УДК 004.056.55:003.27

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ВИКОРИСТАННЯ МЕТОДІВ СТЕГАНОГРАФІЇ В ТЕКСТОВИХ ФАЙЛАХ ДЛЯ ПОКРАЩЕННЯ ЗАХИСТУ ДОСТУПУ ДО ОБЛІКОВОГО ЗАПИСУ ЗАВДЯКИ ШИФРУВАННЮ З ВИКОРИСТАННЯМ КУБИКА РУБІКА

Чорнуха К. Д., Мартинчук О.О.
e-mail: kateryna.chornukha@nure.ua
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна

The paper explores the possibilities of using steganographic techniques in text files in combination with encryption methods based on Rubik's Cube permutations to improve the security of access to user accounts. The proposed approach integrates classical cryptographic transformations with information hiding mechanisms, creating a multi-level protection model. Special attention is paid to the use of steganographic embedding methods that allow sensitive information, such as authentication tokens or encryption keys, to remain undetectable in text data. The results highlight the potential of hybrid cryptographic-steganographic approaches to improve account security mechanisms.

У сучасному цифровому середовищі питання захисту облікових записів користувачів є однією з ключових проблем інформаційної безпеки. Традиційні механізми автентифікації, такі як паролі або навіть двофакторна автентифікація, можуть бути вразливими до різних видів атак, зокрема фішингу, перебору паролів та витоку даних. У зв’язку з цим зростає інтерес до альтернативних методів підвищення безпеки, зокрема до використання криптографічних та стеганографічних технологій.

Стеганографія дозволяє приховувати інформацію всередині інших даних таким чином, щоб сам факт передавання секретного повідомлення залишався непомітним. Особливий інтерес становить використання текстових файлів як контейнера для прихованої інформації, оскільки вони є найпоширенішим форматом обміну даними в інформаційних системах.

Одним із цікавих підходів до шифрування інформації є використання механіки кубика Рубіка. Його структура базується на послідовностях перестановок елементів, що робить його природною моделлю для криптографічних алгоритмів. Класичний кубик Рубіка 3×3×3 має понад 4.3×1019 можливих станів, що створює велике простір можливих трансформацій даних. Завдяки цьому виникає можливість застосування принципів перестановок кубика для створення методів шифрування, які можуть використовуватися у поєднанні зі стеганографічними методами для прихованого зберігання ключів або автентифікаційної інформації.

Метою даного дослідження є аналіз можливостей використання принципів шифрування на основі кубика Рубіка у поєднанні зі

стеганографією в текстових файлах для підвищення безпеки доступу до облікових записів.

Однією з перших спроб використання кубика Рубіка в криптографії став метод, запропонований Дугласом Мітчеллом у 1992 році. Його підхід базувався на транспозиційному шифрі, у якому текст повідомлення розміщувався на розгортці кубика, після чого до нього застосовувалася послідовність поворотів граней. Кожен поворот відповідає певній перестановці символів, а вся послідовність поворотів утворює ключ шифрування.

У такій системі відкритий текст розміщується на поверхні кубика у визначеному порядку, після чого застосовується певна послідовність обертів. У результаті символи перемішуються відповідно до перестановок, які створюються рухами кубика. Для отримання шифртексту символи зчитуються у заданому порядку з різних граней кубика.

Ключ шифрування в такій системі складається з двох частин:

розширення ключа, яке визначає порядок зчитування символів із граней кубика;

послідовності поворотів, що задає конкретні перестановки символів.

Кількість можливих комбінацій таких перестановок є надзвичайно великою, що створює значний простір ключів. Однак подальші дослідження показали, що сам по собі цей метод не є достатньо криптостійким. Основною причиною є те, що не всі перестановки символів можуть бути реалізовані реальними обертами кубика, оскільки вони обмежені груповою структурою головоломки.

Незважаючи на це, принципи перестановок, які лежать в основі кубика Рубіка, можуть бути використані у сучасних криптографічних системах. Особливо перспективним є поєднання таких методів із технологіями стеганографії. Наприклад, зашифрований за допомогою перестановок текст може бути додатково прихований у текстових файлах шляхом використання спеціальних маркерів, невидимих символів або варіацій форматування.

У контексті захисту облікових записів це може реалізовуватися у вигляді прихованого зберігання ключів або автентифікаційних даних у текстових документах. У такому випадку зловмисник, навіть отримавши доступ до файлу, не зможе легко виявити наявність прихованих даних або відновити їх без знання алгоритму перестановок та ключа.

Крім того, сучасні дослідження показують, що принципи кубика Рубіка використовуються у різних криптографічних підходах, зокрема в алгоритмах шифрування зображень та мультимедійних даних. У таких системах застосовуються методи багаторівневих перестановок, хаотичних відображень та дифузії, що дозволяє досягти високого рівня криптографічної стійкості.

Таким чином, використання перестановок кубика Рубіка може розглядатися не лише як навчальний приклад криптографічного алгоритму, але і як джерело ідей для створення нових методів захисту інформації.

У результаті проведеного дослідження було проаналізовано можливості використання принципів перестановок кубика Рубіка у криптографічних системах та їх поєднання зі стеганографічними методами у текстових файлах.

Встановлено, що механіка кубика Рубіка може слугувати наочною моделлю для реалізації транспозиційних шифрів, оскільки послідовності поворотів утворюють складні перестановки елементів. Хоча класичний метод Мітчелла має певні криптографічні обмеження, його концепція демонструє потенціал використання перестановок для шифрування текстових даних.

Поєднання такого підходу зі стеганографією дозволяє створювати додатковий рівень захисту інформації, приховуючи зашифровані дані у текстових файлах. Це може бути використано для підвищення безпеки доступу до облікових записів, зокрема шляхом прихованого зберігання ключів або автентифікаційної інформації.

Отримані результати свідчать про перспективність подальших досліджень у напрямку інтеграції криптографічних алгоритмів, заснованих на перестановках, зі стеганографічними методами захисту інформації.

Список використаних джерел:

1. Шифрування зображень на основі генерації ключів за принципом кубика Рубіка для алгоритму AES // International Journal of Computer Applications. 2021. Т. 183, № 4. С. 24–31.

2. Петі К., Кіскватер Ж.-Ж. Кубик Рубіка для криптографів // Cryptology ePrint Archive, Report 2013/118. 2013. 15 с..

3. Схема шифрування кольорових зображень на основі керованого кубика Рубіка та квантового випадкового блукання // Scientific Reports. 2022. № 12. URL: https://pmc.ncbi.nlm.nih.gov/articles/PMC9395402/.