УДК 004.414

Глеб Владислав Юрійович, *здобувач вищої освіти*
КПІ ім. Ігоря Сікорського, Україна
Науковий керівник: Тарасенко-Клятченко Оксана Володимирівна, *кандидат технічних наук, доцент кафедри системного програмування та спеціалізованих комп'ютерних систем*
КПІ ім. Ігоря Сікорського, Україна

ПЕРЕДАЧА ІНФОРМАЦІЇ, ЗАХИЩЕНОЇ ЗА ДОПОМОГОЮ АСИМЕТРИЧНИХ АЛГОРИТМІВ ШИФРУВАННЯ

Анотація. Доповідь присвячена розгляду застосування асиметричних алгоритмів шифрування, зокрема RSA, для передачі інформації в безпечних комунікаційних системах. У доповіді буде проаналізовано принципи роботи асиметричних шифрів, їхню основну концепцію та математичні засади. Особлива увага буде приділена практичним застосуванням RSA для забезпечення конфіденційності та цілісності інформації під час її передачі через відкриті мережі. Доповідь також розгляне можливі ризики та виклики, пов'язані з використанням асиметричних алгоритмів, та запропонує рекомендації щодо забезпечення ефективного та безпечного використання цих методів шифрування в різних сферах інформаційної безпеки.
КЛЮЧОВІ СЛОВА: асиметричне шифрування, шифрування, асиметричні алгоритми шифрування

Abstract. The presentation is dedicated to the exploration of the application of asymmetric encryption algorithms, particularly RSA, for secure information transmission in communication systems. The presentation will analyze the working principles of asymmetric ciphers, their core concepts, and mathematical foundations. Special attention will be given to the practical implementations of RSA to ensure the confidentiality and integrity of information during transmission over open networks. The presentation will also examine potential risks and challenges associated with the use of asymmetric algorithms, offering recommendations for ensuring effective and secure utilization of these encryption methods in various realms of information security.
KEYWORDS: asymmetric encryption, encryption, asymmetric encryption algorithms

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.

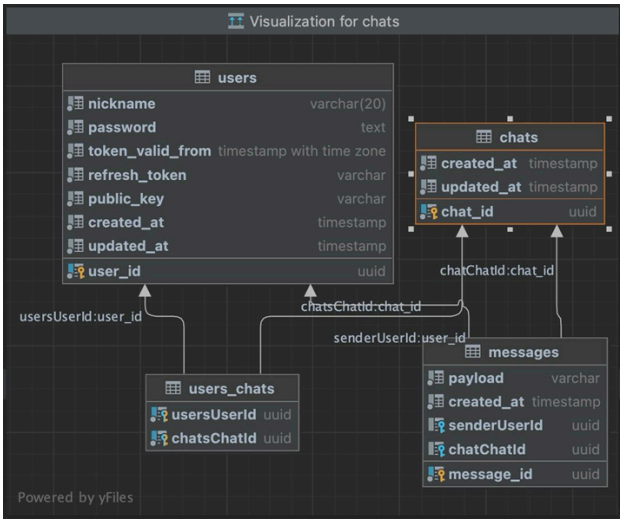

Рис.1 Схема таблиць в базі даних PostgreSQL

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. За останні десятиліття потужність комп’ютерів збільшилась в тисячі разів. Сьогодні в кожної людини в кармані є комп’ютер який ще кілька десятиліть назад міг займати цілу кімнату. В зв’язку з цим багато алгоритмів можуть бути зламані звичайним перебором. На протидію цим потужностям були винайдені асиметричні алгоритми шифрування. На даний момент ці алгоритми використовуються в генерації ключів доступу для держустанов, https протокол використовує асиметричні алгоритми для передачі даних в браузер і з браузера. Ці алгоритми мають високі ступені захисту, що дозволяє їх використання в будь яких програмах, для яких безпека є одним з основних критеріїв.

Список інформаційних джерел

1. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. 1978. URL:https://web.williams.edu/Mathematics/lg5/302/RSA.pdf

2. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer, 2004. URL:http://tomlr.free.fr/Math%E9matiques/Math%20Complete/Cryptography/Guide%20to%20Elliptic%20Curve%20Cryptography%20-%20D.%20Hankerson,%20A.%20Menezes,%20S.%20Vanstone.pdf

3. Stallings W. Cryptography and Network Security: Principles and Practice. 6th ed. Pearson, 2016. URL:https://uomustansiriyah.edu.iq/media/lectures/6/6_2017_03_17!10_56_57_PM.pdf

4. Antoniewicz B. Elliptic Curve Cryptography Explained. 2018. URL:https://hal.science/hal-01914807/document