Кам’янець-Подільський національний університет імені Івана Огієнка

Кафедра комп’ютерних наук

Навчальна дисципліна

**«Технології захисту інформації»**

Лабораторна робота №5

Криптографія в практиці (OpenSSL, gpg, hashcat)

Виконав:

студент 4-го курсу

групи KN1-B22

**Демченко Дмитро**

Кам’янець-Подільський – 2025

**Мета:** попрактикуватися в шифруванні, підписах та підборі паролів.

**Опис середовища:**

ПЗ для віртуальної машини: VMware® Workstation 17 Pro 17.6.4 build-24832109, OpenSSL 3.5.2 5 Aug 2025, gpg (GnuPG) 2.4.8, libgcrypt 1.11.2, hashcat 6.2.6, Local Kali ip: 192.168.135.128

**Команди:**

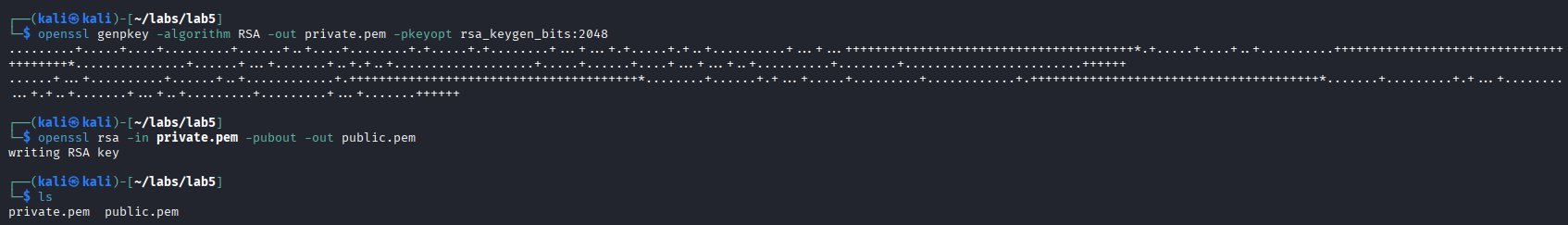
1) Створення файлу з прикладом тексту для подальшої роботи:



2) Генерація ключів RSA:

openssl genpkey -algorithm RSA -out private.pem -pkeyopt rsa\_keygen\_bits:2048

openssl rsa -in private.pem -pubout -out public.pem





3) Шифрування/розшифрування з openssl:

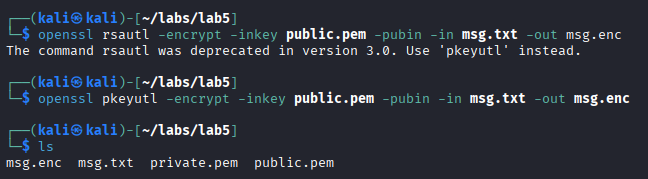
openssl rsautl -encrypt -inkey public.pem -pubin -in msg.txt -out msg.enc

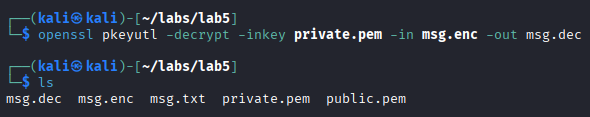
openssl rsautl -decrypt -inkey private.pem -in msg.enc -ou

Команди вище не працюють. Робочі команди:

openssl pkeyutl -encrypt -inkey public.pem -pubin -in msg.txt -out msg.enc

openssl pkeyutl -decrypt -inkey private.pem -in msg.enc -out msg.dec



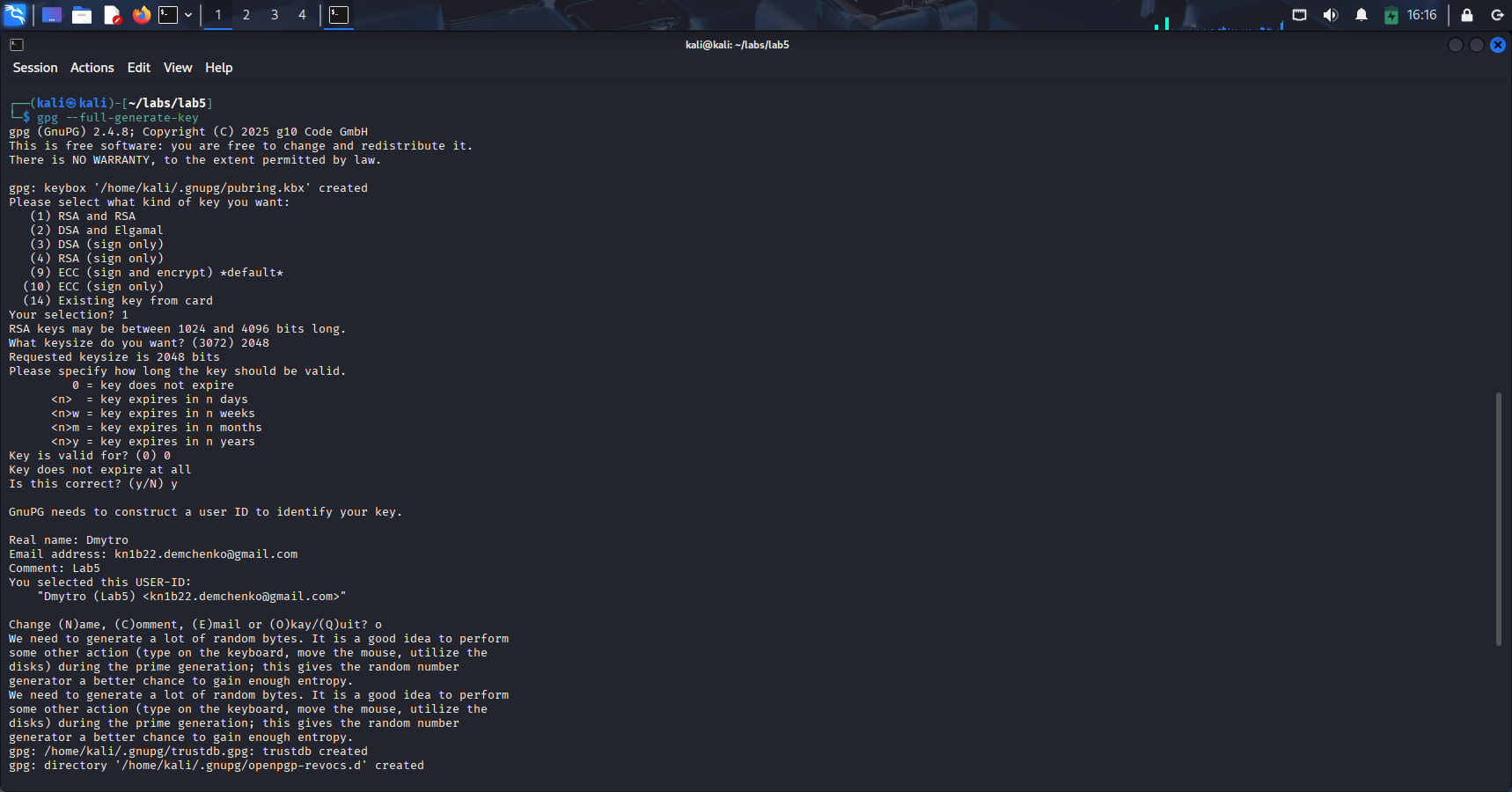


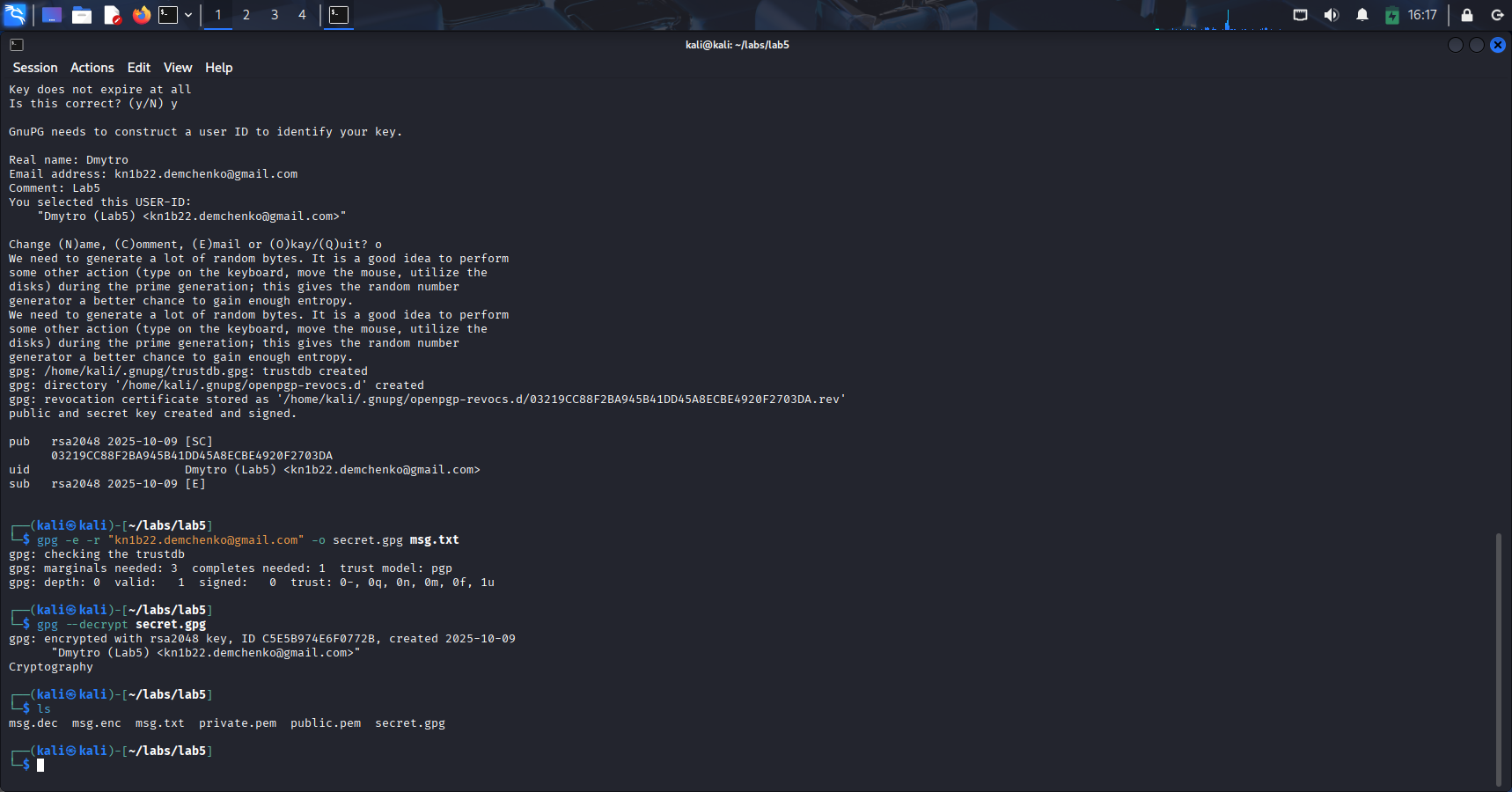


4) GPG операції:

gpg --full-generate-key

gpg -e -r "kn1b22.demchenko@gmail.com" -o secret.gpg msg.txt

gpg --decrypt secret.gpg





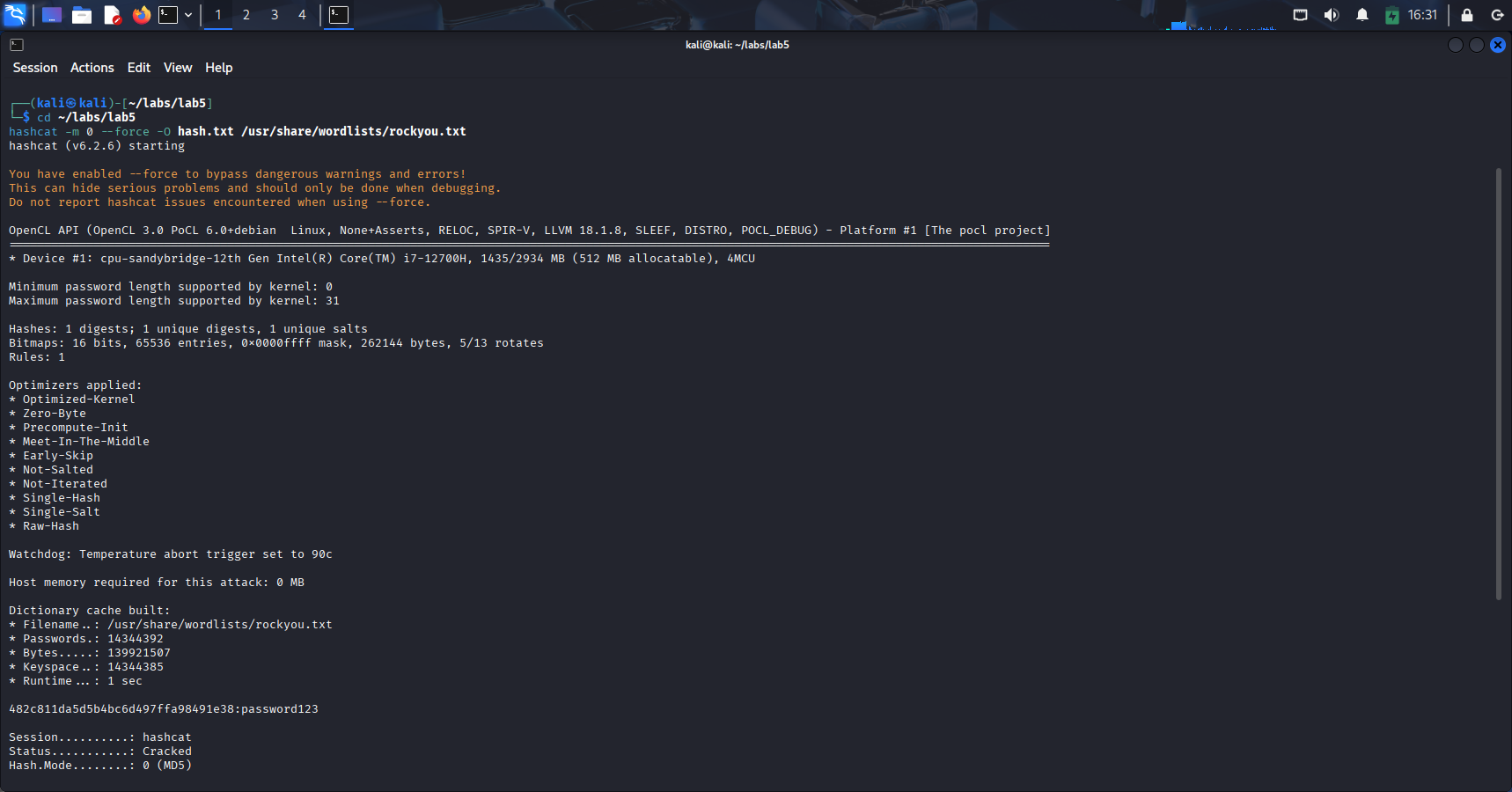
5) Hashcat демонстрація (малий тест):

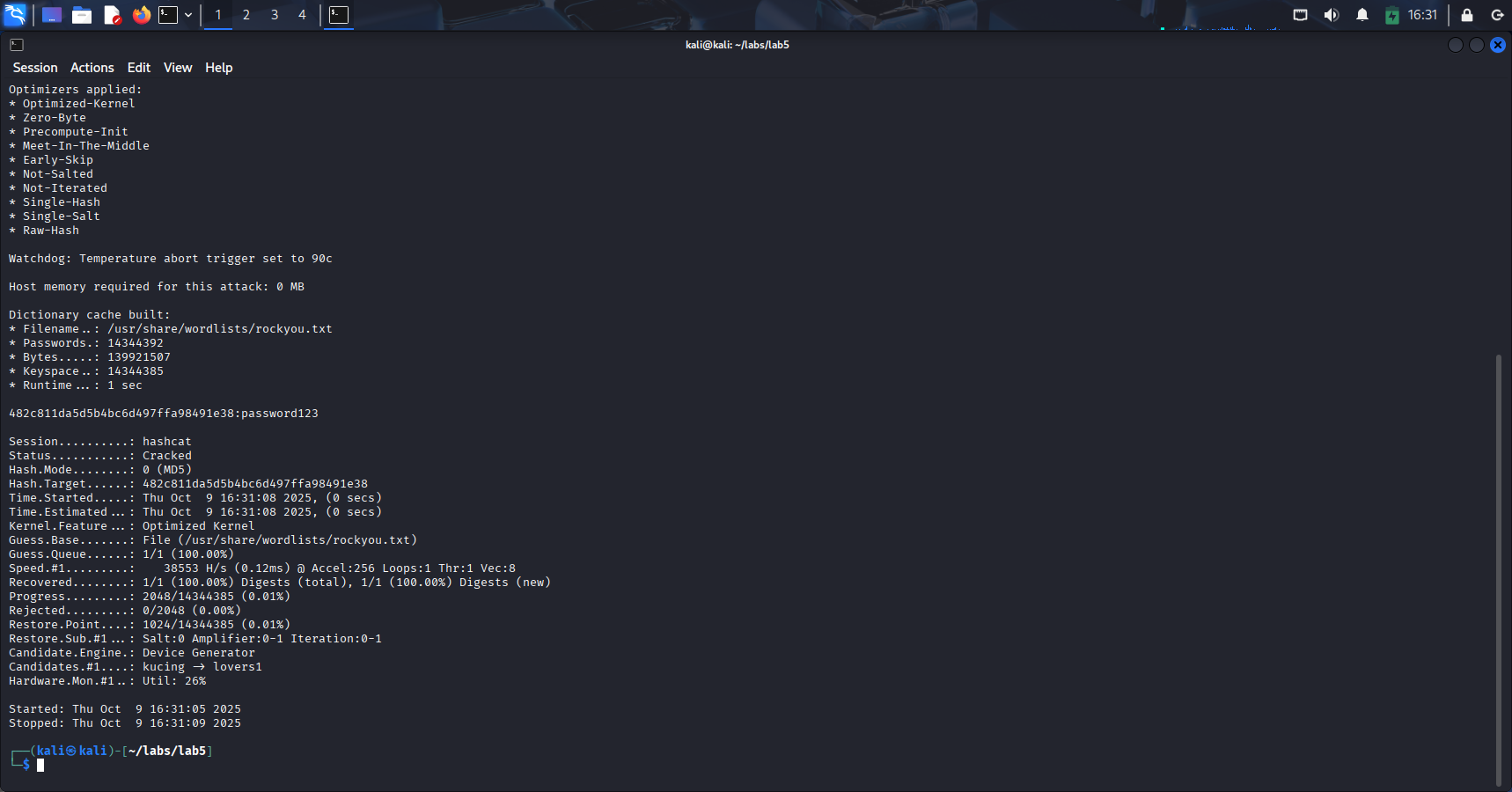
echo -n 'password123' | md5sum > hash.txt

hashcat -m 0 hash.txt /usr/share/wordlists/rockyou.txt –show

Для оптимізації та швидкості додав флаги та виділив більше оперативної пам’яті віртуальній машині. Готова робоча команда:

hashcat -m 0 --force -O hash.txt /usr/share/wordlists/rockyou.txt





**Сила паролів та рекомендації:**

Сила пароля визначається часом і ресурсами, які потрібні зловмиснику для його підбору. Як показав експеримент з Hashcat, прості та поширені паролі, що містяться у словниках на кшталт rockyou.txt, зламуються миттєво. Надійний пароль має протистояти як атакам за словником, так і методу повного перебору (brute-force).

Що визначає силу пароля?

* Довжина: Це найважливіший фактор. Кожен додатковий символ експоненціально збільшує кількість можливих комбінацій. Пароль з 8 символів можна зламати значно швидше, ніж пароль з 16 символів, навіть якщо останній складається з простих слів.
* Складність: Використання різних наборів символів — малих літер (a-z), великих літер (A-Z), цифр (0-9) та спеціальних символів (!@#$) — значно ускладнює перебір.
* Непередбачуваність: Пароль не повинен містити очевидної інформації. Слід уникати:
  + Словникових слів: password, sunshine, iloveyou.
  + Послідовностей: 123456, qwerty, abcdef.
  + Особистої інформації: вашого імені, дати народження, клички домашнього улюбленця.
  + Простих замін: P@ssw0rd замість Password не є надійним, оскільки такі заміни враховані в алгоритмах зламу.
* Унікальність: Один пароль не можна використовувати для кількох сервісів. Якщо один сайт зламають, ваш скомпрометований пароль спробують використати на інших популярних платформах.

Рекомендації для надійного захисту

1. Використовуйте менеджер паролів
2. Створюйте парольні фрази
3. Вмикайте багатофакторну автентифікацію (MFA/2FA)
4. Перевіряйте свої дані на наявність у витоках.

**Висновки:** Під час виконання лабораторної роботи було згенеровано ключі RSA та GPG, виконано шифрування і розшифрування повідомлень, було створено MD5‑хеш пароля та за його допомогою підібрано пароль, а також проаналізовано силу паролів і рекомендації щодо безпеки.