ГЕНЕРАЦІЯ СТЕГОКОНТЕЙНЕРІВ ДЛЯ ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КАНАЛІВ ПЕРЕДАЧІ ДАНИХ

Шевченко Н. Ю., к.е.н, доцент, natalygustav@gmail.com;
Парамонова К. О., магістрант, ekaterinaparamonova5230@gmail.com
Донбаська державна машинобудівна академія,
м. Краматорськ, Україна

Питання захисту інформаційних потоків під час їх передачі каналами зв'язку займає провідну позицію у процесі забезпечення інформаційної безпеки. Для збереження конфіденційності інформації традиційно використовують два способи програмного захисту: криптографічні та стеганографічні методи. Сутність криптографічного захисту полягає в тому, що інформація зашифровується певним алгоритмом в нечитабельний формат [1]. Стеганографічний захист — це приховування самого факту існування інформації шляхом вбудовування її в цифрові об'єкти (контейнери) [2].

Для забезпечення більшої надійності даних, що передаються, доцільно забезпечити як їх шифрування, так і приховування.

В загальному випадку стегосистему можна представити як сукупність контейнерів, повідомлень та перетворень, що їх зв'язують. Припустимо, що в якості повідомлення передаються згенеровані випадковим чином дані: логін і пароль. В якості візуальних контейнерів можна використовувати стохастичні фрактали, а шифрування даних здійснювати методом RSA. Далі зашифроване повідомлення ховається в молодших бітах зображення-фрактала і передається каналами відкритого зв'язку.

Отже, алгоритмічна модель для безпечної передачі даних через відкритий канал зв'язку передбачає реалізацію п'яти етапів: генерація логіна і пароля; побудова стохастичного фрактала «Плазма»; шифрування логіна і пароля алгоритмом RSA; приховування зашифрованого повідомлення в молодших бітах зображення-фрактала методом LSB (Least Significant Bits); відправлення зображення на електронну адресу користувача; розшифрування та витягування логіну та паролю з фрактала «Плазма».

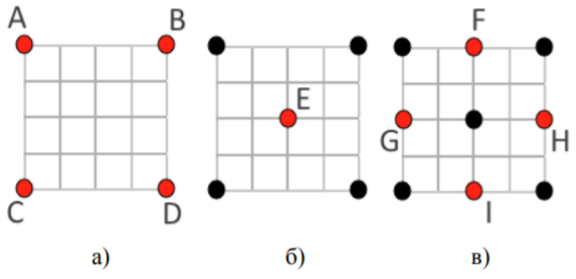

Рисунок 1. Алгоритм Diamond Square
(а) висота в кутових точках; б) значення в центральній точці; в) значення на серединах сторін)

Для побудови стохастичного фракталу «Плазма» використовується алгоритм Diamond Square [3]. Спочатку чотирьом кутам квадрата присвоюються випадкові величини. Після того, як задані кордони квадрата, він розбивається на чотири рівних квадрати, в кожному з яких відомо значення одного з кутів. Значення висоти центральної точки — сума

усереднення висот всіх чотирьох кутових точок і випадкового значення (шуму).

Алгоритм RSA складається з 4 етапів: генерації ключів, шифрування, розшифрування та розповсюдження ключів. Безпека алгоритму RSA побудована на принципі складності факторизації цілих чисел. Алгоритм використовує два ключі — відкритий (public) і закритий (private), разом відкритий і відповідний йому закритий ключі утворюють пари ключів (keypair). Якщо повідомлення було зашифровано відкритим ключем, то розшифрувати його можна тільки відповідним закритим ключем.

Сутність методу заміни найменш значущого біта LSB полягає в приховуванні інформації шляхом зміни останніх бітів зображення, які кодують колір на біти приховуваного повідомлення. У форматі BMP зображення зберігається як матриця значень відтінків кольору для кожної точки зображення.

Для реалізації наведеного алгоритму приховування та шифрування даних був спроєктований та розроблений відповідний програмний модуль.

Приклад роботи модуля наведений на рис. 2.

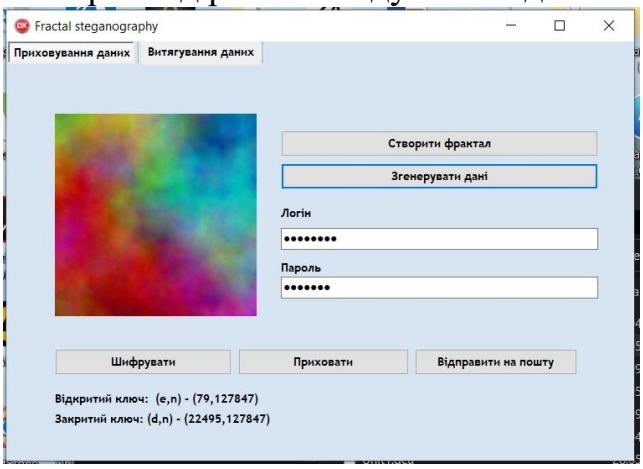

Рисунок 2. Генерація логіну та паролю

На вкладинці «Приховування даних» проходить повний цикл дій для отримання готового зображення с зашифрованими даними для ролі «Відправник». На початку треба натиснути на кнопку «Створити фрактал» для генерації стохастичного фрактала «Плазма». Після відображення фракталу на формі для генерації логіну та паролю потрібно натиснути на кнопку «Генерувати дані». Дані невидимі для відправника, захищені зірками. Наступним кроком циклу дій для отримання готового зображення з зашифрованими даними (приховування даних) буде шифрування логіну та паролю методом RSA. Для цього треба натиснути на кнопку «Шифрувати». Після цієї дії нижче кнопки з’являється відкритий та закритий ключі. Закритий ключ передається користувачу через захищений канал зв’язку. Після шифрування треба натиснути на кнопку «Приховати». Відбудеться приховування даних у останні біти згенерованого раніше фракталу методом LSB, растрування та зберігання зображення. Для відправки збереженого зображення на електронну пошту треба натиснути на кнопку «Відправити на пошту».

На вкладинці «Витягування даних» проходить повний цикл дій для отримання логіна та пароля для ролі «Отримувач». На початку треба перейти до своєї електронної пошти та знайти там відповідне повідомлення з прикріпленим зображенням (рис. 3). Повідомлення повинно мати: тему

«Фрактал», текст, який надрукував «Відправник», а також прикріплений малюнок стохастичного фрактала «Плазма».

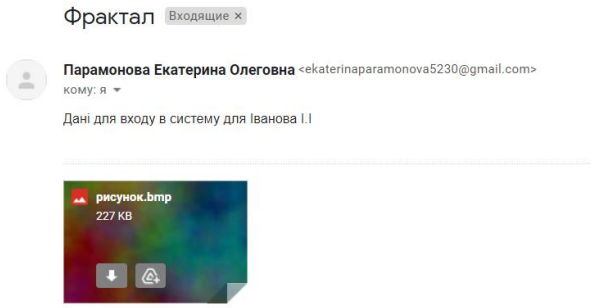

Рисунок 3. Повідомлення, яке прийшло на e-mail отримувача

Далі потрібно натиснути на кнопку «Дешифрування» для того, щоб система почала витягувати дані з зображення, а потім дешифрувати за допомогою закритого ключа. Після описаних вище дій в полях «Логін» та «Пароль» з'являться передані користувачеві вхідні дані. Отже, в умовах необхідності підвищення інформаційної безпеки даних, що передаються відкритими каналами зв'язку, наприклад електронною поштою, доцільно поєднувати криптографію із стеганографією, генеруючи при цьому для підвищення якості приховування даних контейнери-стохастичні фрактали.

Література

1. Криптографія [Електронний ресурс]. — URL: https://sci.ldubgd.edu.ua/bitstream/123456789/6169/1/1.pdf.

2. Комп'ютерна стеганографія [Електронний ресурс]. — URL: https://ela.kpi.ua/bitstream/123456789/23826/4/Romanchuk_magistr.pdf.

3. Алгоритм Diamond Square [Електронний ресурс]. — URL: http://wiki-org.ru/wiki/Алгоритм_Diamond-Square.

Анотація

Наведений алгоритм підвищення інформаційної безпеки даних, що передаються відкритими каналами зв'язку, який передбачає реалізацію декількох етапів: генерацію логіна і пароля; побудову стохастичного фрактала «Плазма»; шифрування логіна і пароля алгоритмом RSA; приховування зашифрованого повідомлення в молодших бітах фрактала методом LSB.

Ключові слова: криптографія, стеганографія, стохастичний фрактал.

Аннотация

Приведен алгоритм повышения информационной безопасности данных, которые передаются открытыми каналами связи, который предусматривает реализацию нескольких этапов: генерацию логина и пароля; построение стохастического фрактала «Плазма»; шифрование логина и пароля алгоритмом RSA; сокрытие зашифрованного сообщения в младших битах изображения-фрактала методом LSB.

Ключевые слова: криптография, стеганография, стохастический фрактал.

Abstract

An algorithm over of increase of informative safety of data that is passed by open communication channels is brought, that envisages realization of several stages: generation of login and password; a construction of stochastic fractal is Plasma; encipherement of login and password by the algorithm of RSA; hiding of in cipher report in the junior bats of image-fractal by the method of LSB.

Keywords: cryptography, steganography, stochastic fractal.