ДЕЯКІ ПИТАННЯ ВИКОРИСТАННЯ ХАОТИЧНИХ КАРТ ДЛЯ КРИПТОГРАФІЇ

Журило О.Д., Ляшенко О.С.

Харківський національний університет радіоелектроніки, м. Харків

Теорія хаосу з другої половини XX ст. прочно увійшла в наукові дисципліни: від математики та інформатиці і до біології та робототехніки. Не є виключенням і криптографія. За останні 10 років теорію хаосу та нелінійну динаміку було використано при розробці багатьох криптографічних примітивів, які включали хеш-функції, потокові шифри, системи шифрування текстів та зображень, безпечні генератори псевдовипадкових чисел і багато іншого.

В останні роки питання захисту комп'ютерних даних стає все гострішим. Одним з можливих варіантів захисту інформації є створення цифрових водяних знаків, стійких до спотворень саме з використанням теорії хаосу.

Найбільш простими варіантами хаотичних карт для створення стабільних цифрових міток є логістична карта (1976 р.), карти Хенона (1976 р.) та карти кота Арнольда (1967 р.).

Аналіз придатності використання хаотичних карт на предмет їх здатності забезпечувати стабільність диспетчера вікон робочого стола було виконано в 2021 р. Дискретні відображення працюють у вигляді повторюваних функцій, які тотожні криптосистемним раундам. Ця тотожність між криптографією та хаотичними динамічними системами дискретного ладу є основою для розробки хаотичних криптосистем. Кожна карта містить оригінальні параметри, які дорівнюють криптографічним ключам шифрування. Хаотична система використовується в потокових шифрах для генерації потоку псевдовипадкових ключів, а відкритий або секретний ключ використовується в блокових шифрах в якості початкового і керуючого параметра, а потім зашифрований текст виходить із застосуванням певної кількості ітерацій до хаотичних систем. Безпека та складність є основними проблемами в криптосистемах. Чисельні алгоритми, засновані на хаосі, забезпечують достатнє поєднання високої швидкості та безпеки при мінімумі обчислювань. А ще й, чимала кількість алгоритмів, які засновані на хаосі, як і деякі динамічні системи забезпечують роботу масивів властивостей, таких як псевдовипадкові властивості, ергодичність та неперіодичність генерованих символів, залежність до початкових параметрів.

На початку 2020 рр. було запропоновано виконувати аналіз гістограми зображення, як найпростіший методів демонстрації якості шифрування, який дозволяє генерувати зашифроване зображення з рівномірно розподіленою інтенсивністю гістограми. Отримана кореляція між сусідніми пікселями в різних напрямках (горизонтальному, вертикальному або діагональному) визначається як показник ефективності шифрування. З використанням хаотичних карт значно ускладнюється розшифровка без точних значень ключа споживачем.

Таким чином, в останні десятиріччя було виконано використання хаотичних карт для забезпечення стабільності диспетчера вікон робочого стола. Це дозволить вийти на новий рівень захисту інформації, та забезпечити безпеку використання інформації, захисту авторських прав на графічну інформацію та геометричні образи, зробити роботу комп'ютерних систем більш безпечною.