

УДК 004.9

Миронова Н.О.¹, Ковальов Р.В.², Резніченко А.С.², Рогова Є.В.²,
Тихоновська Т.В.²

¹ канд. техн. наук, доц. НУ «Запорізька політехніка»

² студ. гр. КНТ-219сп НУ «Запорізька політехніка»

ВІЗУАЛІЗАЦІЯ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ ДЛЯ BLOCKCHAIN ТЕХНОЛОГІЙ. RSA (RIVEST–SHAMIR–ADLEMAN)

Актуальність роботи полягає в практичному підході до роботи із текстом і зображенням, де введена інформація зчитується та додається до масиву, що шифрується за відповідним ключем та дешифрується за другим ключем відповідним першому повертаючи початкову інформацію.

Метою даної роботи є розробка візуалізації криптографічних алгоритмів для Blockchain технології, а саме алгоритму шифрування RSA (Rivest–Shamir–Adleman).

Задачі роботи – це створити програмний продукт, який шляхом взаємодії з користувачем шифрувати і дешифрувати зображення за створеними ключами.

Система повинна забезпечувати:

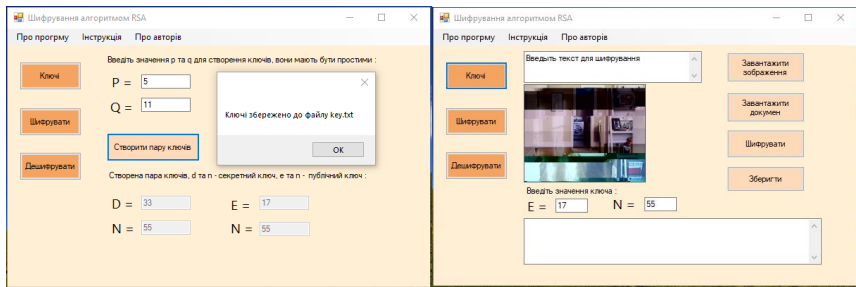
- завантаження зображення або тексту;
- зчитати зображення або текст в масив;
- шифрувати елементи масиву;
- вивести шифровану інформацію;
- завантажити шифроване зображення або текст;
- зчитати шифроване зображення або текст в масив;

- дешифрувати елементи масиву;
- вивести дешифровану інформацію.

Під час розробки було реалізовано наступні алгоритми:

- файлове зчитування та запис у файл;
- відображення візуальних та текстових елементів;
- завантаження зображення або тексту;
- розбиття зображення на байтовий масив та переведення цього масиву в інший формат;
- застосування алгоритму криптографічного шифрування RSA (Rivest–Shamir–Adleman).

На рисунку 1 представлено результати виконання розробленого коду.



а) Генерація ключів;

б) Шифрування зображення

Рисунок 1 – Приклади екранів форм програми

Під час виконання роботи було розроблено імітаційну програму на тему «Візуалізація криптографічних алгоритмів для Blockchain технології. RSA (Rivest–Shamir–Adleman)» для роботи з даними для забезпечення відображення алгоритму шифрування і дешифрування.

Створена імітаційна програма організовує систему для забезпечення вибору даних: зображення, текстовий файл. Для шифрування та дешифрування було використано криптографічний алгоритм RSA (Rivest–Shamir–Adleman). Таким чином, розробивши імітаційну програму можна зробити висновок, що алгоритм є ефективним для шифрування даних, проте його час роботи залежить від розміру цих даних. Відповідно, якщо файл є великим тоді і час виконання є довшим.

Вирішені наступні завдання роботи:

- виконано огляд сучасних програмних засобів реалізації візуалізації;
- розглянуті можливості та переваги мови програмування C#;
- розглянуті можливості та переваги середовища розробки JetBrains Rider;

– розроблено систему для відображення результатів роботи алгоритму шифрування RSA.