричне шифрування використовує один публічний ключ для обох операцій а асиметричне шифрування використовує пару ключів, публічний та приватний.

1. **Чому приватний ключ не можна передавати?**

Приватний ключ використовується для розшифрування та створення підпису. Передача приватного ключа відкриє доступ до всієї конфіденційної інформації.

1. **Що перевіряє команда gpg - - verify?**

Ця команда перевіряє автентичність підпису та чи не було змінено цілісність файлу.

1. **Які переваги має підпис над простим шифруванням?**

Підпис гарантує не лише конфіденційність, а й авторство та цілісність вайлу.

## **Частина 6. Висновки:**

* Чого я навчився?

Генерувати та керувати ключами RSA/ESS в GPG. Шифрувати/дешифрувати файли асиметрично та симетрично. Створювати та перевіряти підписи. Перевіряти цілісність через Get-FileHash

* Які проблеми виникали?

Кодування в PowerShell: редирект зберігав UTF-16LE і псував кирилицю вирішив через gpg -o, Get-Content\_Encoding UTF8.

* Як можна застосувати це у реальному житті?

Захищати навчальні та особисті документи (звіти, PDF) перед передаванням або зберіганням у хмарі.  
Підписувати файли для підтвердження авторства й цілісності; перевіряти підписи отриманих матеріалів.