КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БУДІВНИЦТВА І АРХІТЕКТУРИ

«Реалізація тестової системи шифрування на основі NIST PQC стандартів»

123 «Комп’ютерна інженерія»

Здобувач: студент групи КСМс-23, **Сутула Андрій Олександрович**

Керівник: к.ф.-м.н., доцент Кондакова С. В.

Київ 2026

Актуальність та квантова загроза

Загроза "Q-Day"

- Розвиток квантових обчислювачів ставить під загрозу класичні алгоритми (RSA, ECC).
- **Алгоритм Шора** дозволяє факторизувати числа за поліноміальний час.
- Концепція **"Harvest Now, Decrypt Later"** вимагає захисту даних вже сьогодні.

Традиційні криптосистеми стануть вразливими протягом наступного десятиліття, що потребує негайної міграції на PQC.

Мета та завдання роботи

Мета

Розробка та реалізація тестової системи на основі стандартів NIST PQC для дослідження їх ефективності.

Завдання

Аналіз сучасних PQC стандартів, проектування архітектури та програмна реалізація прототипу.

Об'єкт

Процеси забезпечення криптографічного захисту в умовах розвитку квантових обчислень.

Стандарти NIST PQC: Вибір алгоритму

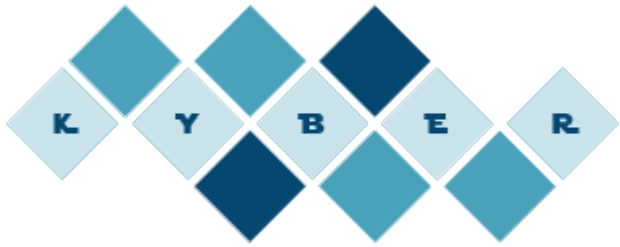
У ході роботи було проаналізовано переможців конкурсу NIST. Для реалізації обрано **CRYSTALS-Kyber (ML-KEM)**.

Переваги Kyber:

- Висока швидкість операцій.
- Компактні розміри ключів.
- Безпека на основі Module-LWE.

Рівні стійкості:

- Kyber-512 (AES-128 equiv).
- **Kyber-768** (AES-192 equiv) - обрано як баланс.
- Kyber-1024 (AES-256 equiv).



Концепція гібридної системи

Для практичної реалізації обрано гібридний підхід **KEM-DEM**:

$$C = E_{AES}(K, M) \parallel Encaps_{Kyber}(pk, r)$$

Kyber (ML-KEM)
Відповідає за безпечне узгодження спільного секрету.

AES-256 GCM
Забезпечує конфіденційність та автентичність даних.

HKDF-SHA256
Використовується для деривації сеансового ключа.

Наукова новизна та внесок

Практична значимість та новизна роботи полягають у:

Створенні інтегрованого **експериментального стенду** для дослідження PQC алгоритмів у Python-середовищі.

Реалізації концепції **Crypto-Agility** (можливість швидкої зміни алгоритмів).

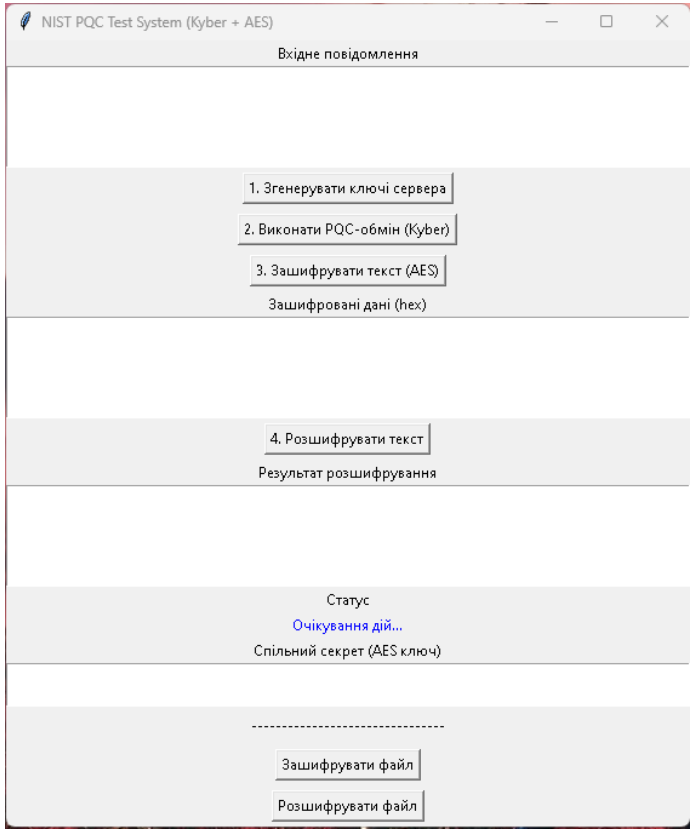
Дослідженні продуктивності гібридного шифрування для різних типів файлів.

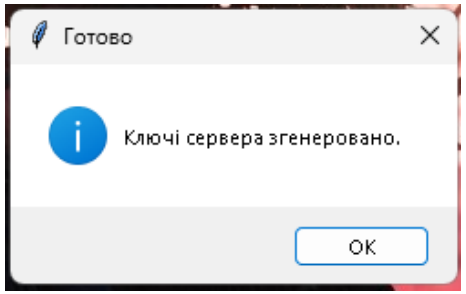
Робота доводить можливість безшовної інтеграції постквантових стандартів у прикладне ПЗ без суттєвої втрати швидкодії.

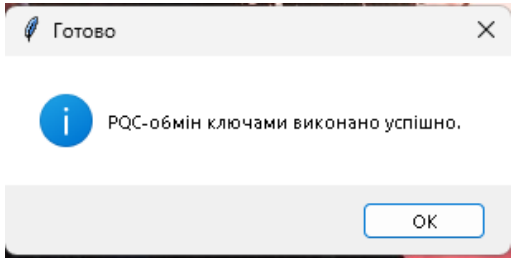
Архітектура програмної системи

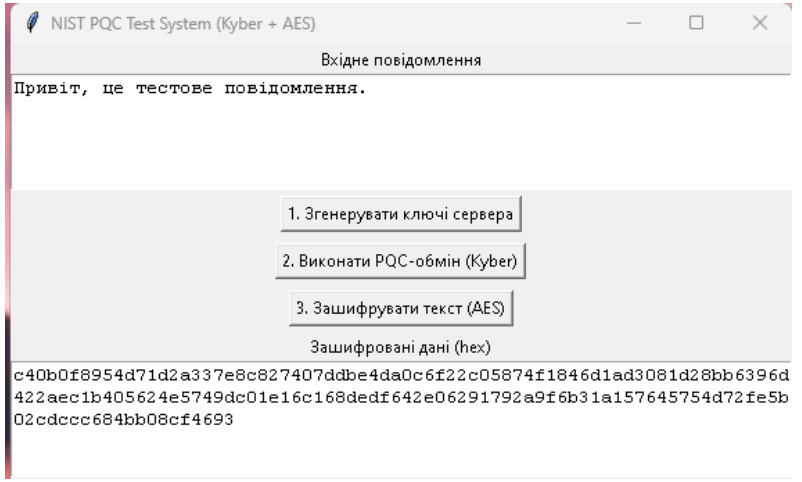
Рівень	Функціонал	Інструментарій
GUI	Tkinter	Python 3.10+
Логічний рівень	Управління станами, обробка помилок	Process Manager
Крипто -ядро	Kyber, AES, HKDF	PyCryptodome, liboqs
I/O Система	Binary Chunking (поблокова обробка)	FileManager

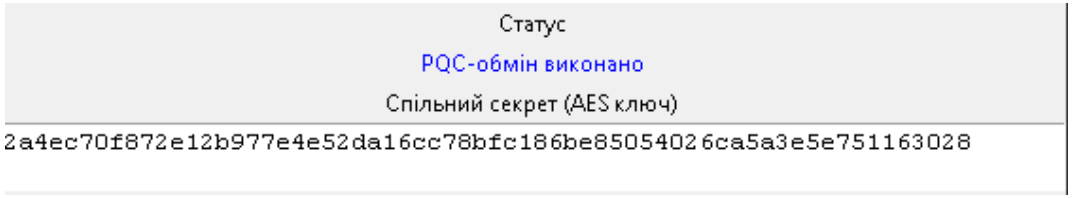
Інтерфейс та робота програми











Система реалізує 3-кроковий процес: Генерація ключів → PQC-обмін → Шифрування.

Порівняльний аналіз стійкості

Параметр	RSA-3072	Kyber -768
Тип задачі	Факторизація	Lattice (решітки)
Квантова стійкість	Вразливий	Стійкий
Розмір ключа (байт)	384	1184
Час обробки	До 1 мс	0.20 мс

Загальні висновки

1. Реалізовано програмну систему на Python із використанням ML-KEM (Kyber-768).
2. Реалізовано гібридну схему ML-KEM + AES-256-GCM.
3. Проведено тестування працездатності на файлах різних типів.

Дякую за увагу!

GitHub: https://github.com/Andrejj6/project/tree/main/work