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

ЗВІТ
о виконанні лабораторної роботи №5
з дисципліни «Захист інформації»
за темою «Захищена електронна пошта»

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

Мета роботи: Налаштувати шифрування для захисту особистої електронної кореспонденції та реалізувати власний алгоритм шифрування повідомлень.

Порядок виконання практичної частини

Крок 1. Дослідження PGP-шифрування

1) Завантажити та встановити GPG4Win або GPG Suite для Mac;
2) Згенерувати PGP-ключі для власної електронної адреси;
3) Експортувати публічний ключ для обміну з одногрупниками;
4) Спробувати зашифрувати та розшифрувати тестове повідомлення.

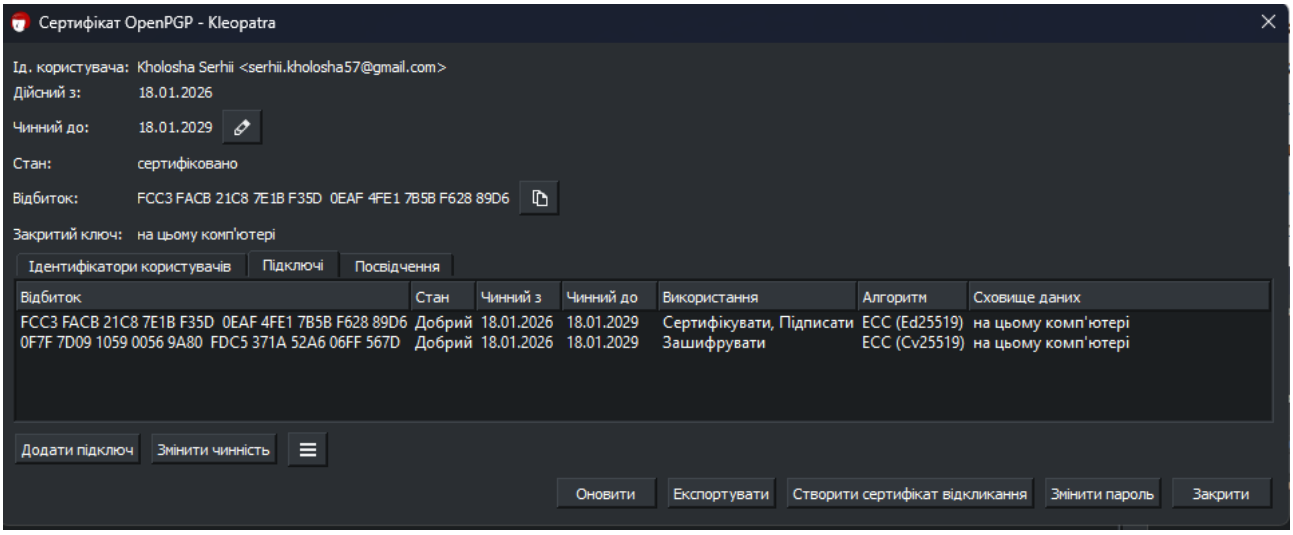

Рис. 1 Створена пара ключів

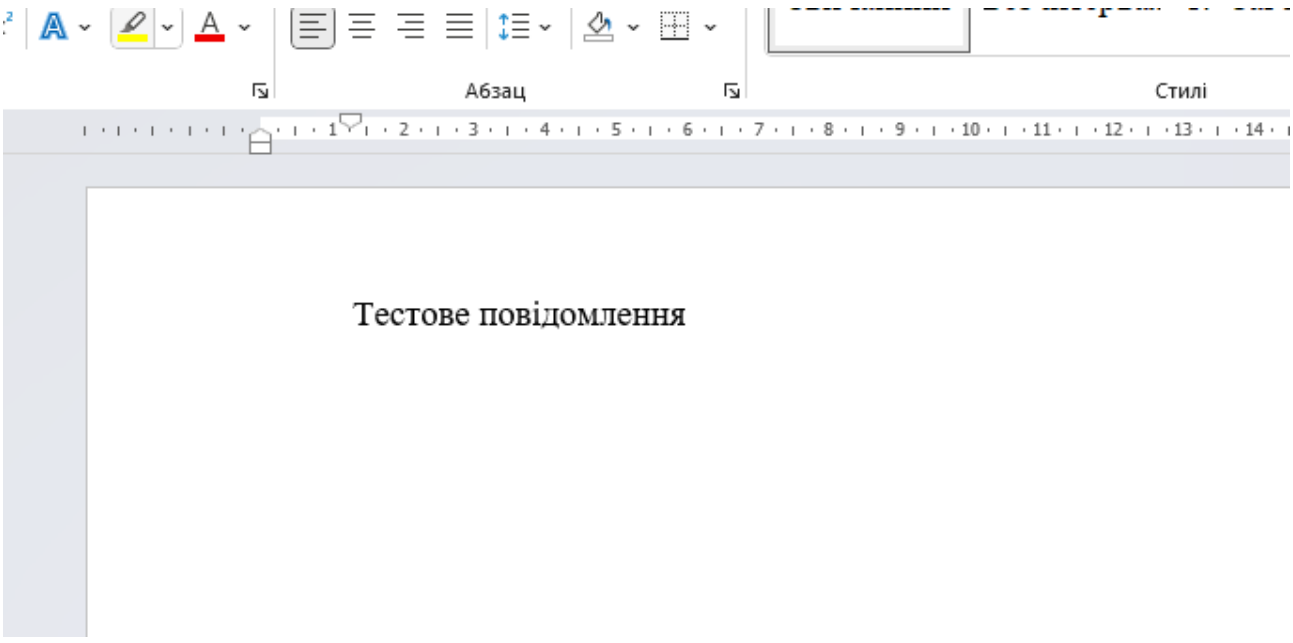

Рис. 2 Створене повідомлення

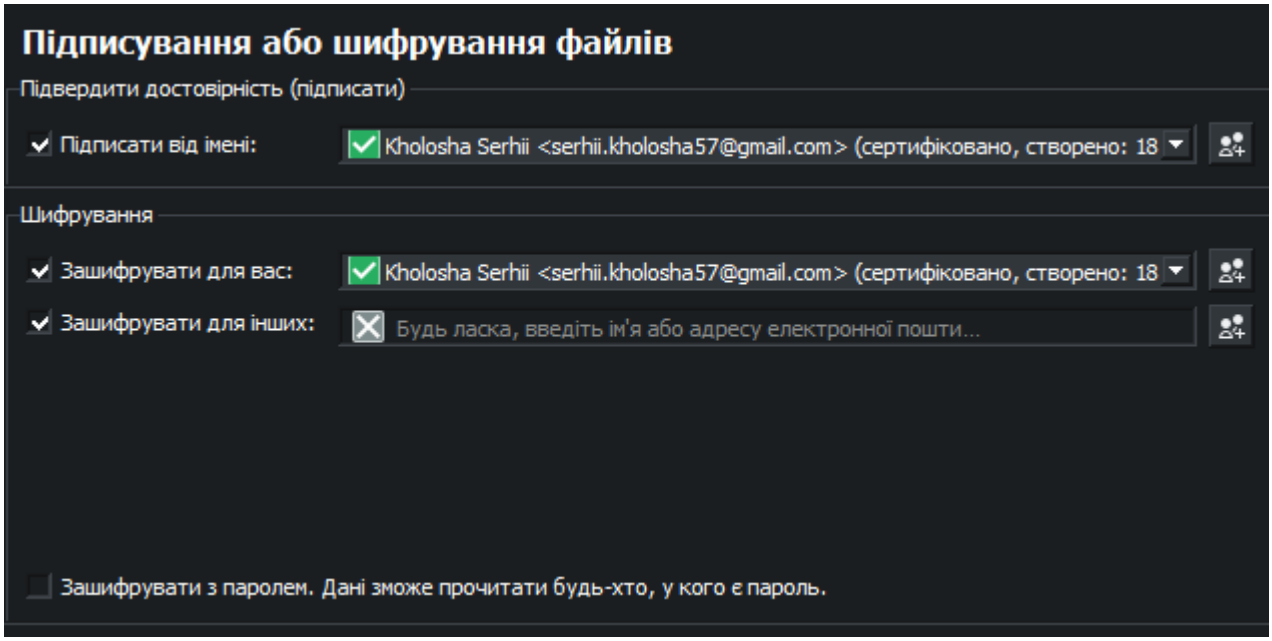

Рис. 3 Параметри шифрування

Рис. 4. Отриманий в результаті файл

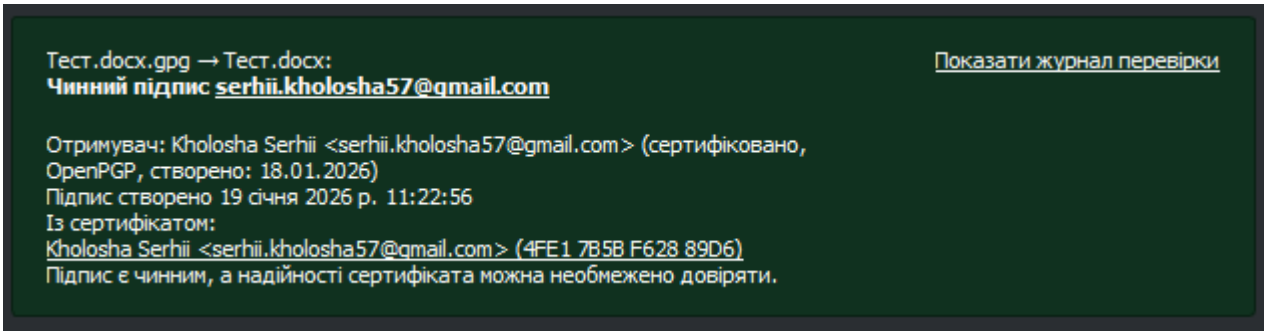

Рис. 5. Розшифрування повідомлення

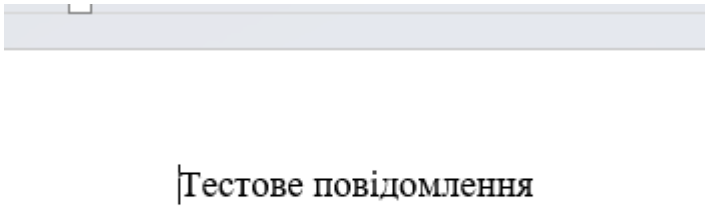

Рис. 6 Повідомлення розшифроване без змін

Крок 2. Зашифрована кореспонденція

1) Обмінятися публічними ключами з одногрупниками;
2) Відправити зашифрований лист з персональним повідомленням;
3) Розшифрувати отримані від інших студентів повідомлення.

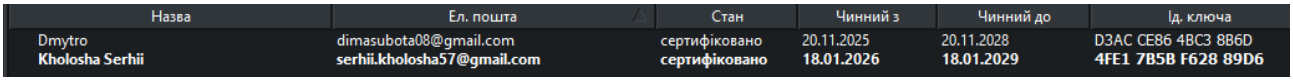

Рис. 7. Імпортований публічний ключ одногрупника

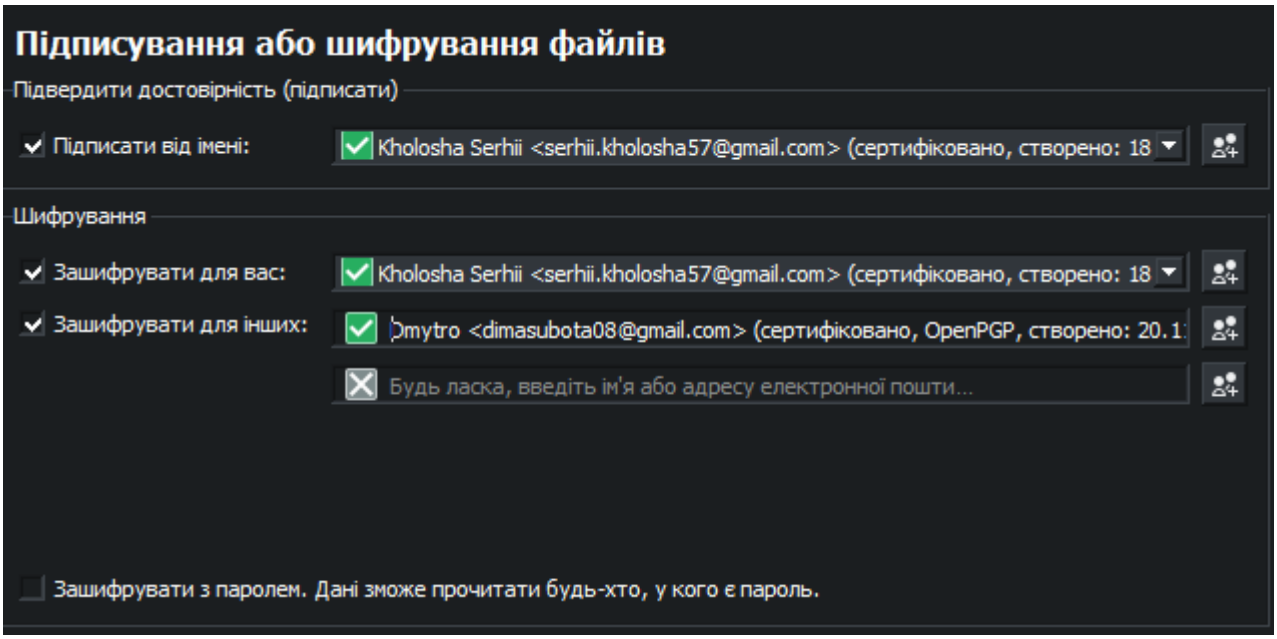

Рис. 8. Шифрування файлу для одногрупника

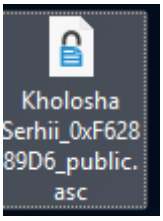

Рис. 9 Експортований особистий ключ

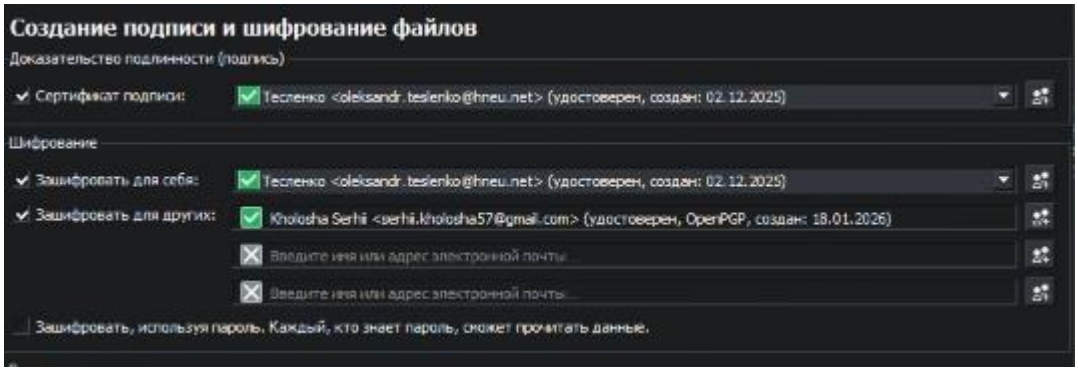

Рис. 10 Параметри шифрування одногрупника

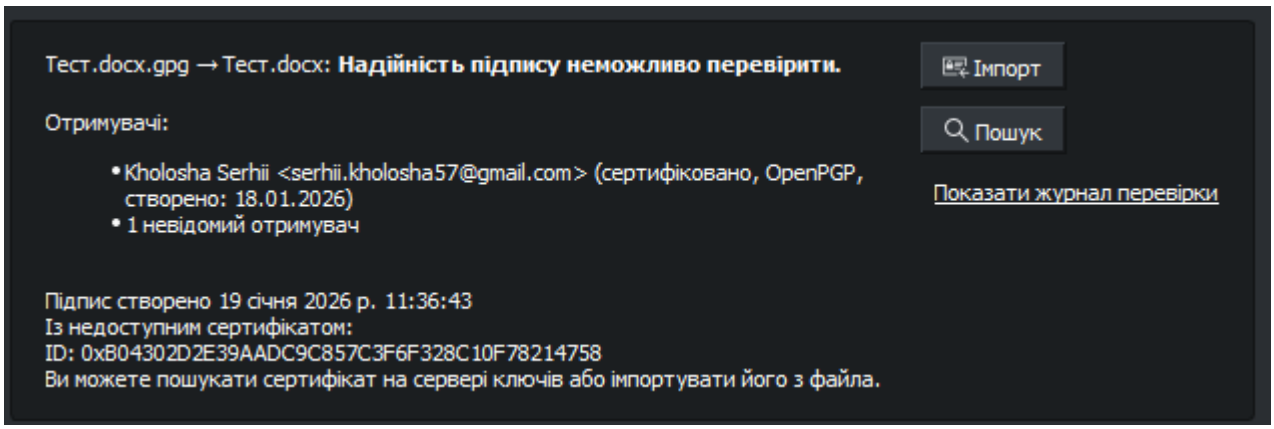

Рис. 11 Розшифрування файлу

На зображенні бачимо напис «надійність підпису неможливо перевірити», він виникає з тої причини що в моєму клієнті Kleopatra не імпортований ключ одногрупника який шифрував повідомлення для мене

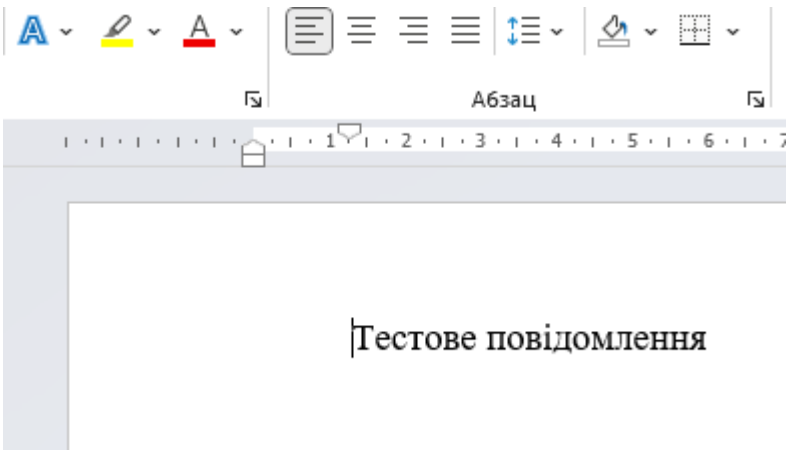

Рис. 12 Повідомлення розшифроване без змін

Крок 3. Аналіз безпеки електронної пошти

1) Порівняти заголовки звичайного та зашифрованого листа;
2) Дослідити метадані, що залишаються видимими після шифрування;
3) Оцінити рівень приватності, досягнутий за допомогою шифрування.

```
MIME-Version: 1.0
Date: Mon, 19 Jan 2026 11:42:15 +0200
Message-ID: <CAOd_q1H7jZdVXEY5_B7k4WNe--9h4KhD5G5JcMsJkuv-=4VhqQ@mail.gmail.com>
Subject: Файл без шифрування
From: "Сергій Холоша" <serhii.kholosha57@gmail.com>
To: "Сергій Холоша" <serhii.kholosha57@gmail.com>
Content-Type: multipart/mixed; boundary="00000000000096cc310648ba8135"

--00000000000096cc310648ba8135
Content-Type: multipart/alternative; boundary="00000000000096cc2f0648ba8133"

--00000000000096cc2f0648ba8133
Content-Type: text/plain; charset="UTF-8"



--00000000000096cc2f0648ba8133
Content-Type: text/html; charset="UTF-8"

<div dir="ltr"><br></div>

--00000000000096cc2f0648ba8133--
--00000000000096cc310648ba8135
Content-Type: application/vnd.openxmlformats-officedocument.wordprocessingml.document; name="Тест.docx"
Content-Disposition: attachment; filename="Тест.docx"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_mkkz7u7a0
Content-ID: <f_mkkz7u7a0>


--00000000000096cc310648ba8135--
```

Рис. 13 Оригінал повідомлення без шифрування

```
MIME-Version: 1.0
Date: Mon, 19 Jan 2026 11:42:28 +0200
Message-ID: <CAOd_q1HydYYbLKQ9T-DbAOeDuibmFDJaxZ9U+8e5mv88VBx9ww@mail.gmail.com>
Subject: Файл з шифруванням
From: "Сергій Холоша" <serhii.kholosha57@gmail.com>
To: "Сергій Холоша" <serhii.kholosha57@gmail.com>
Content-Type: multipart/mixed; boundary="0000000000006a34420648ba821e"

--0000000000006a34420648ba821e
Content-Type: multipart/alternative; boundary="0000000000006a34410648ba821c"

--0000000000006a34410648ba821c
Content-Type: text/plain; charset="UTF-8"



--0000000000006a34410648ba821c
Content-Type: text/html; charset="UTF-8"

<div dir="ltr"><br></div>

--0000000000006a34410648ba821c--
--0000000000006a34420648ba821e
Content-Type: application/octet-stream; name="Тест.docx.gpg"
Content-Disposition: attachment; filename="Тест.docx.gpg"
Content-Transfer-Encoding: base64
X-Attachment-Id: f_mkkz85gj0
Content-ID: <f_mkkz85gj0>


--0000000000006a34420648ba821e--
```

Рис. 14 Оригінал повідомлення з шифруванням

Оригінали листів є ідентичними за змістом, відрізняються лише надісланим файлом

Технічне завдання

Завдання: Реалізувати простий алгоритм шифрування електронних повідомлень для демонстрації принципів захищеної комунікації.

Обов'язкові функціональні вимоги:

– шифрування тексту повідомлень за допомогою симетричного алгоритму;

– розшифрування отриманих зашифрованих повідомлень;

– генерація ключів на основі персональних даних користувачів;

– демонстрація процесу безпечного обміну повідомленнями.

Приклад реалізації:

Email-шифратор з функціоналом:

– Електронна адреса: ivan.petrenko@gmail.com;

– Ключ шифрування: хеш від "IvanPetrenko1995";

– Повідомлення: "Зустрічаємося завтра о 15:00";

– Зашифровані дані: "U2FsdGVkX1+vupppZksvRf5pq5g5XjFRIipRkwB0K1Y96Qsv2Lelz/…";

– Процес розшифрування у отримувача.

Технології реалізації: мова програмування, фреймворк та тип програми – на ваш вибір.

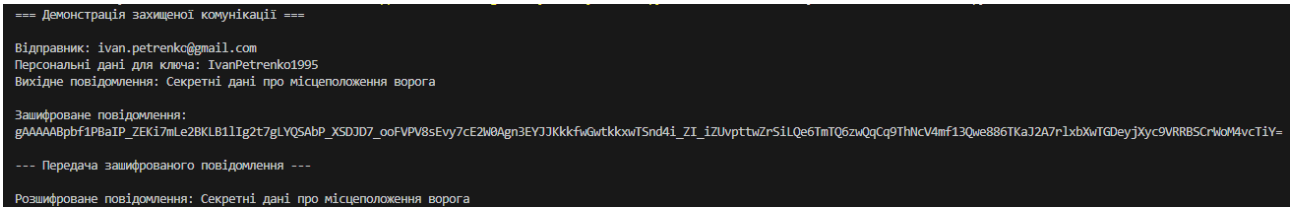

Рис. 15 Виконання програми

Посилання на GitHub: [zahist-informaciji/lab5 at main · serhiikholosha57/zahist-informaciji]

Висновок: в ході лабораторної роботи було налаштовано шифрування для захисту особистої електронної кореспонденції та реалізовано власний алгоритм шифрування повідомлень