

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСКИЙ 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.

Мета роботи: Налаштuvати 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.

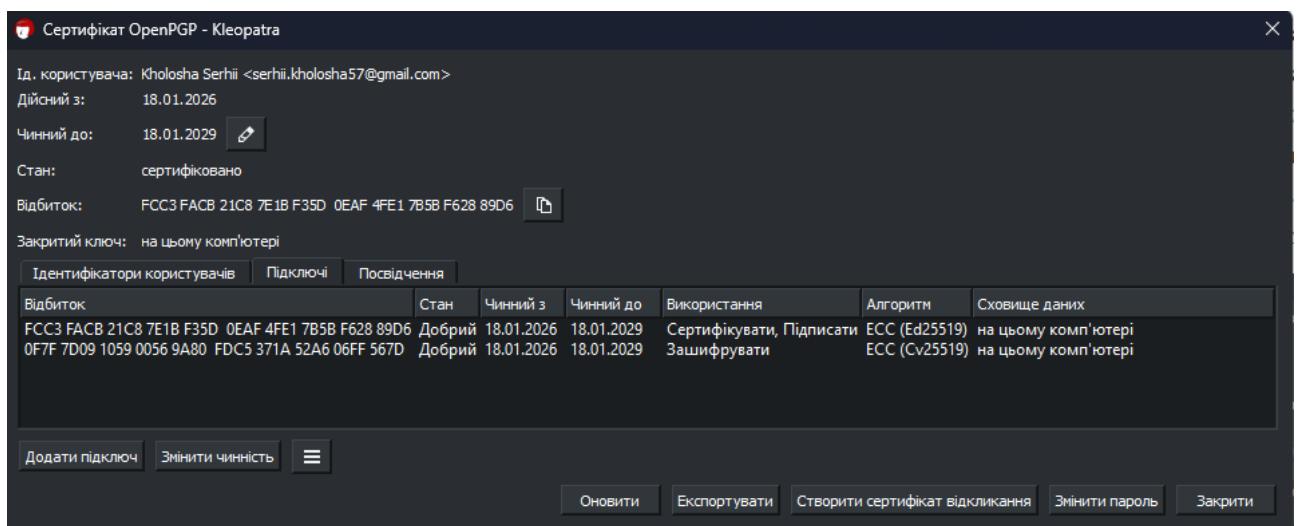


Рис. 1 Створена пара ключів

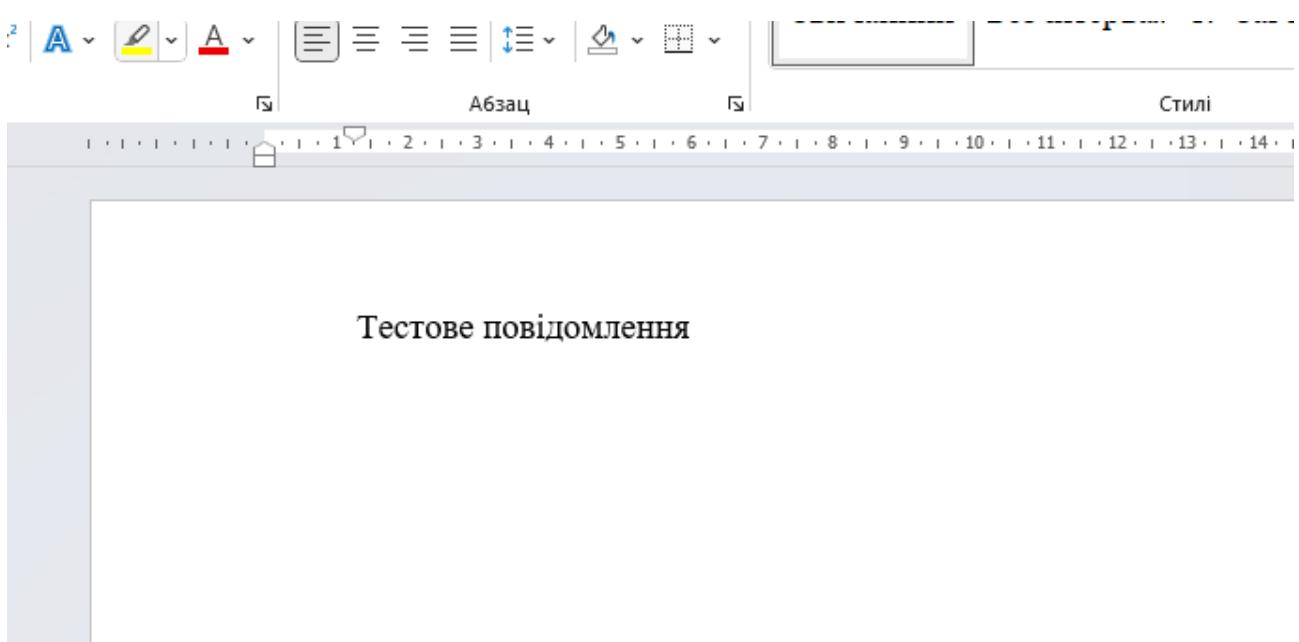


Рис. 2 Створене повідомлення

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.

Рис. 3 Параметри шифрування

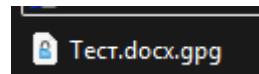


Рис. 4. Отриманий в результаті файл

Test.docx.gpg → Test.docx:
Чинний підпис [serhii.kholosha57@gmail.com](#) [Показати журнал перевірки](#)

Отримувач: Kholosha Serhii <serhii.kholosha57@gmail.com> (сертифіковано, OpenPGP, створено: 18.01.2026)
Підпис створено 19 січня 2026 р. 11:22:56
Із сертифікатом:
[Kholosha Serhii <serhii.kholosha57@gmail.com> \(4FE1 7B5B F628 89D6\)](#)
Підпис є чинним, а надійності сертифіката можна необмежено довіряти.

Рис. 5. Розшифрування повідомлення

| Тестове 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.

Назва	Ел. пошта	Стан	Чинний з	Чинний до	Ід. ключа
Dmytro Kholosha Serhii	dimasubota08@gmail.com serhii.kholosha57@gmail.com	сертифіковано сертифіковано	20.11.2025 18.01.2026	20.11.2028 18.01.2029	D3AC CE86 4BC3 886D 4FE1 7B5B F628 89D6

Рис. 7. Імпортований публічний ключ одногрупника

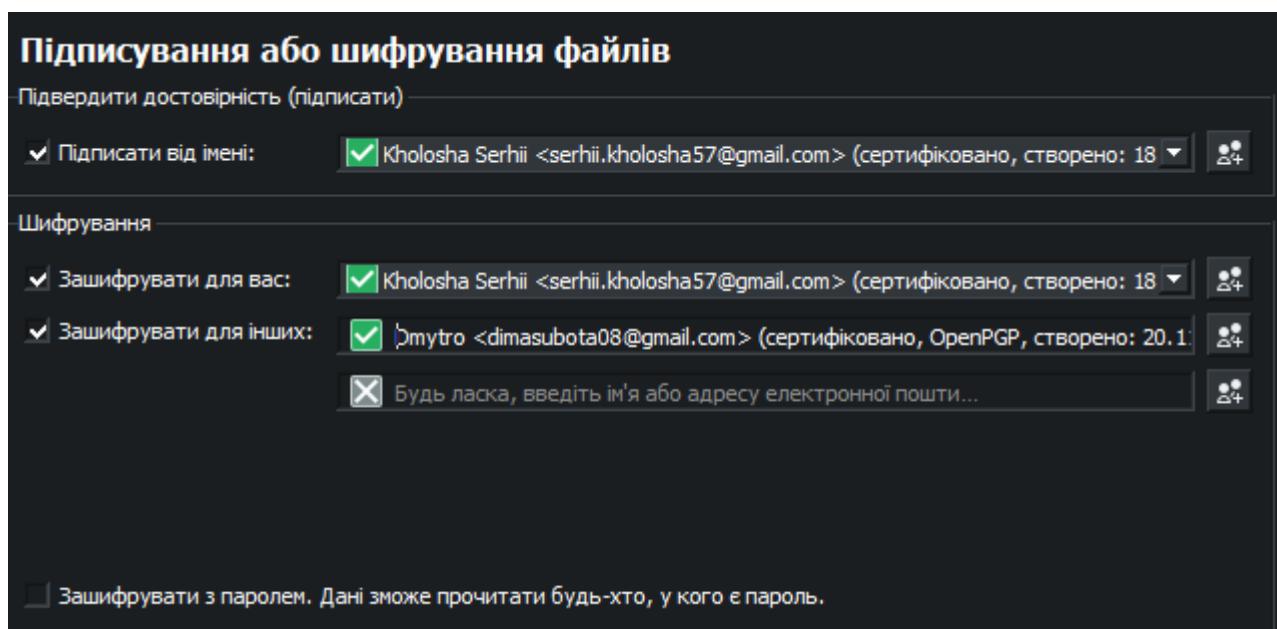


Рис. 8. Шифрування файлу для одногрупника

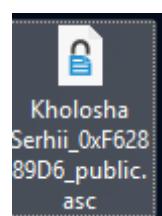


Рис. 9 Експортований особистий ключ

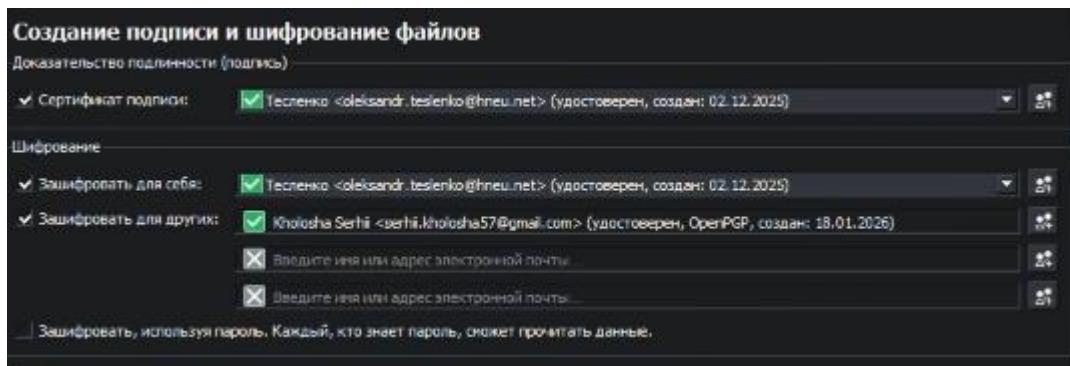


Рис. 10 Параметри шифрування одногрупника

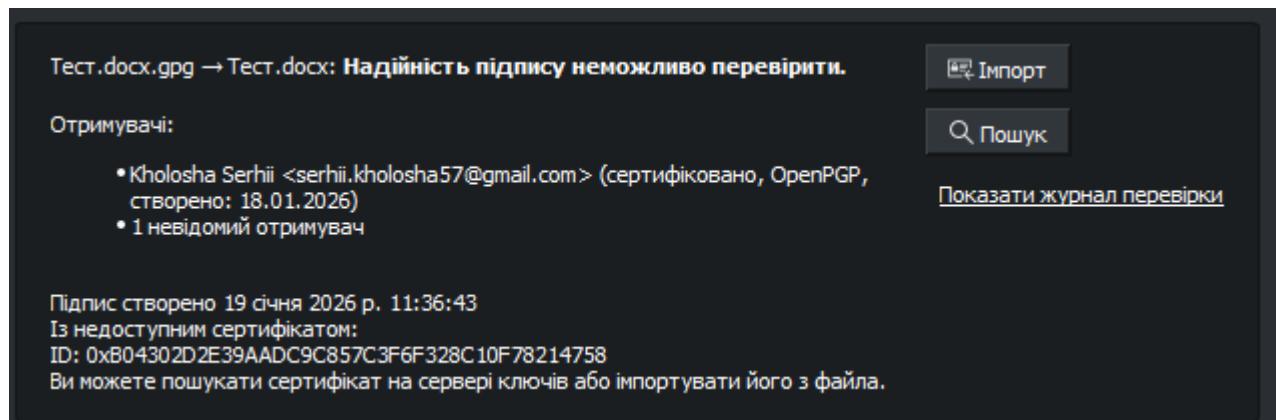


Рис. 11 Розшифрування файлу

На зображені 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

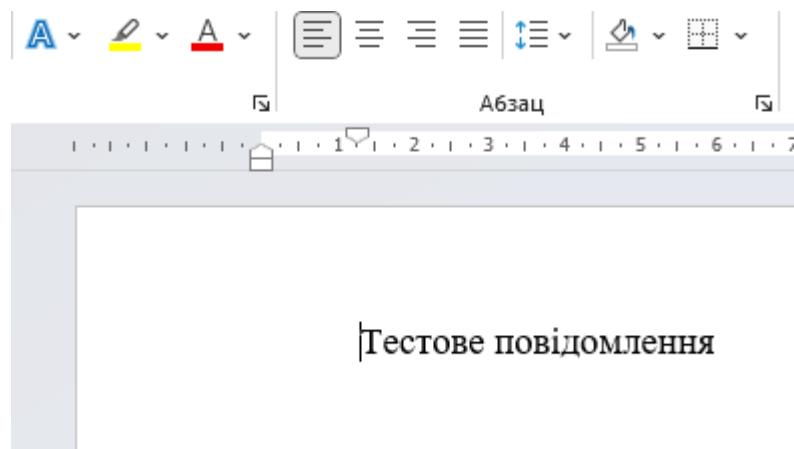


Рис. 12 Повідомлення розшифроване без змін

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: <CA0d_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: <CA0d_q1HydYYbLKQ9T-DbAOeDuibmFDJaxZ9U+8e5mv88VBx9wu@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 безпечної обміну повідомленнями.

Приклад реалізації:

Email-шифратор з функціоналом:

- Електронна адреса: ivan.petrenko@gmail.com;
- Ключ шифрування: хеш від “IvanPetrenko1995”;
- Повідомлення: “Зустрічамося завтра о 15:00”;
- Зашифровані дані:
“U2FsdGVkX1+vupppZksvRf5pq5g5XjFRIipRkwB0K1Y96Qsv2Lelz/...”;
- Процес розшифрування у отримувача.

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

```
==== Демонстрація захищеної комунікації ====
Відправник: ivan.petrenko@gmail.com
Персональні дані для ключа: IvanPetrenko1995
Вихідне повідомлення: Секретні дані про місцеположення ворога

Зашифроване повідомлення:
gAAAAABpbF1PBaiP_ZEKi7mLe2BKLBl1Ig2t7gLYQSAbp_XSDJD7_o0FVPV8sEvy7cE2w0Agn3EYJJkkfvGvtkkxwTSnd4i_ZI_iZUvpttwZr5iLQe6TmTQ6zwQqCq9ThNcV4mf13Qw886TKaJ2A7rlxbXwTGDeijXyc9VRRB5CrWoM4vcTiY=

--- Передача зашифрованого повідомлення ---

Розшифроване повідомлення: Секретні дані про місцеположення ворога
```

Рис. 15 Виконання програми

Посилання на GitHub: [zahist-informaciji/lab5 at main · serhiikholosha57/zahist-informaciji](https://github.com/zahist-informaciji/lab5)

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