Пастернак Юрій Юрійович
Національний університет «Одеська юридична академія»,
студент 1-го курсу магістратури факультету кібербезпеки
та інформаційних технологій

СПОСІБ ВИКОРИСТАННЯ ЕЛЕМЕНТАРНИХ КЛІТИННИХ АВТОМАТІВ ДЛЯ ШИФРУВАННЯ ДАНИХ

Клітинні автомати – це дискретна модель, набір клітинок що формують решітку значень, які залежать від стану клітини в момент часу та стану клітин-сусідів. Клітинні автомати, незважаючи на простоту опису їх клітин, як складових частин, можуть мати дуже складну поведінку. Кожна клітина в кожен момент часу може мати один з кінцевої множини станів. Однорідний бінарний клітковий автомат з двома можливими станами, в якому стан клітини в кожен момент часу залежить лише від її особистого стану і стану суміжних з нею клітин в минулий момент часу називають елементарним автоматом [1]. Кожна клітина автомату може приймати значення 0 чи 1. В кожен момент часу кожна клітина може мати різне значення. Це дає можливість використати множину значень клітин у якості ключа для XOR-шифрування. Таким ключем може виступити n-ітерація зміни значень клітин. У цій ситуації виникає проблема кінцевості автомату та теоретичної можливості розшифрування даних за допомогою повернення до його початкового стану.

Спосіб використання алгоритму буде наступним: спочатку необхідно розбити строку інформації, яку необхідно зашифрувати на окремі символи, а потім код кожного окремого символу необхідно розташувати в клітини автомату. Після цього використовується правило переходу станів та через n-число ітерацій автомату результат його еволюції необхідно використати як код символу. Таку процедуру необхідно повторити для кожного символу строки інформації. У результаті отримується зашифрований текст. Загрозою розкриття такого шифру може бути метод грубої сили, завдяки якому можна

розшифрувати текст, повернувши автомат до первинного значення (особливо враховуючи існування лише 256 елементарних кліткових автоматів[2]). Звісно, навіть у такій ситуації розшифрування займе дуже велику кількість часу, але метод можна ускладнити, наприклад, використовуючи його лише як один з етапів шифрування. Також можна використати еволюцію іншого клітинного автомату для повторного шифрування вже зашифрованої інформації. Враховуючи існування 256 елементарних клітинних автоматів, процедуру можна провести 256 раз. В такій ситуації метод грубої сили, скоріш за усе, втратить можливість розшифрувати інформацію через виникнення так званого «комбінаторного вибуху».

Станом на сьогодні клітинні автомати активно використовуються в багатьох сферах наукових досліджень – в фізиці, хімії, біології тощо. В моделях клітинних автоматів вдається доволі точно відтворювати велику кількість природніх явищ завдяки моделюванню процесів, які лежать в їх основі. В цих дослідженнях значною перевагою є регулярна структура решітки клітин автомату, однак в криптографії така регулярність стає недоліком у питанні криптостійкості. Недолік виправляється за рахунок математичного збільшення можливих комбінацій для шифрування та збільшення кількості часу, необхідного для методу грубої сили, але разом зі збільшенням часу, необхідного для дешифрування даних, збільшується і час, необхідний для шифрування.

Останнім часом спостерігається зростання уваги до клітинних автоматів в сфері криптографічних досліджень. Це пояснюється самою природою клітинних автоматів, їх паралельністю та циклічністю. Це дозволяє використовувати їх для одночасної обробки великої кількості процесів. Таким чином, використовуючи паралельні процеси для кожного окремого символу строки, що шифрується, можливо позбавитись проблеми, необхідності занадто великої кількості необхідних ресурсів для шифрування інформації. Таким чином, враховуючи стрімкий розвиток технологій та виникнення нових

обчислюваних можливостей, складнощі використання клітинних автоматів стають все менш актуальними.

Список використаних джерел:

1. Cellular Automata. Stanford Encyclopedia of Philosophy [Електронний ресурс] – Режим доступу до ресурсу: https://plato.stanford.edu/entries/cellular-automata/.

2. Index to Elementary Cellular Automata [Електронний ресурс] – Режим доступу до ресурсу: https://oeis.org/wiki/Index_to_Elementary_Cellular_Automata.

3. Elementary Cellular Automaton [Електронний ресурс] – Режим доступу до ресурсу: https://mathworld.wolfram.com/ElementaryCellularAutomaton.html.

Ключові слова: криптографія, клітинні автомати, шифрування, елементарні клітинні автомати

Ключевые слова: криптография, клеточные автоматы, шифрование, элементарные клеточные автоматы

Keywords: cryptography, cellular automata, encryption, elementary cellular automata.

Науковий керівник: *к.т.н. доцент Бойко В. Д.*

Васильєв Богдан Георгійович
Національний університет «Одеська юридична академія»
студент 4-го курсу факультету кібербезпеки
та інформаційних технологій

SQL-ІН'ЄКЦІЯ ТА ЇЇ НЕБЕЗПЕКА

SQL-ін'єкція-це хакерська техніка, яка була виявлена більше п'ятнадцяти років тому і до сих пір доводить свою руйнівну ефективність сьогодні, залишаючись головним пріоритетом безпеки баз даних.

Є багато негативних наслідків SQL-ін'єкції, наприклад, 21 лютого 2014 року на форумі Організації Об'єднаних Націй з управління інтернетом стався витік даних 3215 облікових записів. У серпні 2014 року в Мілуокі компанія комп'ютерної безпеки Hold Security повідомила, що виявила крадіжку