**Сеанс зв’язку системи Secure\_messenger**

**Реалізовано:**

**1. DH (Діффі-Хеллман) обмін ключами**

* **Мета**: Узгодження **спільного ключа** між двома клієнтами через сервер.
* **Алгоритм**:
  + Використовується **X25519** (еліптична крива Curve25519) для обчислення спільного секрету.
  + Клієнти обмінюються публічними ключами через сервер.
  + На основі DH-обміну обчислюється **спільний ключ**.

**Стан**: Реалізовано та працює.

**2. Шифрування повідомлень: ChaCha20-Poly1305**

* **Мета**: Шифрування тексту повідомлень між клієнтами з додатковим захистом цілісності (автентифікація).
* **Алгоритм**:
  + Використовується ChaCha20-Poly1305 – сучасний AEAD (Authenticated Encryption with Associated Data) алгоритм.
  + Шифрування включає:
    - **Nonce**: 12-байтовий випадковий вектор ініціалізації для унікальності шифру.
    - **Ciphertext**: Зашифроване повідомлення.
  + Результат:
    - **Nonce та Ciphertext передаються отримувачу для розшифрування.**

**Стан**: Реалізовано та працює.

**3. Ключова деривація (KDF)**

* **Мета**: Генерація нових ключів з існуючого секрету для забезпечення безпеки.
* **Алгоритм**:
  + Використовується **HKDF** (HMAC-based Key Derivation Function) з **SHA-256** як хеш-функцією.
  + Застосовується у DH-обміні для отримання кореневого ключа.

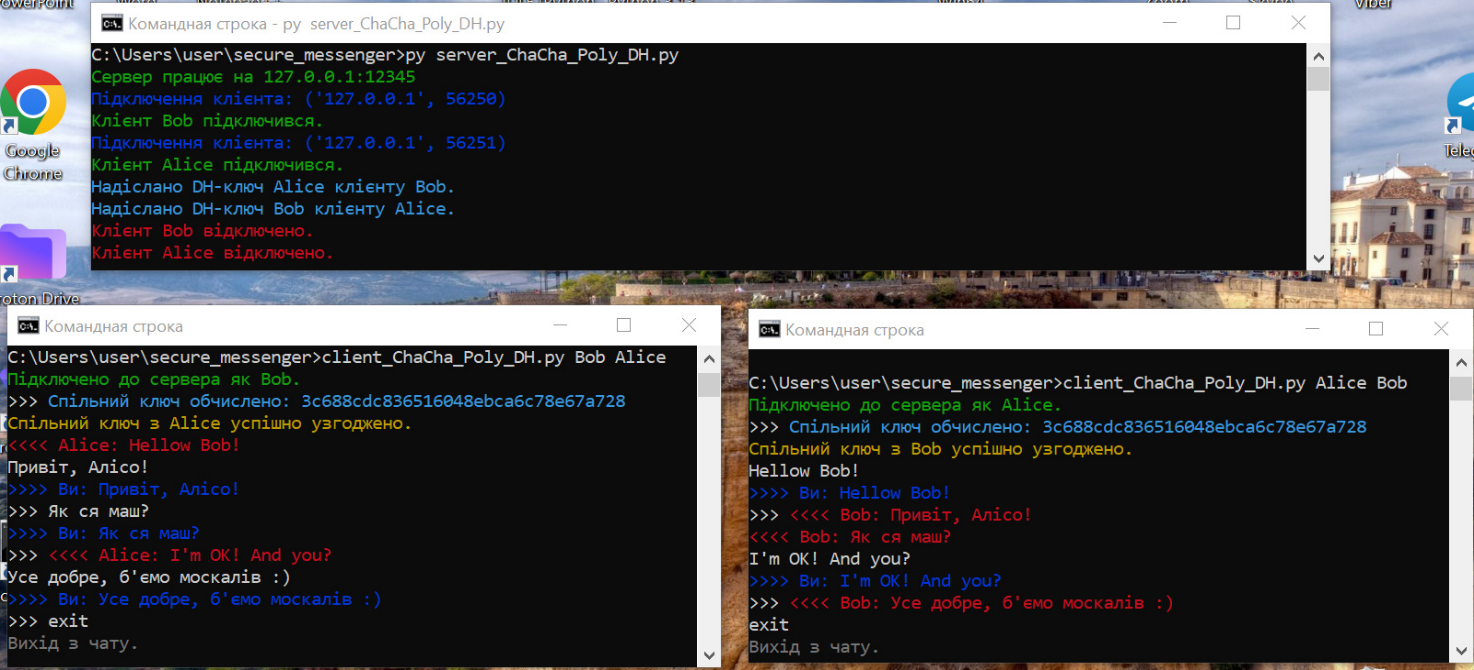
**Стан**: Реалізовано у DH-клієнті.

**4. Логування подій**

* **Мета**: Відстеження ключових криптографічних подій та дій у системі.
* **Логуються**:
  + Підключення клієнтів.
  + Надсилання та отримання **DH-публічних ключів**.
  + Узгодження спільного ключа.
  + Шифрування та розшифрування повідомлень.
  + Відправка та отримання повідомлень.

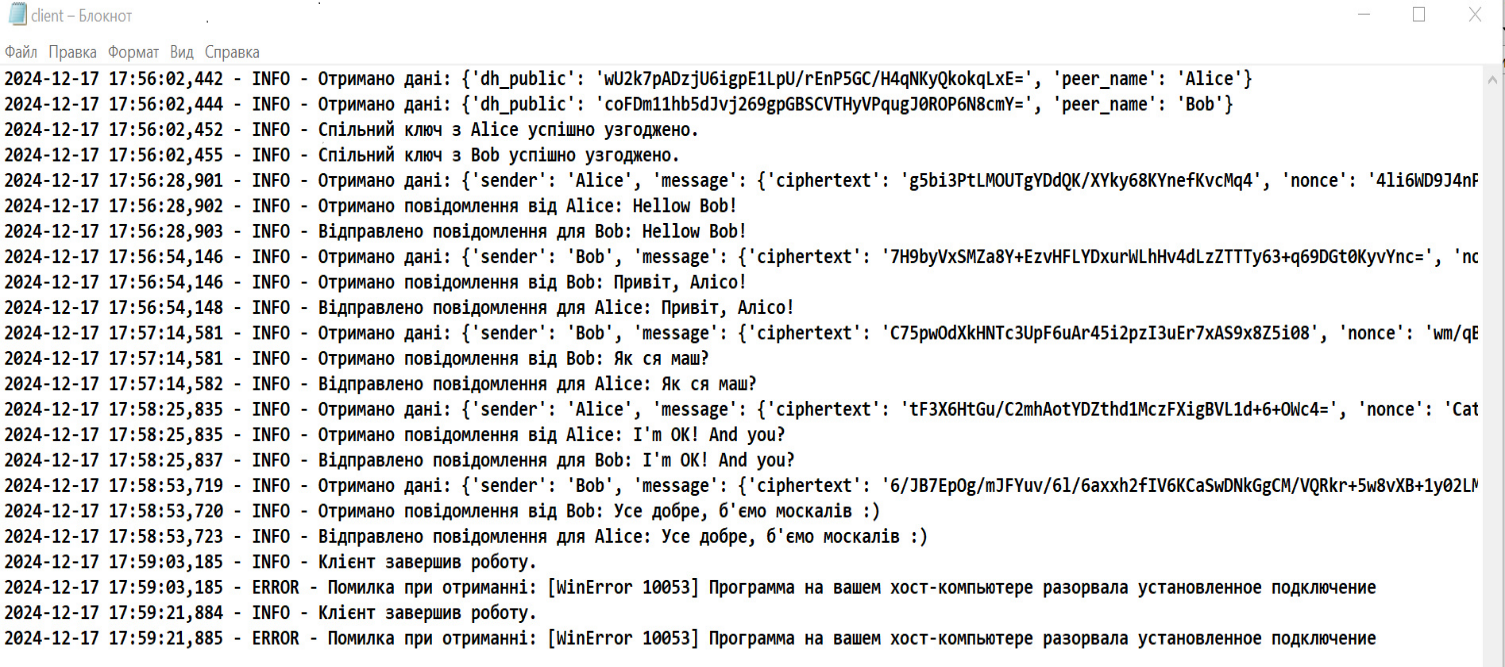
**Стан**: Реалізовано та працює.

**Скрин екрану**



**Скрин логів**

**лог сервера**



**лог клієнта**

