Глеб Владислав Юрійович, магістрант

КПІ ім. Ігоря Сікорського, Київ

**«Застосунок для передачі інформації, захищеної за допомогою асиметричних алгоритмів шифрування(RSA та ін.)»**

**Вступ**

Захист конфіденційної інформації є найважливішою задачею в сучасному цифровому світі. Асиметричні алгоритми шифрування, такі як RSA (Rivest-Shamir-Adleman), надають високий рівень безпеки у передачі інформації через мережі. У даному рефераті розглянемо застосування цих алгоритмів для захисту передачі конфіденційної інформації.

**Постановка задачі**

Основною метою цього дослідження є створення застосунку для шифрування повідомлень. Цей застосунок повинен реалізувати підхід асиметричних алгоритмів для шифрування і розшифрування даних

**Основні принципи асиметричного шифрування**

Асиметричні алгоритми шифрування використовують пари ключів: публічний і приватний. Публічний ключ використовується для шифрування інформації, а приватний — для розшифрування. Така схема гарантує високий рівень безпеки, оскільки навіть володар публічного ключа не може розшифрувати дані без відповідного приватного ключа.

**Опис запропонованої архітектури застосунку**

Застосунок буде складатись з таких вузлів як:

* Інтерфейс користувача
* Серверна частина
* База даних

**Інтерфейс користувача**

В інтерфейсі повинні бути реалізовані весь функціонал який надає

 змогу відправляти повідомлення від відправника до одержувача. А саме повинна бути сторінка авторизації, автентифікації, створення, виладення і відправка повідомлень. Як основну платформу для інтерфейсу було обрано веб браузер як кросплатформове рішення, яке буде працювати на всіх операційних системах і комп'ютерах. Для розробки самого інтерфейсу був вибраний фреймворк React, як один з найпопулярніших фреймворків для створення користувацьких інтерфейсів.

**Серверна частина**

Оскільки нам потрібно передавати повідомлення з комп'ютера А на комп'ютер Б, нам потрібно сервер який буде під час відправки повідомлення отримувати дані і відправляти їх на комп'ютер отримувача. За основу було взято мову JavaScript і фреймворк Nest.js, як один з найпопулярніших фреймворків для написання серверу. Отримувати і відправляти запити сервер буде через http протокол.

**База даних**

Повідомлення в зашифрованому виді повинні зберігатись в базі даних, щоб в отримувача завжди був доступ до історії повідомлень. Також в базі даних повинен бути збережений сам обліковий запис для авторизації і ідентифікації користувача. За основу було вибрано реляційну базу даних PostgreSQL. Всі дані приводяться до нормальних форм і записуються в відповідні таблиці, приведені до першої, другої і третьої нормальної форми.



*Рис.1 Схема таблиць в базі даних PostgreSQL*

**Запуск**

Для повного запуску програми нам потрібний комп'ютер з встановленим ядром Node.js та базою даних PostgreSQL. Щоб спростити підготовку до запуску ми можемо використати Docker. В такому випадку ми будемо запускати на нашому сервері віртуальну машину, яка уже буде мати потрібні нам програми.

**Висновки**

Сьогодні захист інформації є важливою складовою при користуванні інтернетом по всьому світу і дуже важливо щоб передача інформації була строго конфіденційна. Для захисту передачі інформації була створена програма яка дозволяє шифрувати дані. В такому випадку при використанні асиметричних алгоритмів тільки одержувач матиме змогу розшифрувати отримане повідомлення

**Література**

1. [*https://www.docker.com/*](https://www.docker.com/)
2. [*https://react.dev/*](https://react.dev/)
3. [*https://nestjs.com/*](https://nestjs.com/)
4. [*https://nodejs.org/en*](https://nodejs.org/en)