ДОСЛІДЖЕННЯ ТА РЕАЛІЗАЦІЯ АЛГОРИТМІВ КРИПТОГРАФІЇ НА C++

Чернявська А.О., Мєтєльов В.О.
Національний технічний університет «Харківський політехнічний інститут», м. Харків

Метою роботи було дослідити основні алгоритми криптографії, такі як симетричне та асиметричне шифрування, хешування та цифровий підпис, а також розробити програмне забезпечення з графічним інтерфейсом користувача для їх практичної реалізації. Створено зручний та інтуїтивний спосіб використання цих алгоритмів для шифрування, розшифрування, хешування та цифрового підпису файлів і даних.

Важливість роботи полягає в тому, що криптографія відіграє ключову роль у забезпеченні конфіденційності, цілісності та автентичності даних у сучасному цифровому світі. Реалізація криптографічних алгоритмів з графічним інтерфейсом користувача дозволяє широкому колу користувачів легко та безпечно застосовувати ці методи для захисту своїх даних. Крім того, робота демонструє практичне застосування теоретичних концепцій криптографії та сприяє поширенню знань у цій галузі.

Розроблене програмне забезпечення має графічний інтерфейс користувача, створений з використанням бібліотек C++ для створення вікон, меню та елементів управління. Користувач може вибрати потрібний криптографічний алгоритм, з меню яке представлене на інтерфейсі користувача. Для шифрування чи розшифрування користувач завантажує вхідний файл, вводить ключ або генерує його та запускає процес. Для хешування та цифрового підпису користувач завантажує вхідні дані та виконує відповідні операції.

Результати, такі як зашифрований чи розшифрований файл, хеш-значення чи цифровий підпис, відображаються в інтерфейсі або записуються у вихідний файл за вибором користувача. Програма має зручний та інтуїтивно зрозумілий інтерфейс, з можливістю перегляду допоміжної інформації та налаштування додаткових параметрів.

Представлена робота може бути використана для навчальних цілей у галузі криптографії та кібербезпеки. Студенти та викладачі зможуть демонструвати роботу різних криптографічних алгоритмів на практиці, поглиблюючи своє розуміння цієї важливої галузі. Програмне забезпечення відкриває перспективи для подальшого вдосконалення та розширення функціоналу. Завдяки модульній структурі та використанню мови програмування C++, розробники можуть додавати нові криптографічні алгоритми, поліпшувати інтерфейс користувача або інтегрувати додаткові можливості відповідно до потреб користувачів чи нових технологічних вимог.

Таким чином, робота не лише надає користувачам практичний інструмент для захисту даних, але й слугує демонстрацією важливості криптографії, навчальним ресурсом та платформою для подальшого розвитку в цій галузі.