ПРОГРАМНИЙ ЗАСІБ ЗАХИЩЕНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ. ЧАСТИНА 2. ПРОТОКОЛ ОБМІНУ ІНФОРМАЦІЄЮ

Виконав студент гр. 1БС-24м: Володимир КОЗИРА

Науковий керівник: Володимир ЛУЖЕЦЬКИЙ

АКТУАЛЬНІСТЬ ДОСЛІДЖЕННЯ

Актуальність роботи зумовлена швидким розвитком технологій передавання інформації та зростанням потреби у надійних криптографічних протоколах, здатних забезпечити високу швидкодію, цілісність і захищеність інформації під час обміну між користувачами.

МЕТА, ОБ’ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Метою дослідження є пришвидшення процесу встановлення автентифікованого зв’язку між користувачами програмного засобу захищеного передавання інформації шляхом суміщення процесів автентифікації користувачів та процесу реалізації угоди про ключі Діфі-Гелмана.

Об’єкт - процес встановлення автентифікованого зв’язку між користувачами програмного засобу захищеного передавання інформації.

Предметом є протокол автентифікації користувачів та протокол угоди про ключі Діфі-Гелмана.

ЗАДАЧІ

Для досягнення мети потрібно вирішити такі задачі:

- проаналізувати протоколи сучасних месенджерів;
- розробити суміщений протокол автентифікації користувачів та протокол угоди про ключі Діфі-Гелмана;
- розробити метод ущільнення секретного ключа;
- розробити метод побудови секретного ключа у вигляді ортогональної поворотної матриці;
- розробити програмний модуль, що реалізує протокол обміну інформацією та провести його тестування.

ПОСЛІДОВНІСТЬ ІНФОРМАЦІЙНИХ КРОКІВ ПРОТОКОЛУ ОБМІНУ ІНФОРМАЦІЄЮ

Етап	Напрямок	Опис дії
1	$A \to B$	Надсилання запиту на ініціацію обміну
2	$B \to A$	Підтвердження прийняття та передача узгоджених параметрів
3	$A \leftrightarrow B$	Обмін даними згідно за протоколом Діфі-Гелмана
4	A, B	Обчислення спільного секрету K
5	A, B	Формування робочого 64-бітного ключа K_0
6	A, B	Формування поворотної матриці
7	$A \to B$	Надсилання зашифрованого повідомленнями з MAC-кодом
8	B	Перевірка автентичності та підтвердження цілісності повідомлення

ПРОЦЕДУРА ФОРМУВАННЯ СЕКРЕТНОГО КЛЮЧА

$$K = (K_1, K_2, K_3, K_4), \quad K_i \in [0, 2^{256} - 1]$$

$$K_1 = (a_1, b_1, c_1, d_1), K_2 = (a_2, b_2, c_2, d_2), K_3 = (a_3, b_3, c_3, d_3),$$
$$K_4 = (a_4, b_4, c_4, d_4),$$

$$K_1 = a_1 + b_1 i + c_1 j + d_1 k,$$
$$K_2 = a_2 + b_2 i + c_2 j + d_2 k,$$
$$K_3 = a_3 + b_3 i + c_3 j + d_3 k,$$
$$K_4 = a_4 + b_4 i + c_4 j + d_4 k.$$

ПРОЦЕДУРА ФОРМУВАННЯ СЕКРЕТНОГО КЛЮЧА

$$D_1 = K_1K_2 = \begin{cases} a_1a_2 - b_1b_2 - c_1c_2 - d_1d_2 = w_1, \\ a_1b_2 + b_1a_2 + c_1d_2 - d_1c_2 = z_1, \\ a_1c_2 - b_1d_2 + c_1a_2 + d_1b_2 = x_1, \\ a_1d_2 + b_1c_2 - c_1b_2 + d_1a_2 = k_1. \end{cases}$$

$$D_2 = K_3K_4 = \begin{cases} a_3a_4 - b_3b_4 - c_3c_4 - d_3d_4 = w_2, \\ a_3b_4 + b_3a_4 + c_3d_4 - d_3c_4 = z_2, \\ a_3c_4 - b_3d_4 + c_3a_4 + d_3b_4 = x_2, \\ a_3d_4 + b_3c_4 - c_3b_4 + d_3a_4 = k_2. \end{cases}$$

$$Q = D_1D_2 = \begin{cases} w_1w_2 - z_1z_2 - x_1x_2 - k_1k_2 = q_1 \\ w_1z_2 + z_1w_2 + x_1k_2 - k_1x_2 = q_2 \\ w_1x_2 - z_1k_2 + x_1w_2 + k_1z_2 = q_3 \\ w_1k_2 + z_1x_2 - x_1z_2 + k_1w_2. = q_4 \end{cases}$$

УЩІЛЬНЕННЯ СЕКРЕТНОГО КЛЮЧА

$$K_0 = (q_1 + q_2 + q_3 + q_4) \, mod \, 2^{64}$$

Процедура ущільнення має такі властивості:

- K_0 є геш-значенням для коду .
- Нелінійність – кватерніонне множення створює складну залежність між вхідними частинами, що унеможливлює лінійне відновлення початкових компонент.
- Незворотність – через геш-значення.
- Ентропійність – усі 1024 біти початкового ключа впливають на кінцеве значення , забезпечуючи повне змішування.

ОБЧИСЛЕННЯ ПОВОРОТНОЇ МАТРИЦІ

$$K_0 = (w, x, y, z),$$

$$N = (w^2 + x^2 + y^2 + z^2) \bmod p$$

$$t^2 \equiv N^{-1} \pmod p,$$

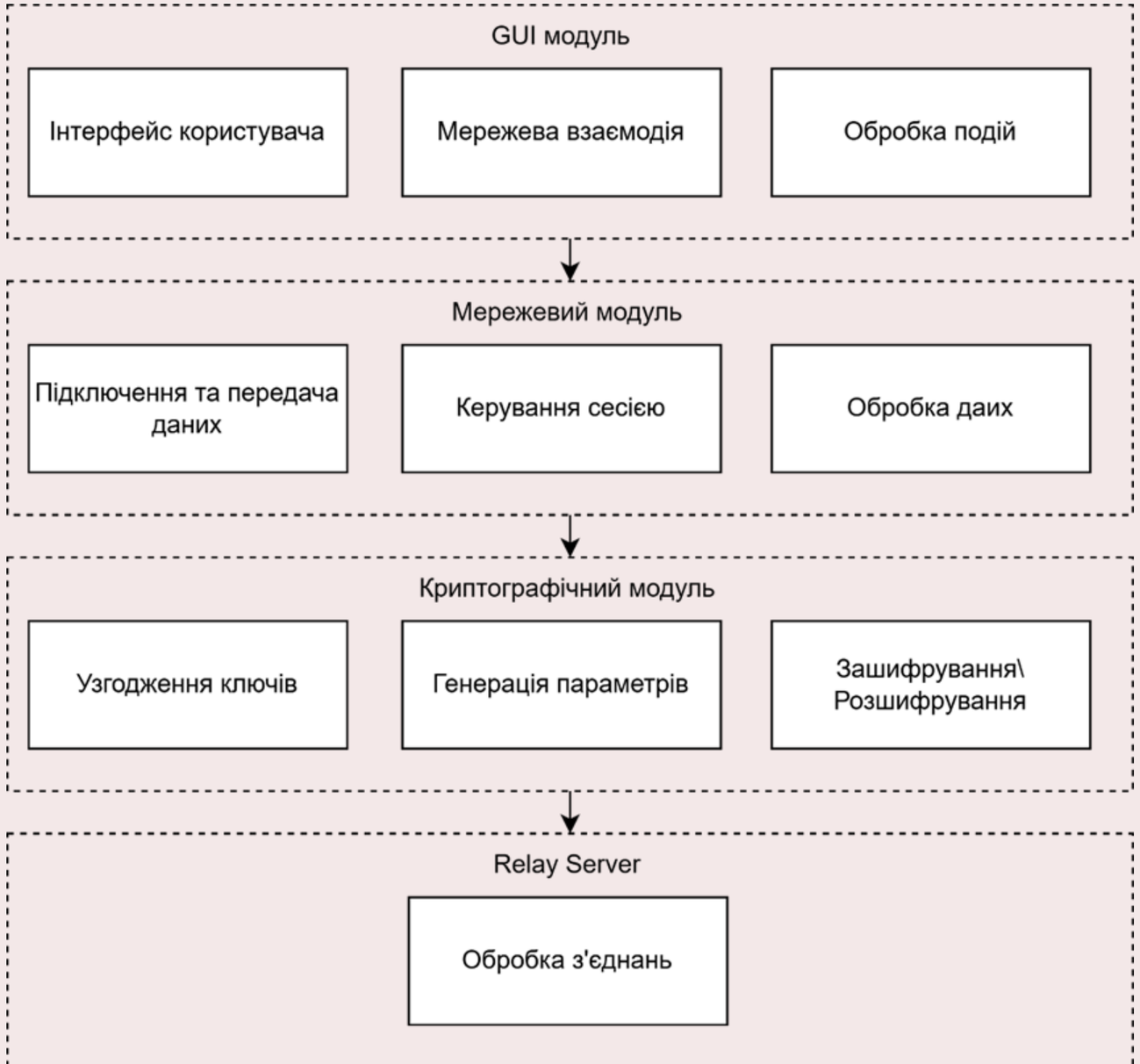
$$||\hat{q}||^2 \equiv 1 \pmod p,$$

$$\hat{q} = t \cdot q \bmod p,$$

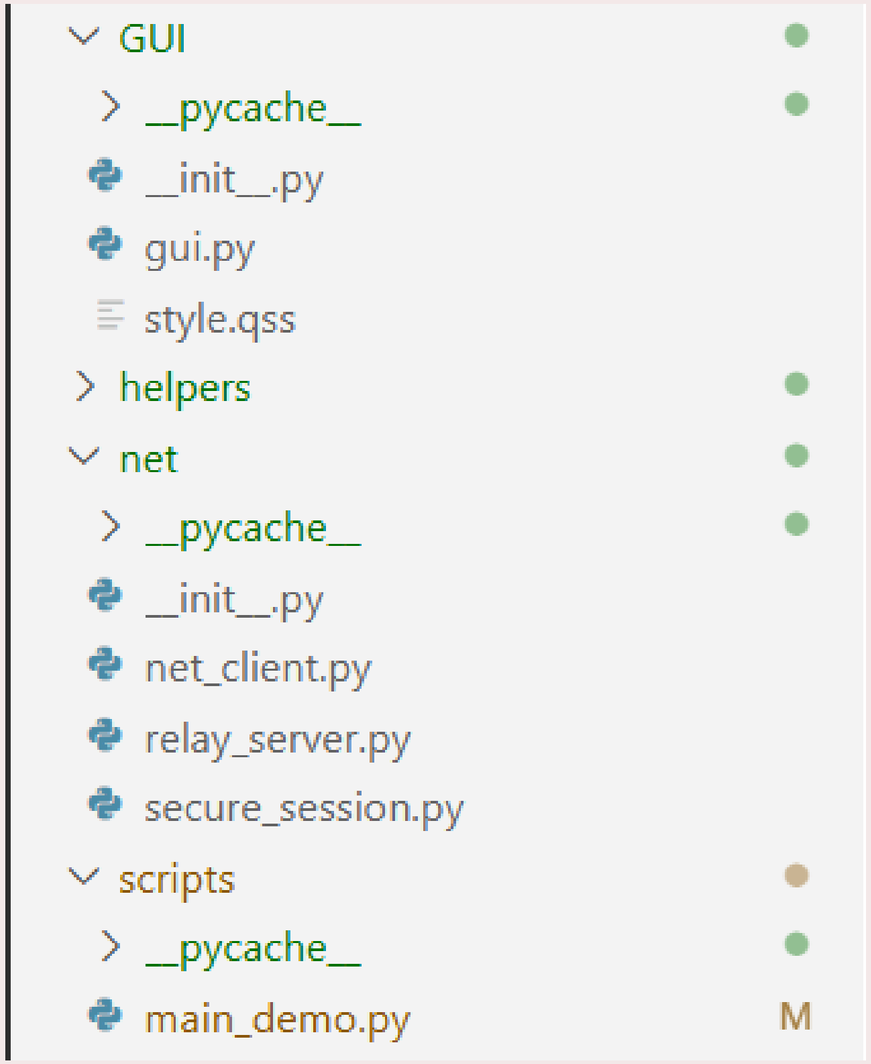
$$\mathbf{\Gamma}(\hat{q}) = \begin{bmatrix} 1 - 2(y^2 + z^2) & 2(xy - wz) & 2(xz + wy) \\ 2(xy + wz) & 1 - 2(x^2 + z^2) & 2(yz - wx) \\ 2(xz - wy) & 2(yz + wx) & 1 - 2(x^2 + y^2) \end{bmatrix}$$

$$\Gamma(\hat{q})^{\mathrm{T}} \Gamma(\hat{q}) \equiv I \pmod p,$$

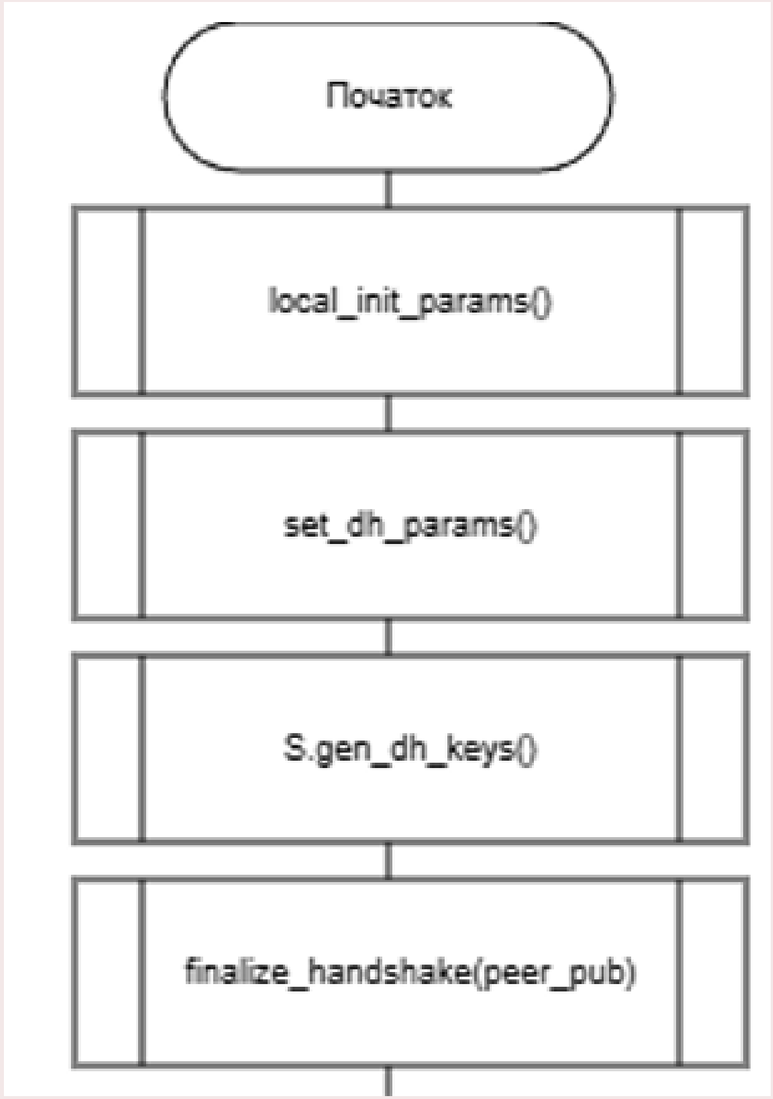
АРХІТЕКТУРА ПРОГРАМНОГО ЗАСОБУ ЗАХИЩЕНОГО ПЕРЕДАВАННЯ ІНФОРМАЦІЇ

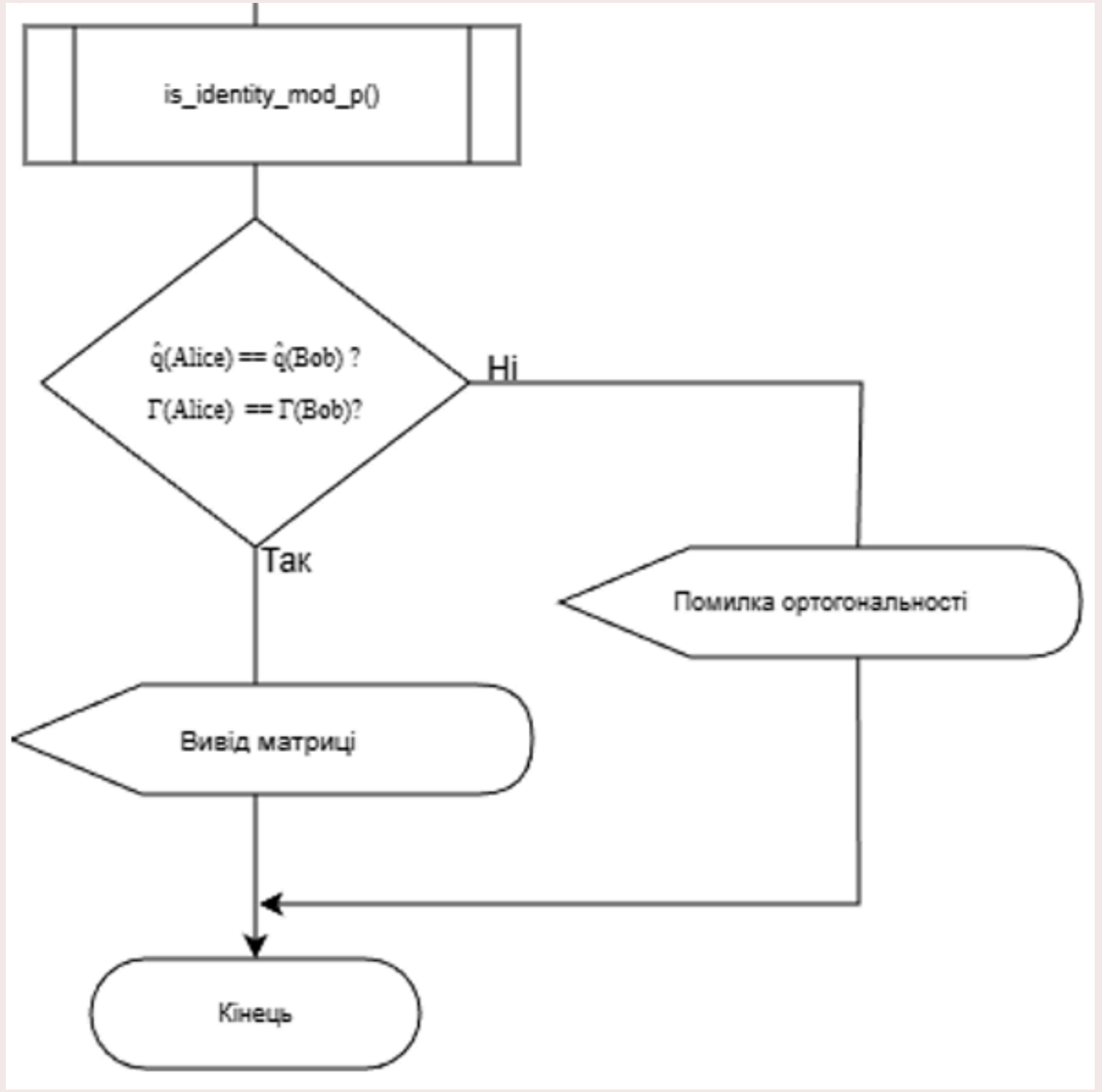


СТРУКТУРА ПРОГРАМНОГО ЗАСОБУ

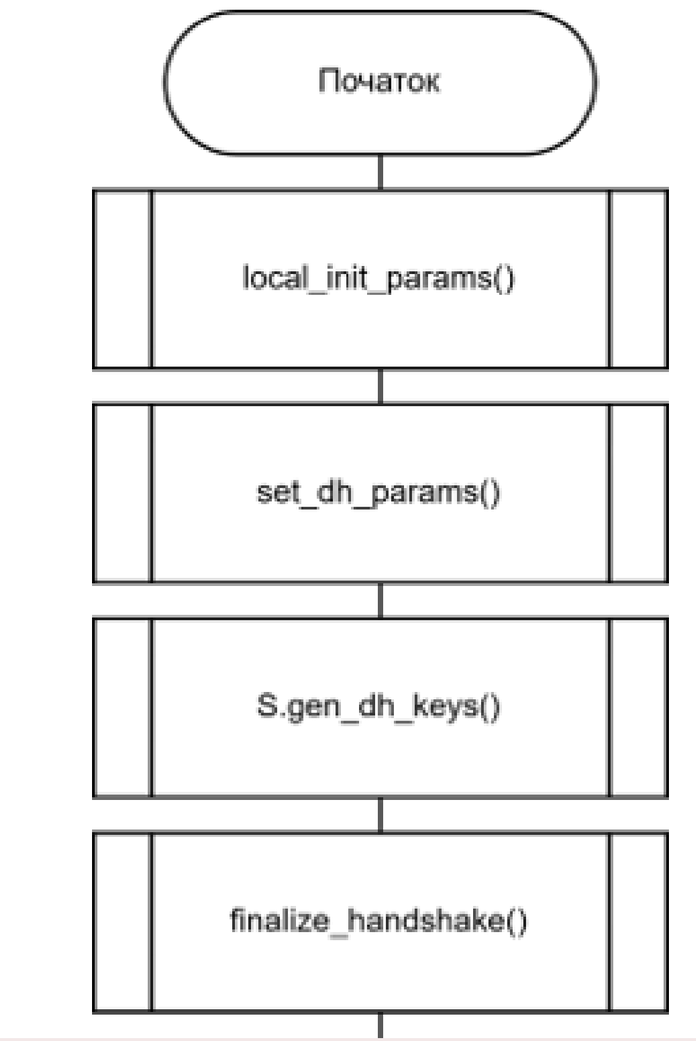


АЛГОРИТМ РЕАЛІЗАЦІЇ УЗГОДЖЕННЯ ПАРАМЕТРІВ ТА ПЕРЕВІРКИ ОРТОГОНАЛЬНОСТІ





АЛГОРИТМ РЕАЛІЗАЦІЇ ФОРМУВАННЯ ПОВОРОТНОЇ МАТРИЦІ ТА ВСТАНОВЛЕННЯ СТАНУ ГОТОВНОСТІ



ВИСНОВКИ

Особливість запропонованого протоколу обміну інформацією полягає у суміщенні процесів автентифікації користувачів та угоди про секретний ключ Діфі-Гелмана в єдиній процедурі встановлення захищеного сеансу.

Криптографічна стійкість розробленої схеми забезпечується двома ключовими механізмами: ущільненням 1024-бітного секретного значення до 64-бітного ключа на основі нелінійних кватерніонних операцій та подальшим побудуванням ортогональної поворотної матриці, яка використовується для формування внутрішніх параметрів стану.

ДЯКУЮ ЗА УВАГУ!