МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

Практические разработки на базе клеточных автоматов

АВТОРЕФЕРАТ
Дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Латышевой Анастасии Игоревны

Научный руководитель
доцент, к.ф.-м.н., доцент _____ А. Н. Гамова
23.01.2021 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2021 г.

Саратов 2021

ВВЕДЕНИЕ

Теория клеточных автоматов существует более пятидесяти лет. Развитием данного направления науки занимались такие выдающиеся учёные, как: Джон фон Нейман, Станислав Улам, Джон Конвей, а также Стивен Вольфрам. Многие из них искали практическое применение теории клеточных автоматов.

Проблема безопасного хранения паролей является актуальной как никогда раньше. Каждый день миллионы пользователей регистрируются на различных сайтах и в различных системах. А с ростом пользователей растёт и количество атак на базы данных паролей. Одним из распространённых решений данного вопроса является хранение хэш-кодов вместо самих паролей.

Другим актуальным направлением разработок в криптографии на сегодняшний день является безопасная передача сообщений между пользователями. Существует множество алгоритмов и протоколов, направленных на решение данной проблемы, но учёные и программисты не перестают создавать новые технологии.

О применении теории клеточных автоматов в криптографии говорят уже давно. Данные структуры очень просты в реализации в программном виде. При этом развитие клеточного автомата происходит относительно быстро, так как, по сути, это линейная замена одних символов на другие в соответствии с правилом развития клеточного автомата. Теорию клеточных автоматов можно применять и для вычисления хэш-кодов паролей и для шифрования сообщений.

Целями данной дипломной работы являются разработка программы вычисления хэш-кода пароля на основе одномерного клеточного автомата и разработка программы шифрования сообщения на основе двумерного клеточного автомата при различных входных данных.

Для достижения целей дипломной работы необходимо решить следующие задачи:

1. Изучить теорию клеточных автоматов;
2. Ознакомиться с основами теории хэш-функций;
3. Ознакомиться с основами шифрования;

4. Рассмотреть методы вычисления хэш-кодов паролей на основе теории одномерных клеточных автоматов;

5. Рассмотреть методы шифрования сообщения на основе теории двумерных клеточных автоматов;

6. Разработать программу вычисления хэш-кода пароля с помощью одномерного клеточного автомата;

7. Разработать программу шифрования сообщения с помощью двумерного клеточного автомата;

8. Провести анализ результатов работы программ.

Дипломная работа состоит из введения, 4 разделов, заключения, списка использованных источников и 4 приложений. Общий объем работы – 106 страниц, из них 68 страниц – основное содержание, включая 76 рисунков и 5 таблиц, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе приводятся теоретические сведения, которые относятся к клеточным автоматам. Здесь излагаются основные определения, связанные с одномерными и двумерными клеточными автоматами, их классификация, правила их развития, а также рассматривается математическая модель клеточного автомата.

В книге Томмазо Тоффоли «Машины клеточных автоматов» приводится следующее определение: «клеточные автоматы являются дискретными динамическими системами, поведение которых полностью определяется в терминах локальных зависимостей».

Одномерный клеточный автомат представляет собой массив, состоящий из клеток, следующее состояние которых определяется её нынешним состоянием и нынешним состоянием её соседей или, другими словами, окрестностью клетки. Как правило, рассматривают одномерные клеточные автоматы с двумя состояниями. Такие клеточные автоматы называют *элементарными*. На рисунке 1 продемонстрирована окрестность клетки одномерного клеточного автомата.

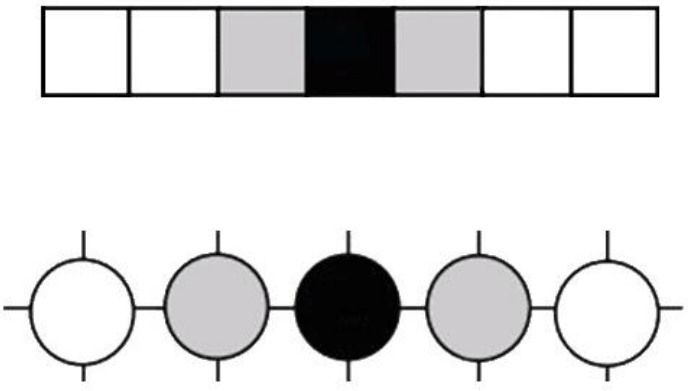

Рисунок 1 – Окрестность клетки одномерного клеточного автомата

Двумерный клеточный автомат представляет собой однородную «решётку», в каждой клетке которой находится конечный автомат. Для такого клеточного автомата следующее состояние клетки определяется её нынешним состоянием и нынешним состоянием её соседей.

Окрестность фон Неймана – это совокупность ячеек в сетке, имеющих общую грань с данной ячейкой.

Окрестность Мура – это совокупность ячеек в сетке, имеющих общую вершину с данной ячейкой. Окрестность Мура порядка r в двумерном случае представляет собой квадрат со стороной $2r + 1$.

На рисунке 2 продемонстрированы окрестность фон Неймана и окрестность Мура для двумерного клеточного автомата.

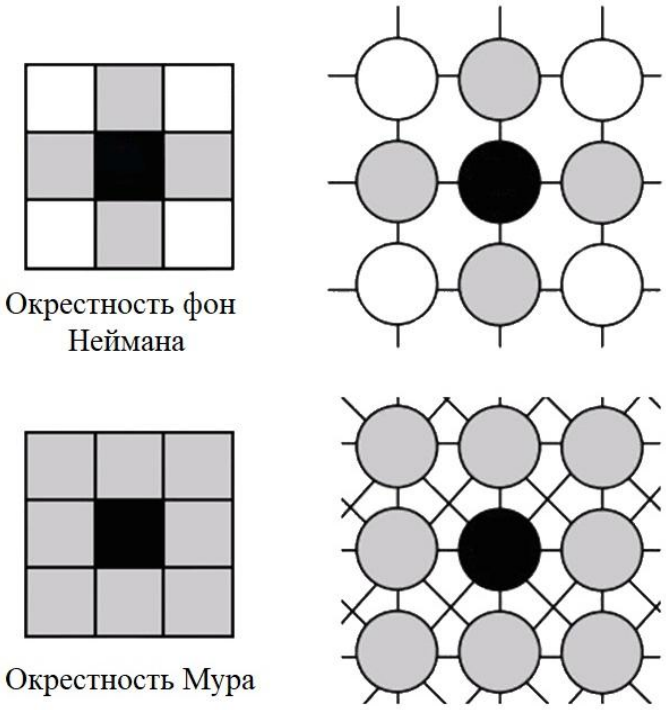

Рисунок 2 – Окрестность клетки двумерного клеточного автомата

Все клетки обладают следующими свойствами:

1. Решётка однородна;
2. Взаимодействия локальны (на состояние клетки влияет только её окрестность);
3. Множество состояний клетки конечно;
4. Изменения значений всех клеток происходят одновременно.

Иногда какие-то свойства могут не выполняться. Это зависит от конкретной задачи, для решения которой применяется клеточный автомат.

Формально клеточный автомат обозначается следующим образом:

$$A =< R, S, O, f >,$$

где:

A – клеточный автомат;

$R -$ решётка автомата (набор его клеток);

$S -$ конечное множество состояний клетки;

O – конечное множество, которое определяет окрестность клетки;

$f: S \times S^{|O|} \to S -$ функция перехода.

Правилами развития клеточных автоматов называются схемы, по которым происходит изменение состояний автомата в следующий момент времени. Всего существует 256 возможных правил для одномерных клеточных автоматов. Они были описаны Стивеном Вольфрамом с помощью кодов Вольфрама, где названия правил совпадают с нумерацией кодов, то есть от 0 до 255.

Во втором разделе приводятся теоретические сведения, которые относятся к хэш-функциям. Здесь излагаются основные определения, связанные с хэш-кодами, перечислены основные виды атак на хэш-коды паролей, а также рассмотрены методы применения теории клеточных автоматов для их вычисления.

В ГОСТе 34.11-2018 приведено следующее определение хэш-функции: «хэш-функция – это функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) По данному значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) Для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) Сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение».

Хэш-код – это строка бит, являющаяся выходным результатом хэш-функции.

Хэш-функции используются в следующих случаях:

- Проверка целостности данных;

- Система аутентификации (применение хэш-функции для паролей);
- Создание и проверка электронной цифровой подписи.

Соль – это строка данных, которая передаётся хэш-функции вместе с входным массивом данных для вычисления хэша.

Применение хэш-функции для вычисления хэш-кодов паролей является односторонним процессом, то есть, нет необходимости в обратимости функции перехода. Следовательно, для получения хэш-кода пароля можно использовать классические 256 правил развития одномерного клеточного автомата, которые являются необратимыми.

В третьем разделе приводятся теоретические сведения, которые относятся к шифрованию. Здесь излагаются основные определения, связанные с процессом шифрования, типы шифрования, а также рассмотрены методы применения теории клеточных автоматов для их вычисления.

Криптография – это совокупность идей и методов, связанных с преобразованием информации с целью её защиты от непредусмотренных пользователей.

Открытый текст – это информация, которая представлена в виде некоторого текста.

Шифр – это способ преобразования открытого текста в защищенную форму.

Шифрование – это процесс применения шифра к защищаемой информации: преобразование открытого текста в криптограмму с помощью определённых правил, содержащихся в шифре.

Криптограмма – полученный в результате шифрования изменённый текст.

Дешифрование – это процесс, обратный шифрованию: преобразование криптограммы в открытый текст с помощью определённых правил, содержащихся в шифре.

Ключ – некоторая дополнительная информация, в которой спрятан секрет шифра. Без знания ключа чтение криптограммы затруднительно.

В криптографии все шифры делятся на два типа: симметричные и асимметричные.

Симметричные шифры – это такие шифры, где для шифрования и дешифрования применяется один и тот же секретный ключ.

Асимметричные шифры – это такие шифры, где для шифрования и дешифрования применяются разные ключи.

На практике клеточный автомат при шифровании может использоваться следующим образом:

1. Открытый текст на входе является начальным состоянием клеточного автомата, над которым и проводятся раунды шифрования (развитие клеточного автомата во времени). В таком случае ключом является только правило развития клеточного автомата;

2. Над начальным состоянием клеточного автомата проводятся раунды шифрования (развитие клеточного автомата во времени), после чего производится некоторая операция между блоками открытого текста и клеточным автоматом. В таком случае ключом является начальное состояние клеточного автомата и правило его развития.

Клеточный автомат будет называться обратимым, только тогда, когда он является инъективным и сюръективным.

Сюръективный клеточный автомат – это такой клеточный автомат, у которого у каждой конфигурации автомата есть родитель (предшествующая конфигурация).

Инъективный клеточный автомат – это такой клеточный автомат, у которого нет конфигураций, имеющих одинаковых детей последующих конфигураций.

Другими словами, *обратимым* клеточный автомат будет называться тогда и только тогда, когда у каждой уникальной текущей окрестности клетки будет своё уникальное новое состояние клетки.

В четвертом разделе приведена реализация практических разработок на основе клеточных автоматов: вычисления хэш-кода пароля с помощью

одномерного клеточного автомата, а также шифрование и дешифрование сообщения с помощью двумерного клеточного автомата. Все разработки были выполнены на языке программирования Python.

Программа для вычисления хэш-кода пароля делится на простую и улучшенную реализацию. В простой реализации считывается логин и пароль с консоли, генерируется соль, происходит выбор правила развития одномерного клеточного автомата на основе логина, развитие клеточного автомата, и запись полученных данных в файл. Так же в программе присутствует функция сравнения новых введённых логина и пароля с хэш-кодом, который хранится в файле.

В улучшенной реализации считывается логин и пароль с консоли, генерируется соль, происходит выбор правила развития одномерного клеточного автомата на основе соли, выбирается n – количество раундов развития клеточного автомата на основе соли, развитие клеточного автомата n раз, и запись полученных данных в файл. Так же в программе присутствует функция сравнения новых введённых логина и пароля с хэш-кодом, который хранится в файле.

При рассмотрении примеров работы программ был сделан вывод, что в простой реализации при определенных входных данных часть хэш-кода у разных пользователей может совпадать. Но подобное в улучшенной реализации не происходит.

Программа для шифрования сообщения делится на две программы: в первой на вход поступает отдельное начальное состояние двумерного клеточного автомата, а во второй открытый текст выступает в роли начального состояния клеточного автомата.

В первой программе происходит считывание входных данных, запись клеточного автомата в двумерный массив размерностью $3 \times x$, развитие клеточного автомата n раз согласно правилу развития клеточного автомата, операция xor между блоками открытого текста и получившимся клеточным

автоматом, и запись полученных данных в файл. Так же в программе присутствует функция дешифрования сообщения из входной криптограммы.

Во второй программе происходит считывание входных данных, запись открытого текста в двумерный массив размерностью $3 \times x$, развитие полученного клеточного автомата n раз согласно правилу развития клеточного автомата, и запись полученных данных в файл. Так же в программе присутствует функция дешифрования сообщения из входной криптограммы.

Отдельно было рассмотрено функционирование программ при одинаковых входных данных, где было проведено не только вычисление хэш-кодов паролей и шифрование сообщения, но и сравнение нового пароля и хэш-кода с корректными и некорректными данными, а также дешифрование сообщения с корректными и некорректными данными.

ЗАКЛЮЧЕНИЕ

Впервые клеточные автоматы были упомянуты в далёких 50-х годах прошлого века, но и по сей день учёные не перестают выдвигать новые гипотезы и создавать новые системы, основываясь на теории клеточных автоматов.

Разработка новых алгоритмов и продуктов в области криптографии не останавливается, и программисты каждый день ищут новые методы и технологии для использования в данном направлении. Одной из таких технологий является теория клеточных автоматов.

Потребность в безопасном хранении паролей и в безопасной передаче сообщений только растёт. Оба направления криптографии можно основывать на теории клеточных автоматов. Если для вычисления хэш-кода пароля достаточно применять и одномерные клеточные автоматы с их классическими 256 правилами развития, то для шифрования они не подходят.

В практической части данной работы были разработаны две программы на основе клеточных автоматов на языке Python. Первая программа включает в себя две реализации вычисления хэш-кода пароля на основе одномерного клеточного автомата: простую и улучшенную. Вторая программа представляет собой систему шифрования и дешифрования сообщения на основе двумерного клеточного автомата. Она состоит из двух реализаций: в одной из них открытый текст выступает в роли начального состояния клеточного автомата, в другой – на вход передаётся отдельное начальное состояние клеточного автомата.

При анализе результатов работы программ было отмечено, что подбор правила развития клеточного автомата и количество раундов подсчёта хэш-кода рекомендуется основывать не на логине, а на соли. Так уменьшается вероятность подбора нужных данных для вычисления хэш-кода третьими лицами. В программе для шифрования сообщения при наличии отдельного начального состояния клеточного автомата есть вероятность появления вместо криптограммы открытого текста или его части. Но подобное не было

обнаружено у программы, которая использует открытый текст в качестве начального состояния. Так же начальное состояние при внедрении данной технологии в криптосистему необходимо будет передавать по защищенному каналу передачи сообщений, что усложняет работу.

Исходя из общего положения и опираясь на вышеперечисленные факты, можно сделать вывод, что применение теории одномерных и двумерных клеточных автоматов в криптографии является перспективным направлением современных разработок.