УДК 004.4

РОЗРОБКА ГІБРИДНОЇ СИСТЕМИ ШИФРУВАННЯ ДАНИХ

Максим Журавський, Юлія Павленко

DEVELOPMENT OF A HYBRID DATA ENCRYPTION SYSTEM

Maxym Zhuravskyi, Yuliia Pavlenko

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

***Abstract**. A software application has been developed that allows encrypting and decrypting data and provides the simplicity of symmetric key exchange through unsecured channels.*

Зростання кількості даних, які передаються через відкриті канали зв'язку, відповідно передбачає і їх захист. Для шифрування даних використовуються симетричні та несиметричні алгоритми. [1,2] Симетричні алгоритми шифрування використовують один і той самий ключ як для шифрування, так і для розшифрування даних, що забезпечує високу швидкість та ефективність при роботі з великими обсягами даних, але робить всю систему вразливою у випадку перехоплення ключа. Асиметричні (несиметричні) алгоритми використовують пару ключів: публічний (для шифрування) і приватний (для розшифрування), не вимагають передачі приватного ключа та є зручними для захисту каналів передачі ключів і цифрових підписів, але значно повільніші і тому менш ефективні для великих обсягів даних. [3,4] Поєднання цих алгоритмів, коли асиметричне шифрування використане для безпечної передачі симетричного ключа, після чого основний обмін даними здійснюється швидким симетричним алгоритмом, є набагато ефективнішим рішенням.

Створення додатку "Cyphering" передбачає поєднання алгоритмів AES (симетричне шифрування) та RSA (асиметричне шифрування) для надання користувачам можливості безпечно генерувати ключі, шифрувати та розшифровувати дані. Алгоритм AES забезпечує швидке та ефективне шифрування великих обсягів даних, а RSA використовується для безпечної передачі ключа AES. Таким чином, дані користувача шифруються надійним симетричним алгоритмом, а ключ для цього шифрування передається за допомогою асиметричного алгоритму.

На етапі проектування додатку був визначений його основний функціонал:

- генерація ключів RSA. Додаток повинен генерувати публічні та приватні ключі для асиметричного шифрування, що використовуються для захисту передачі симетричних ключів;
- обмін ключами. Публічний ключ RSA використовується для шифрування ключа AES, що дозволяє безпечно передати його іншому користувачу;
- AES шифрування та розшифрування. Для захисту великих файлів чи повідомлень використовується алгоритм AES, що забезпечує високу швидкість шифрування;

Додаток повинен мати зручний інтерфейс для генерації ключів, шифрування та розшифрування файлів, а також управління процесом обміну ключами.

В якості інструментальних засобів розробки додатку "Cyphering" вибрані:

- мова програмування Go (Golang) версії 1.21.0. Golang 1.21.0 є сучасною мовою програмування з підтримкою паралельних процесів, що дозволяє ефективно обробляти великі обсяги даних та забезпечувати швидке виконання операцій. Крім того, Go відзначається своїм швидким часом компіляції, що дозволило легко вносити зміни в додаток;
- вебсервер mux, який дозволяє легко організовувати обробку різних маршрутів, що є важливим для налаштування шифрування та розшифрування даних у додатку;

- бібліотека Fyne для створення графічних інтерфейсів користувача на мові Go. Fyne дозволяє швидко та легко розробляти кросплатформні інтерфейси, які працюють на різних операційних системах, таких як Windows, macOS та Linux.

Основною задачею під час програмної реалізації було забезпечення надійного та безпечного процесу шифрування даних за допомогою гібридного методу, який включає симетричне шифрування для основного захисту даних і асиметричне для безпечної передачі ключів.

Реалізація програмної частини шифрування в додатку "Cyphering" відбувалась поетапно. Процес починався з реалізації алгоритму генерації ключів для RSA. У рамках цього етапу програмний код забезпечував створення двох великих простих чисел, які використовуються для обчислення публічного та приватного ключів. Було реалізовано функції для перевірки простоти чисел і генерування таких значень, які були б достатньо великими для надійності шифрування.

Для генерації ключів використані обчислення, що включають обчислення добутку двох простих чисел (модуля), функції Ейлера та знаходження відкритого і закритого ключів на основі рівнянь, що відповідають алгоритму RSA. На основі створених ключів реалізовані методи шифрування та розшифрування. Для асиметричного шифрування використовувався відкритий ключ для зашифровування даних або симетричного ключа, який потім передається через мережу. Розшифрування здійснювалося за допомогою приватного ключа, який дозволяв відновити оригінальні дані або ключ, використаний у симетричному алгоритмі.

Структура інтерфейсу спроектована з урахуванням основних функцій додатку: шифрування даних, генерація та передача ключів, а також обробка вхідних і вихідних даних. Важливим аспектом розробки стала логічна організація елементів інтерфейсу, таких як текстові поля для введення ключів, кнопки для активації операцій шифрування і розшифрування, а також області для відображення результатів. Це дозволило забезпечити зручний доступ до всіх основних функцій програми.

Користувачам надана можливість генерувати публічні та приватні ключі й обирати їх бітність. Кнопки, що відповідають за виконання основних операцій, розміщені в межах інтерфейсу так, щоб користувач міг швидко перейти до бажаної функції без зайвих труднощів.

Для зворотного зв’язку з користувачем передбачено відображення повідомлень про успішне завершення операцій, а також інформаційних повідомлень у разі виникнення помилок. Це дозволяє користувачеві вчасно отримати необхідну інформацію для коректної взаємодії з програмою.

Програмний додаток "Cyphering" забезпечує простий та зрозумілий інтерфейс для користувачів, які бажають захистити свої дані без глибоких технічних знань. Він підходить для застосування в різних сферах, де потрібно зберегти конфіденційність даних під час їх передачі або зберігання, а також забезпечує простоту обміну симетричними ключами через незахищені канали.

Бібліографія

1. Галкін О.В., Шкільняк О.С. Основи криптології: навчальний посібник. Київ, 2023. 119 с.
2. Шифрування: типи і алгоритми. Що це, чим відрізняються і де використовуються? • Hostpro Wiki. *Hostpro Wiki*. URL: https://hostpro.ua/wiki/ua/security/encryption-types-algorithms/ (дата звернення: 20.05.2025).
3. Bauer Friedrich L. Decrypted Secrets: Methods and Maxims of Cryptology. Springer, 2010. 539p.
4. Wenbo M. Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2004. 707 p.