МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

Кафедра кібербезпеки

**Звіт до лабораторної роботи № 12**

на тему “ Функціональні можливості програми PGP та її застосування”

Виконав студент(ка) Борщ Дмитро

Група КБ-01

Перевірила Лаврик Т.В

**Суми 2022**

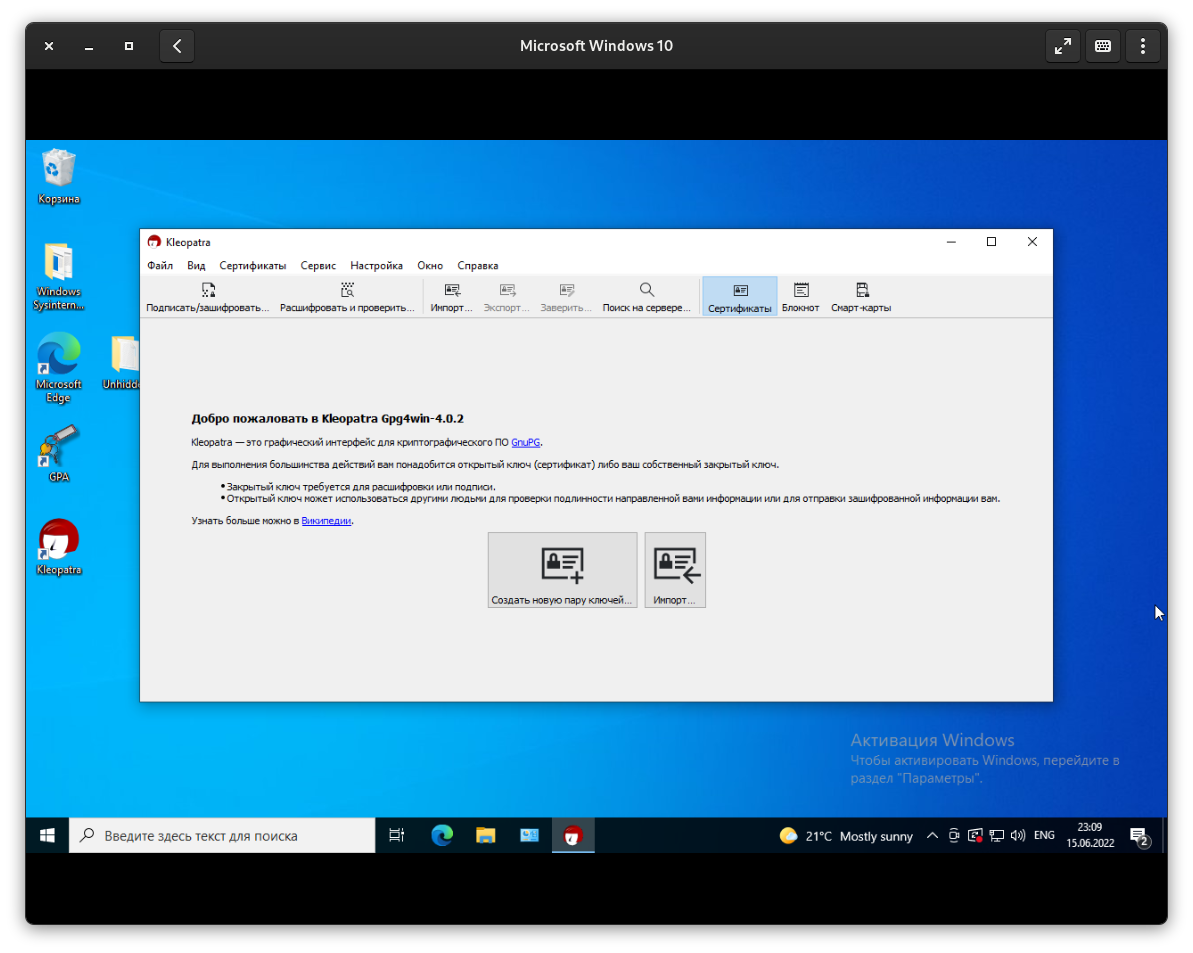
**ЗВІТ 12**

***Примітка:*** Усі дії, що виконуються, у звіті мають супроводжуватися скріншотами.

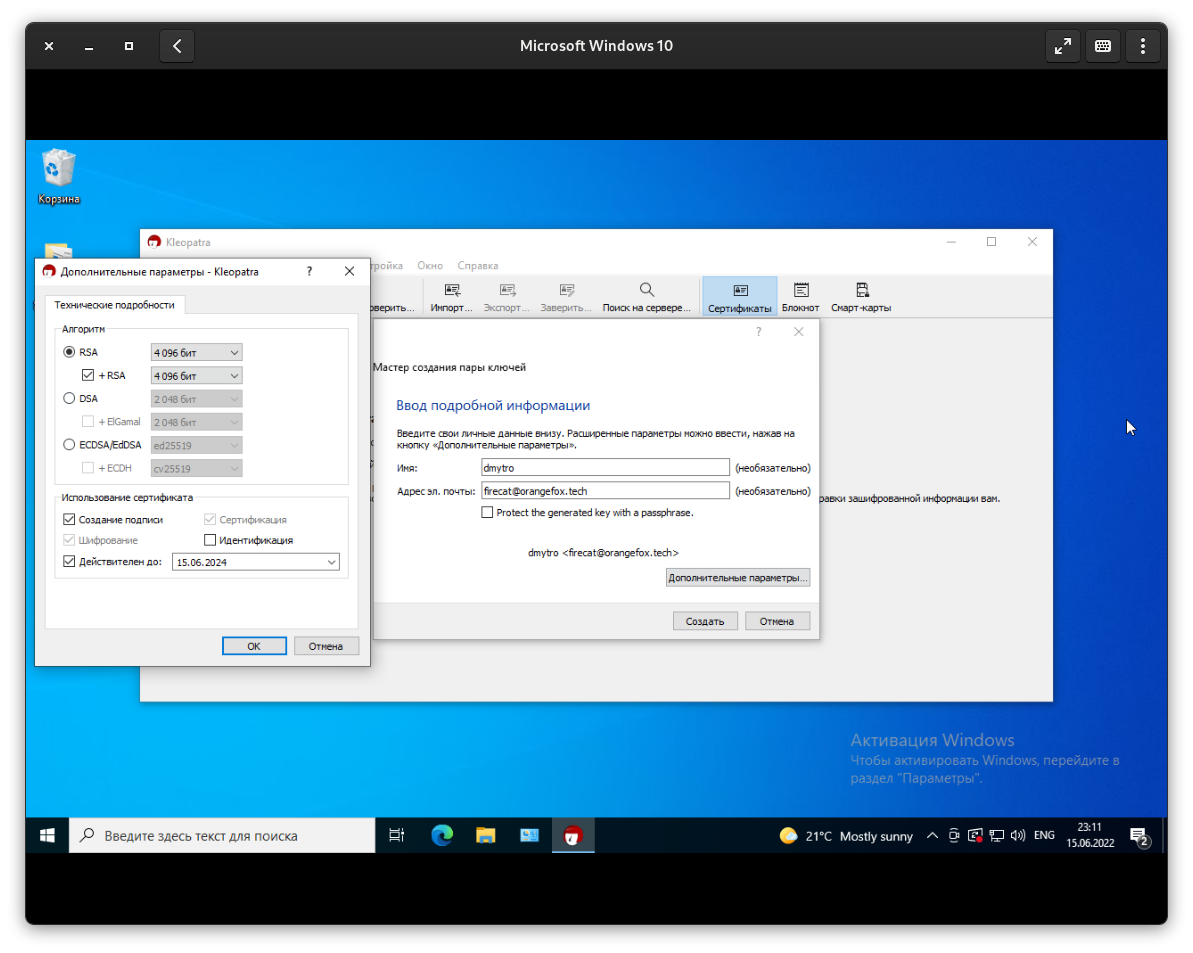
**Завдання і порядок виконання роботи.**

1. Завантажте програму GNU Privacy Guard for Windows (<https://www.gpg4win.org/download.html>) та встановіть її.

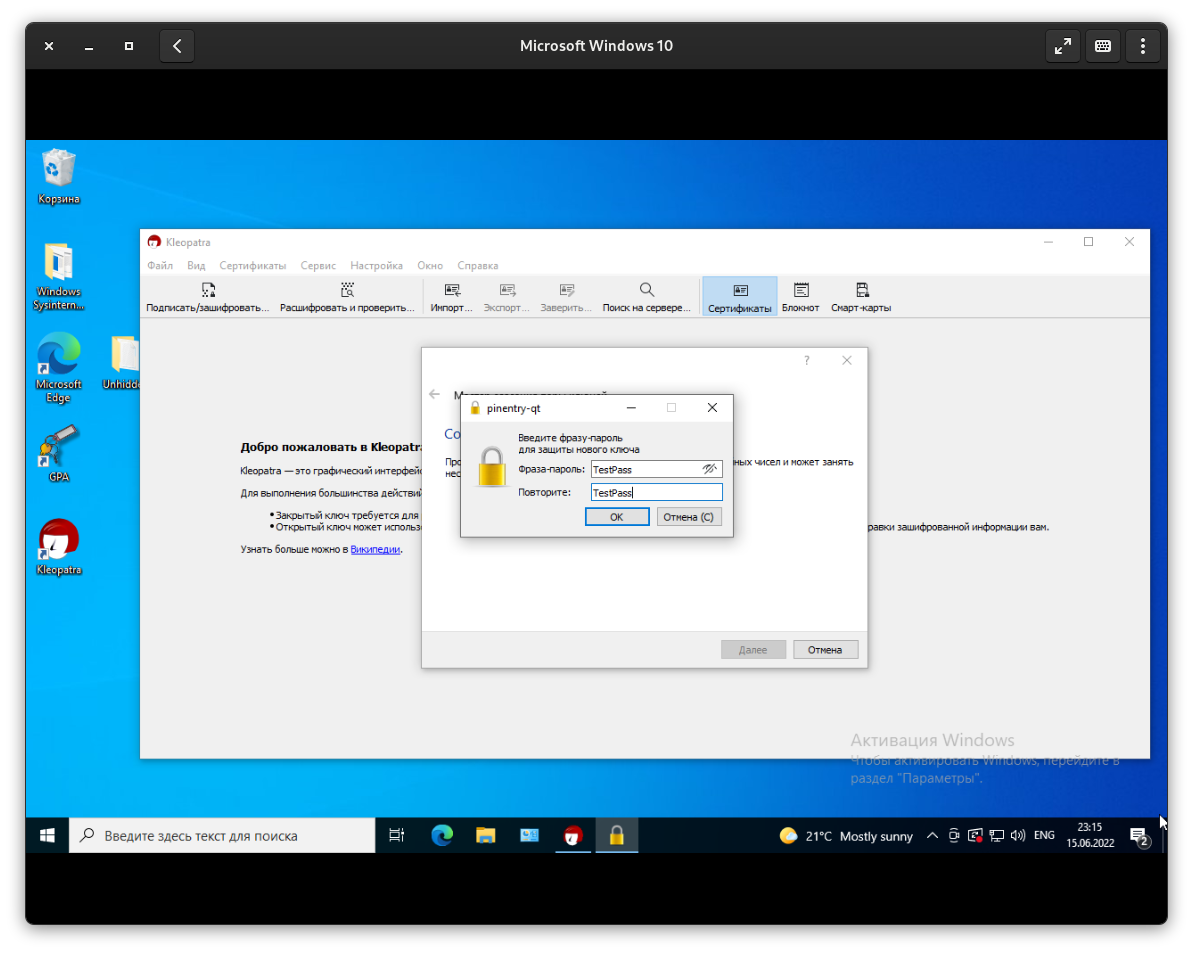
При встановленні оберіть такі компоненти: Kleopatra, GPA, GpgOL, GpgEX.

Рис. 1 — Інтерфейс програми Kleopatra.

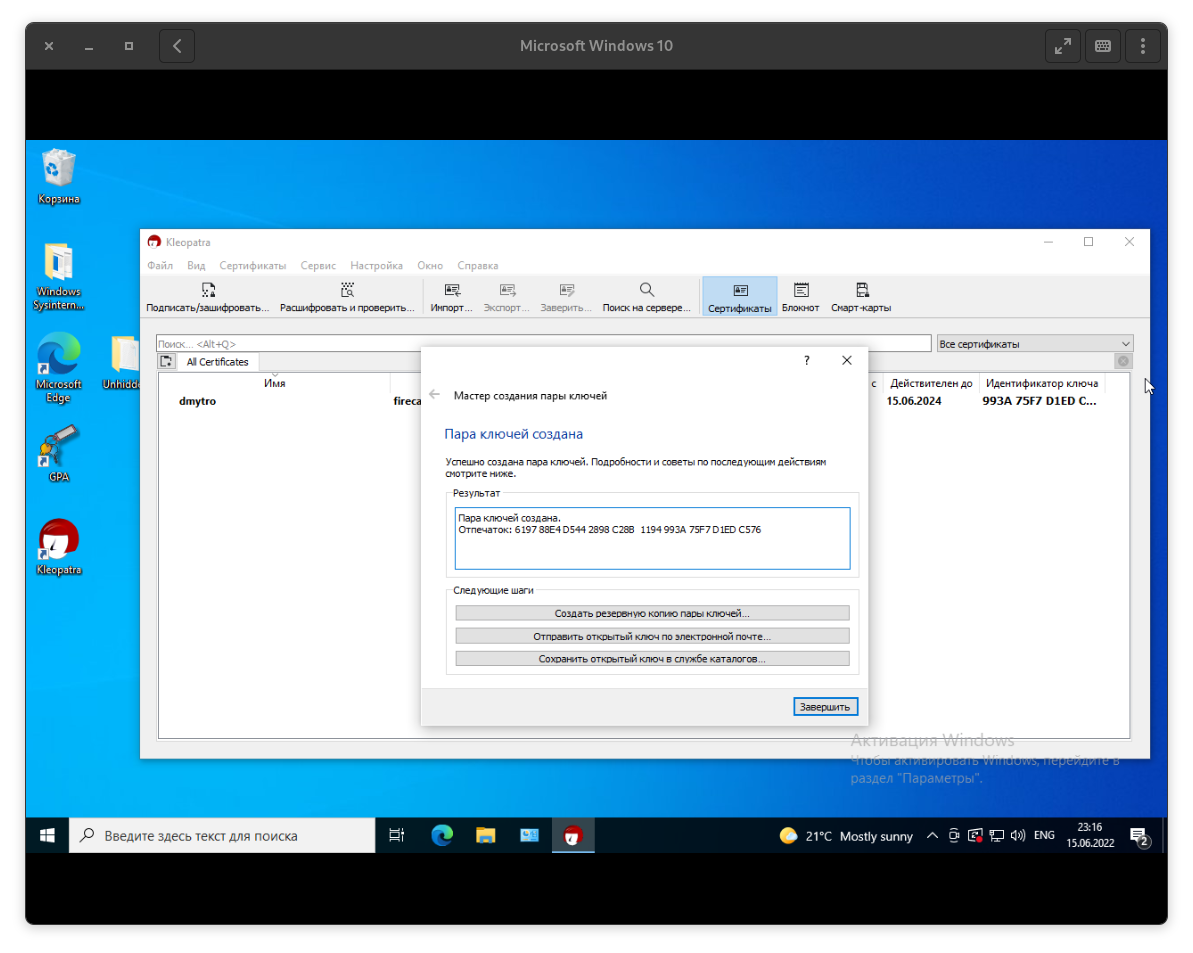
2. Запустіть встановлену програму Kleopatra і створіть пару ключів (відкритий та закритий). При цьому введіть свої дані (Прізвище, ім'я та e-mail) і обов'язково у «Додаткових параметрах» встановіть ключ RSA 4096 біт.

Рис. 2 — Створення пари ключів.

3. Надалі за вимогою програми введіть фразу-пароль, яка потрібна для використання Вами закритого ключа.

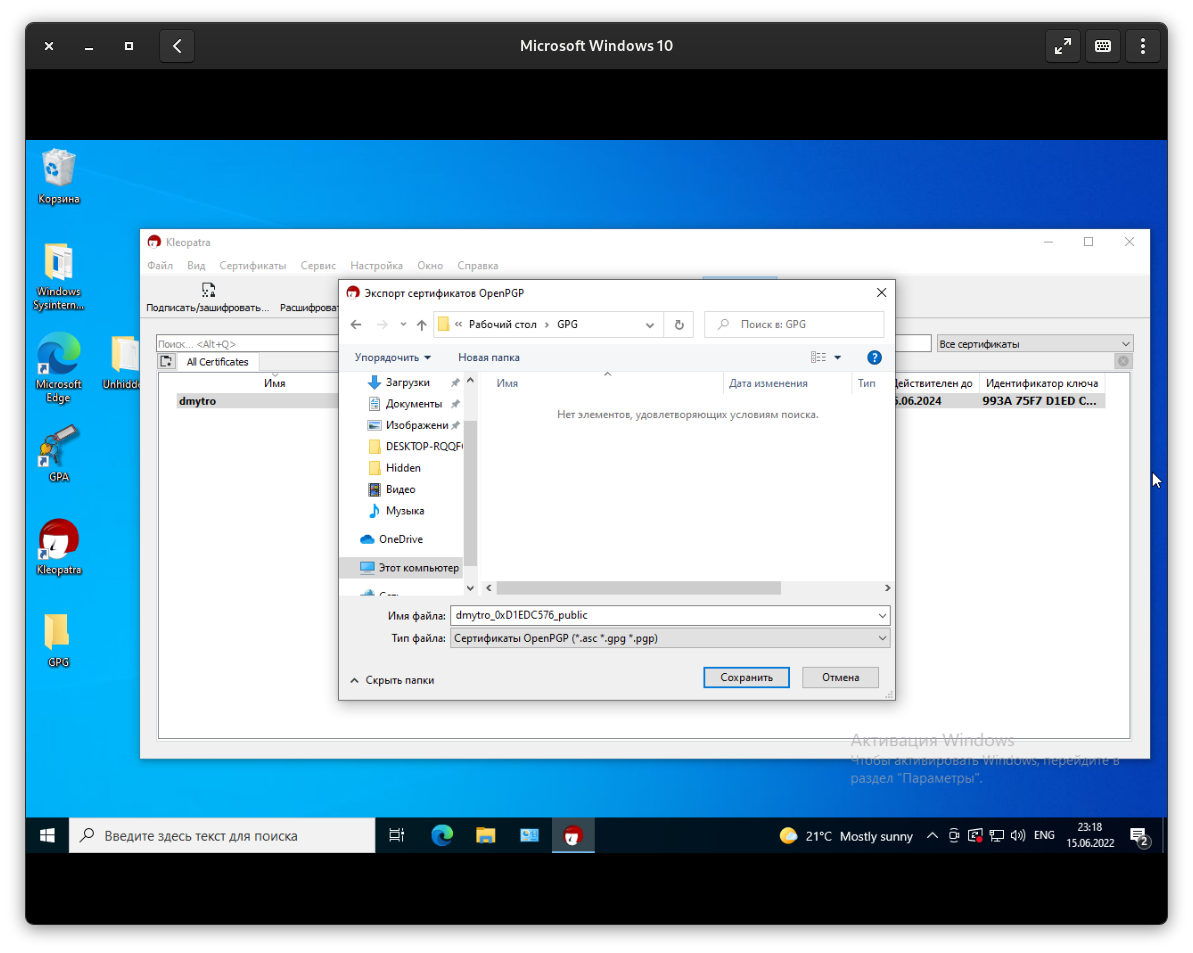
Рис. 3 — Захист паролем.

4. Зробіть висновок: що було створено на початковому етапі.

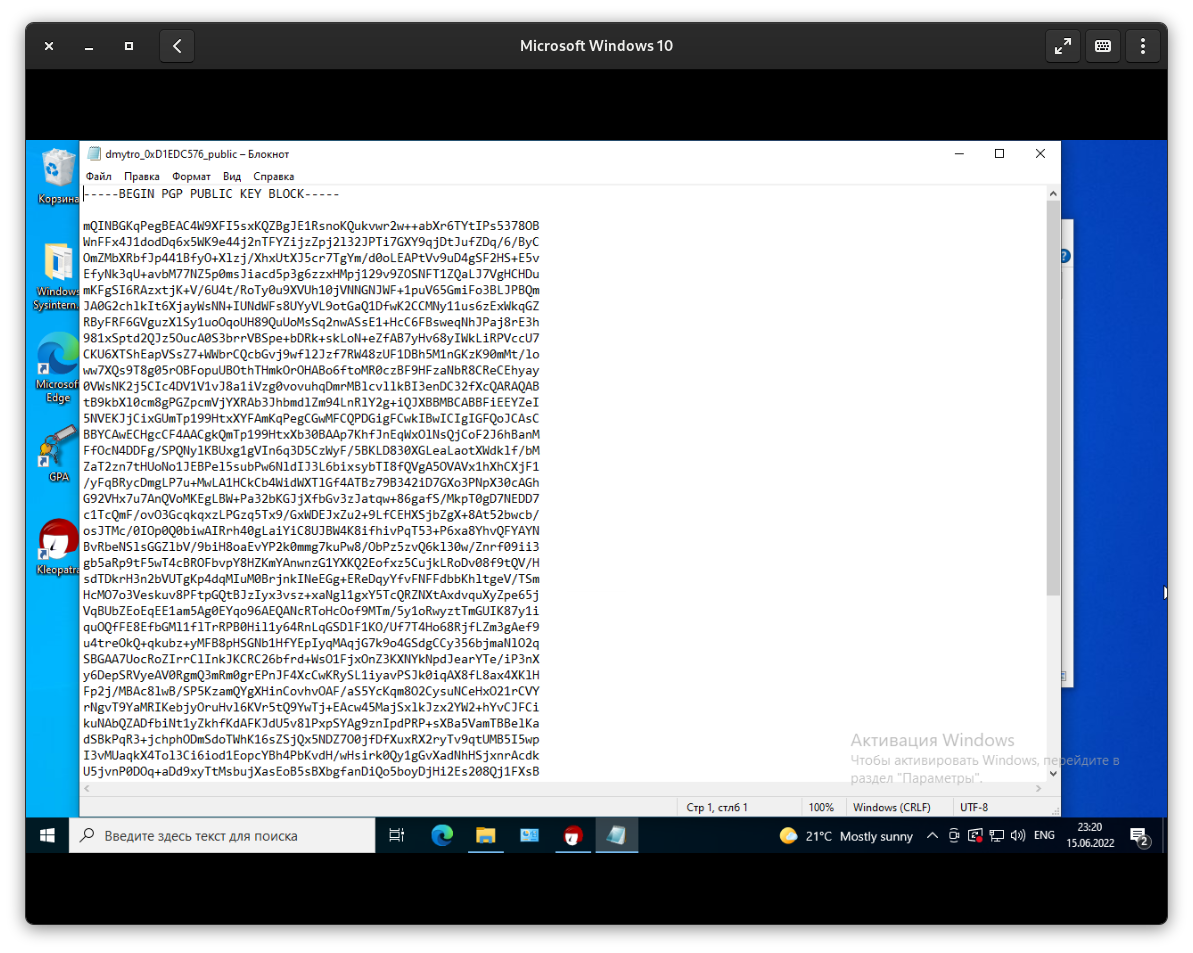
Рис. 4 — Завершення генерації ключів.

На початковому етапі було створено пару ключів, зашифрованих алгоритмом RSA, довжиною 4096 біт, та захищена паролем.

5. Експортуйте ключ (Public Key) для подальшого використання. Для цього оберіть пункт "Експорт" в меню "Файл". Програма запропонує зберегти файл з розширенням **asc**. Збережіть його.

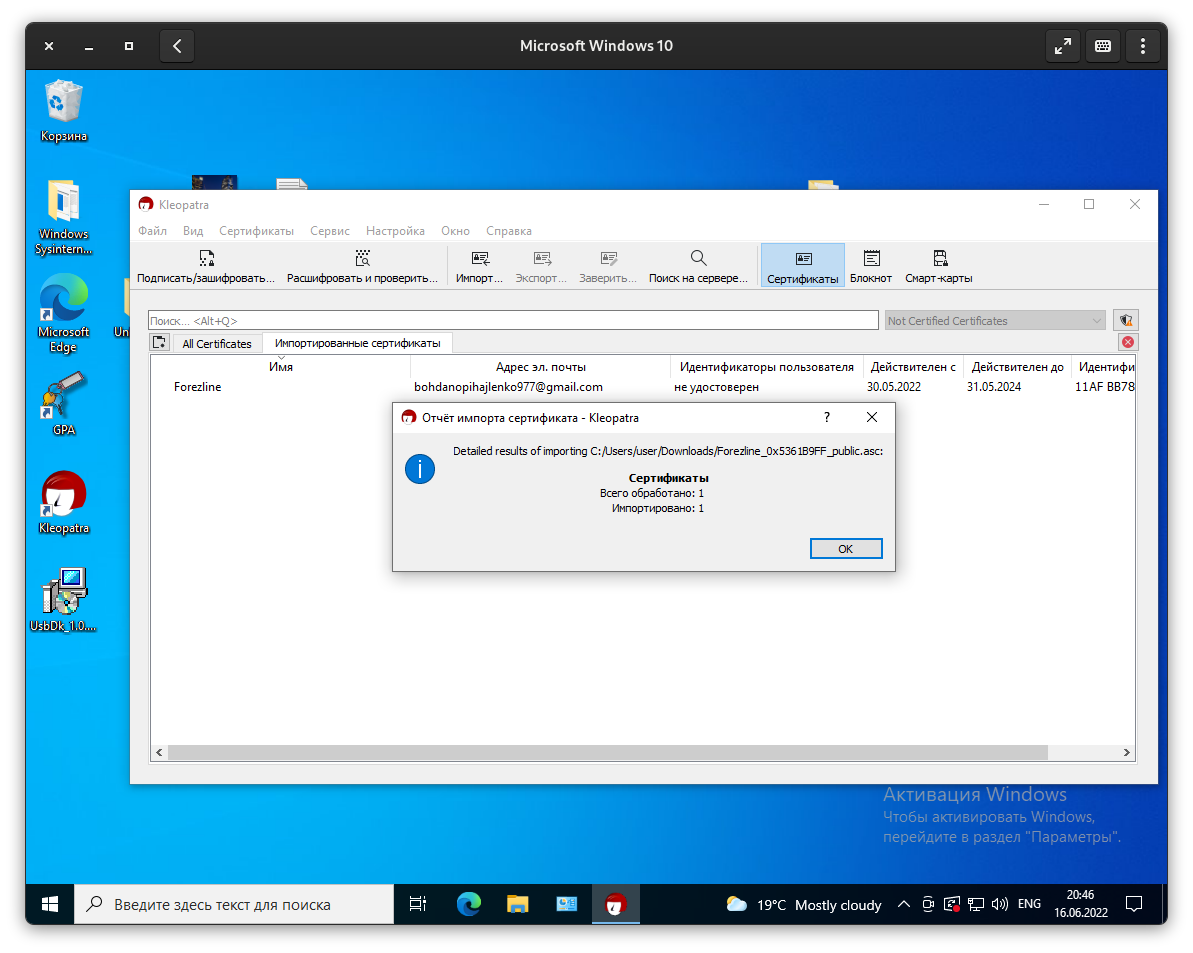
Рис. 5 — Експорт публчного ключа в файл.

6. Відкрийте в Блокноті цей файл і подивіться як виглядає тіло відкритого ключа.

Рис. 6 — Вигляд тіла ключа в текстовому представленні.

7. Здійсніть обмін сертифікатами відкритих ключів з іншим студентом (через електронну пошту, месенджер). Для цього надайте доступ до свого сертифікату відкритого ключа і отримайте сертифікат відкритого ключа одногрупника.

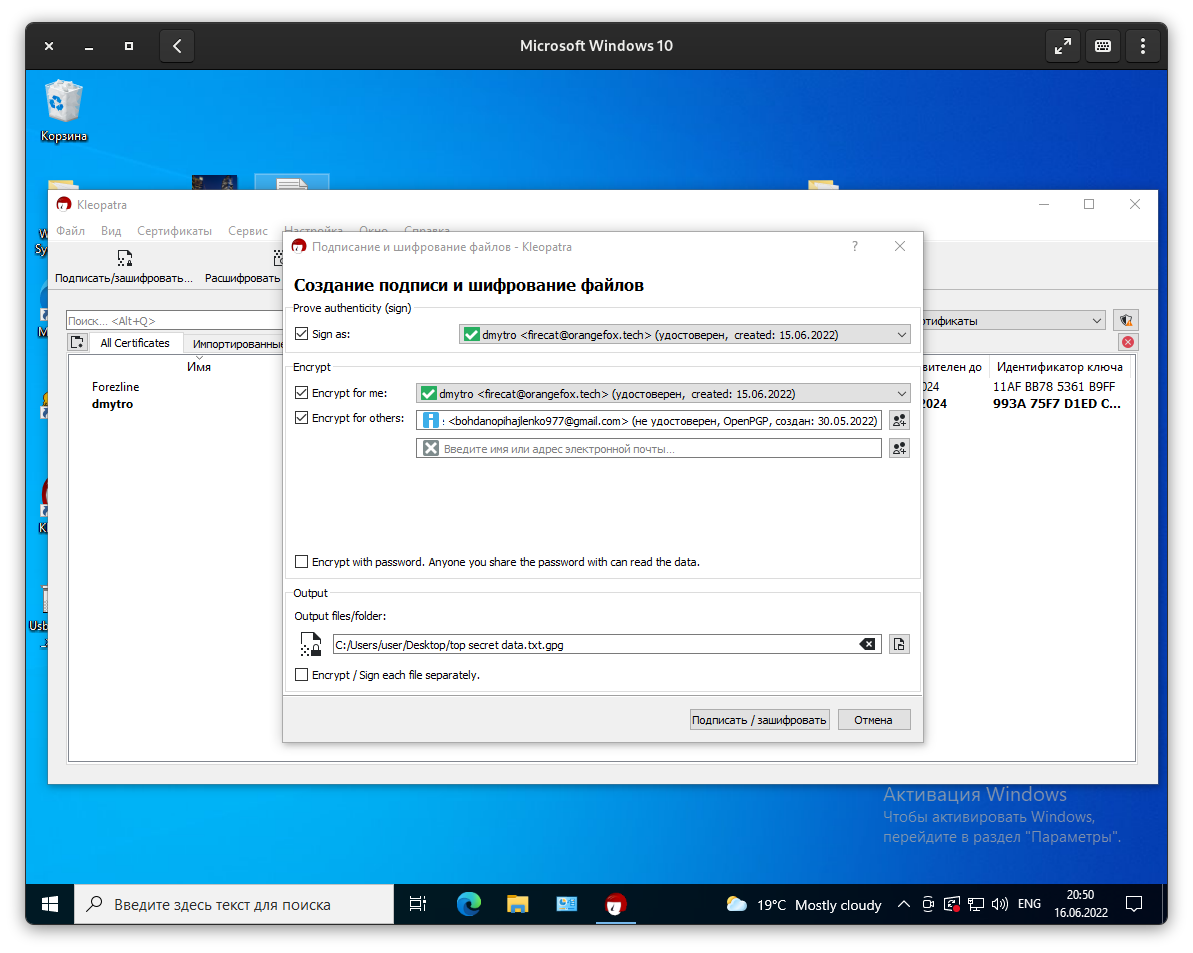
8. Імпортуйте сертифікат відкритого ключа одногрупника у список сертифікатів. Для цього виберіть пункт "Імпорт" в меню "Файл" та відповідний файл \*.asc одногрупника.

Рис. 7 — Імпорт сертифікату одногрупника.

***Шифрування та розшифрування електронного документу***

9. Зашифруйте повідомлення одногрупнику за допомогою його відритого ключа.

Для цього оберіть текстовий файл, який будете шифрувати, і у вікні програми "Kleopatra" виберіть пункт "Підписати / Зашифрувати" в меню "Файл". У вікні, що відкриється, оберіть "Encrypt for others" і завершіть шифрування документу.

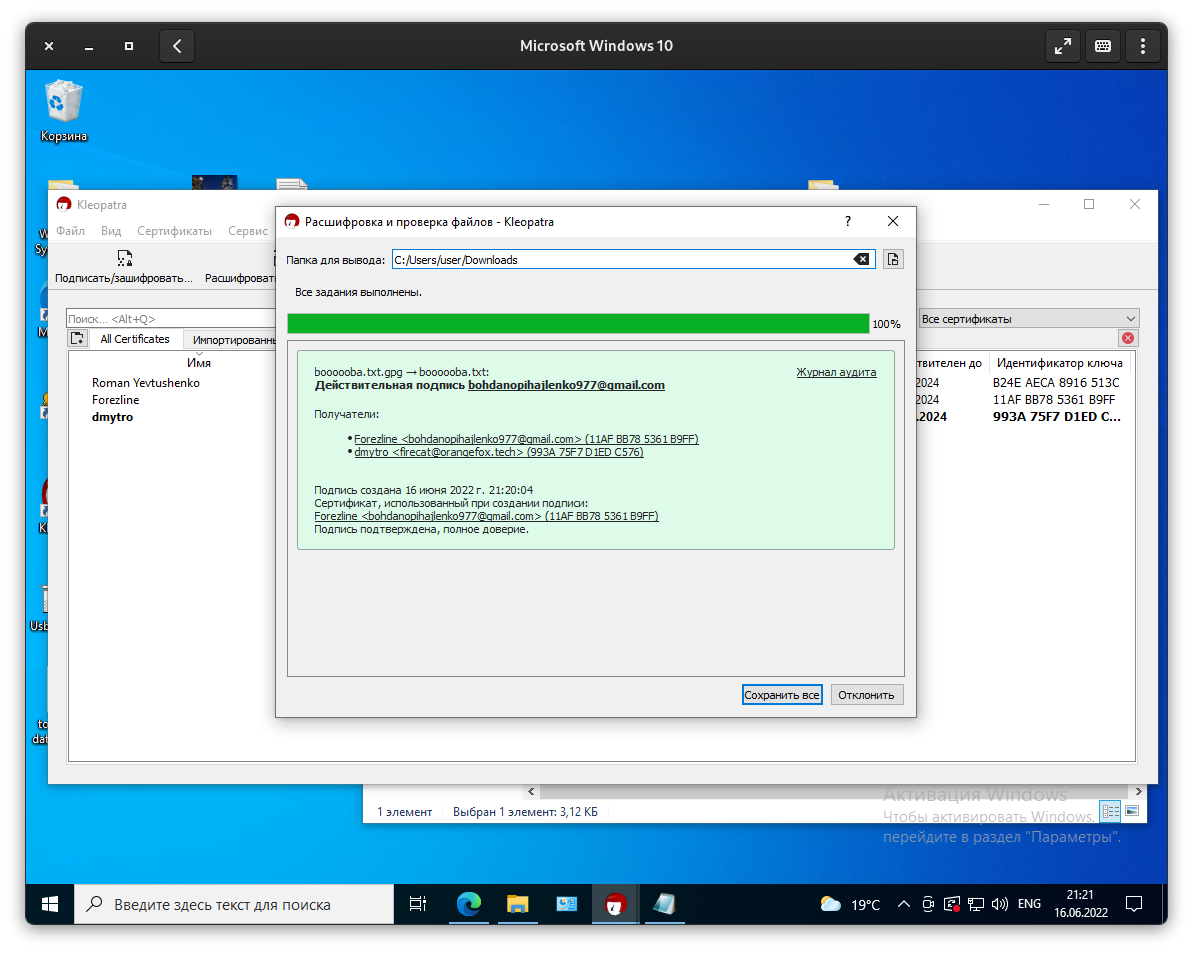
Рис. 8 — Шифрування файлу для одногрупника.

10. Здійсніть обмін зашифрованими повідомленнями з одногрупником (через електронну пошту, месенджер).

11. Розшифруйте отриманий від одногрупника зашифрований файл.

Для розшифрування файлу оберіть пункт "Розшифрувати і перевірити" в меню "Файл" і отриманий зашифрований файл. Скористайтеся власним закритим ключем.

Після успішного процесу розшифрування з'явиться повідомлення та буде створений файл, який містить відкритий текст.

Рис. 9 — Успішне розшифрування файлу.

***Підписання електронного документу***

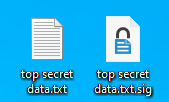
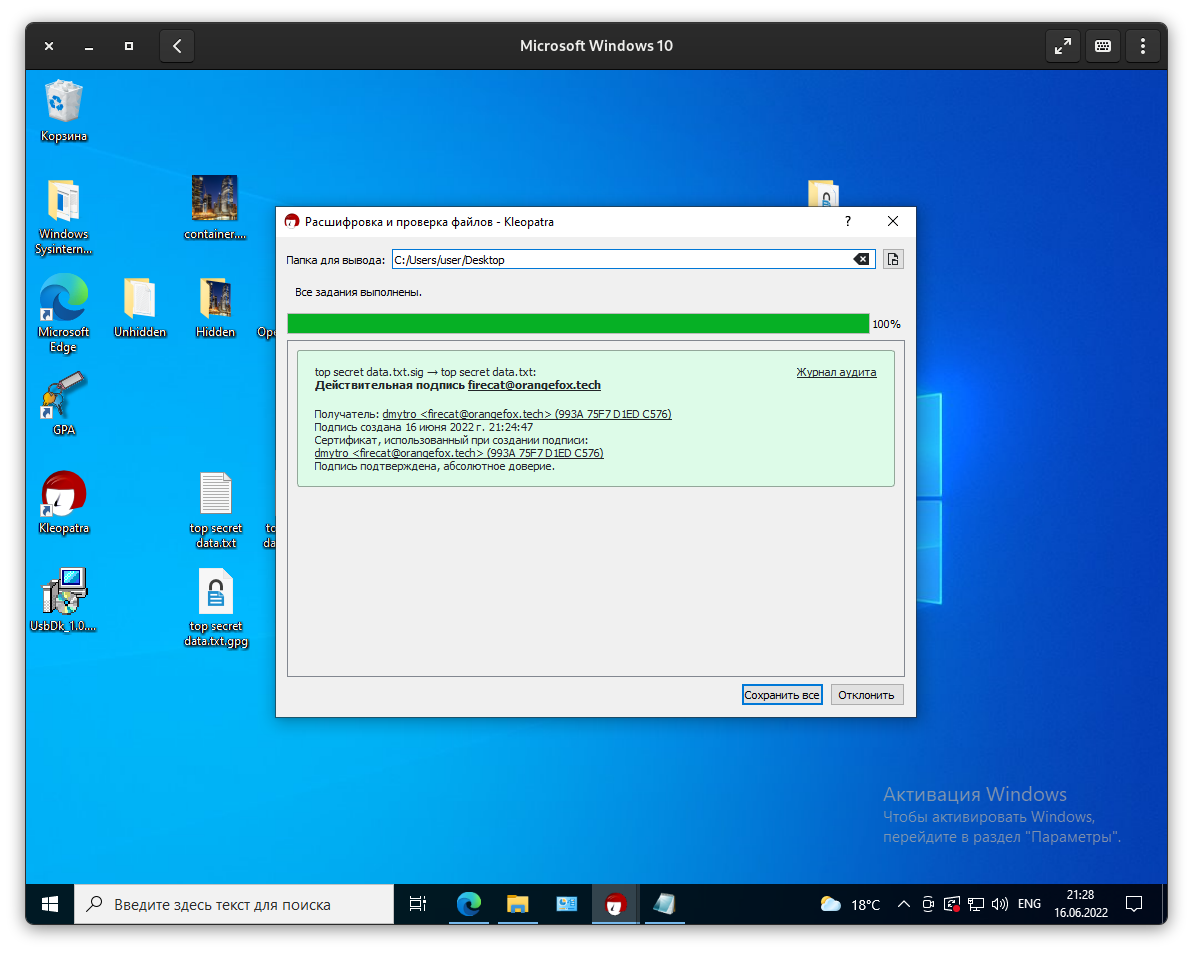
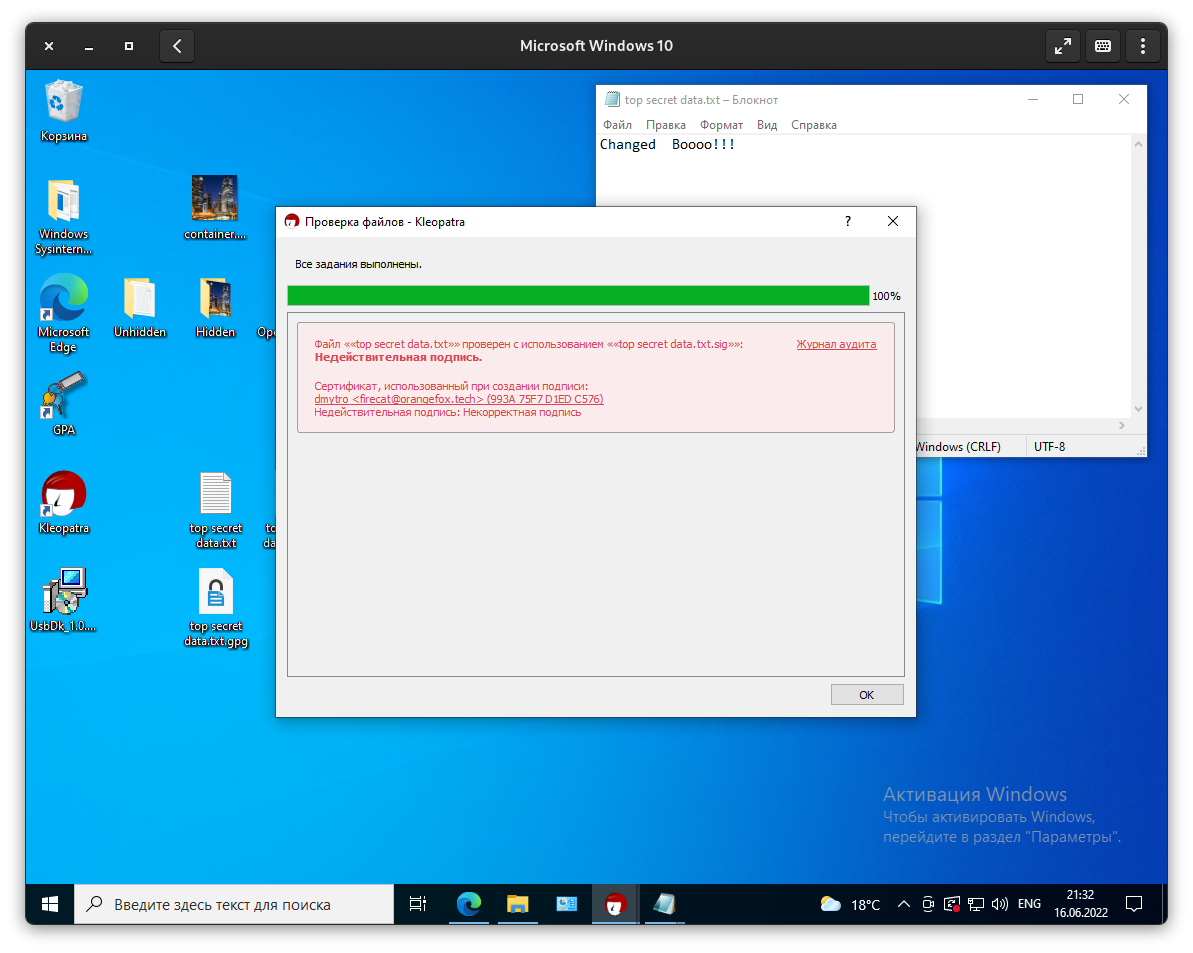
12. Тепер підпишіть Ваш документ (див. п. 9). Після того, як файл буде підписаний, підпис збережеться в окремому файлі з розширенням sig.

Рис. 10 — Збережений підпис.

13. Для перевірки підпису файл з підписом (.sig) перемістіть в один каталог з документом. У контекстному меню файлу з підписом виберіть пункт "More GpgEX options / Verify". Який результат отримано? Збережіть результат перевірки.

Рис. 11 — Успішна перевірка підпису.

14. Після цього внесіть зміни у документ, який підписували, і виконайте ще раз процедуру перевірки. Які зміни відбулися? Збережіть результат.

Рис. 12 — Невдала перевірка підпису.

***Висновки.***

15. Зробіть висновки. У звіті надати відповіді на такі питання:

1) Усі формати файлів, що використовуються і створюються PGP, описуються документом OpenPGP Message Format.

Даний документ визначає такі формати файлів:

**.gpg ;**

**.sig ;**

**.asc .**

Що означає кожне з цих розширень файлів?

*gpg — файл, що зашифрований за допомогою gpg;*

*sig — файл, що містить підпис до певного іншого файлу;*

*asc — файл, що містить публічний ключ.*

2) Які використовуються ключі при шифруванні та розшифруванні повідомлень в асиметричній схемі?

*При шифруванні учасники процесу обміну використувоють свої відкриті ключі, а при розшифруванні — закриті.*

3) Які використовуються ключі при створенні та верифікації цифрового підпису в асиметричній схемі?

*Підписати документ можна лише особистим закритим ключем, а верифікувати відкритим.*