ФРАКТАЛЬНЕ ШИФРУВАННЯ КЛІЄНТ-СЕРВЕРНИХ ЗАСТОСУНКІВ

Сєвєрінов О.В., Лєвтєров О.А., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

При сучасному цифровому розвитку у всіх галузях господарства усе більше залежність від використання технологій, смартфонів, комп'ютерів і Інтернету. Однак, зі збільшенням кількості інформації, яка обробляється й передається через мережі, зростає й ризик несанкціонованого доступу до неї з боку зловмисників [1]. Одним з таких видів передавання інформації є архітектура "Клієнт-Сервер" ("мережа Клієнт-Сервер"). Щоб захистити цифрові данні, що передаються в мережі від злочинців повинно використовувати шифрування.

Одним з альтернативних сучасних методів шифрування є метод фрактального шифрування, який використовує як кодуючу функцію фрактальну послідовність [2]. **Метою доповіді** є розгляд принципів фрактального шифрування клієнт-серверних застосунків.

Фрактальну послідовність одержують за допомогою ітераційної функції, яка у свою чергу є однобічною функцією, у таких функцій визначення аргументів за значенням самої функцій не може бути зроблене більш ефективно, ніж перебором по безлічі значень початкових параметрів [3]. Для опису ітераційної функції, досить указати набір дійсних чисел, які задають початкові умови ітераційного процесу побудови фрактальної послідовності. Це дає досить простий метод шифрування, він є варіантом гамірования - процесу "накладення" гама-послідовності на відкриті дані [4], де в якості гама-послідовності (послідовності псевдовипадкових елементів) використовується фрактальна послідовність, що генерується за допомогою ітераційної функції за початковими параметрами [5].

Таким чином, використання фрактальних послідовностей як ключа для шифрування достатньо просте й ефективне. Для їх побудови необхідна невелика кількість параметрів, при цьому на виході формуються об’єкти зі складними хаотичними межами.

Список літератури

1. Голубничий Д.Ю., Сєвєрінов О.В., Коломійцев О.В., Місюра О.М., Третяк В.Ф., Власов А.В., Крук Б.М. (2021). Аналіз сучасних загроз в інформаційних системах за складовими загроз: кібербезпеки, інформаційної безпеки та безпеки інформації.

2. Mandelbrot, B. The Fractal Geometry of Nature. USA: Echo Point Books & Media, LLC. 2021. 500 p. DOI: https://doi.org/10.1119/1.13295.

3. Soumitro Banerjee. Fractal Image Compression. Available at: https://youtu.be/Lte3xpmH2_g (accessed 23.03.2023).

4. Xian Y., Wang X. Fractal sorting matrix and its application on chaotic image encryption //Information Sciences. – 2021. – Т. 547. – С. 1154-1169.

5. Chen G., Ueta T. Yet another chaotic attractor //International Journal of Bifurcation and chaos. – 1999. – Т. 9. – №. 07. – С. 1465–1466.