**Исследовательская работа**

**на тему:** Алгоритм шифрования на основе элементарных клеточных автоматов

**Автор работы:**

**Обучающийся 8 класса**

**ГБОУ Гимназия №1538**

Чистобаев Андрей Андреевич

**Руководитель работы:**

**Консультант**

Носкова Людмила Николаевна,

Преподаватель математики, высшая категория

**Москва**

**2017 год**

# Содержание

## Введение…………………………………………………………………………3

## Критерии оценки……………………………………………………………….4

## Концепция……………………………………………………………………….5

## Ресурсы…………………………………………………………………………..7

## План выполнения………………………………………………………………8

## Реализация………………………………………………………………………9

## Оценка итогов работы…………………………………………………….….11

## Литература……………………………………………………………………..12

## Приложение. О работе элементарных клеточных автоматов……..……13

# Постановка проблемы

Сохранение конфиденциальности данных пользователей очень важно в нашем информационном обществе. Для обеспечения безопасности используются криптографические алгоритмы и хэш-функции. Но почему мы должны доверять этим инструментам, которыми подчистую пользуются крупные компании, не спросив нашего мнения?

Доверие к используемому инструменту зависит от его надёжности, которая определяется множеством тестов, созданных профессионалами. В криптографии для описания надёжности используется термин криптостойкость.

Поэтому, перед использованием алгоритма необратимого шифрования основанного на элементарном клеточном автомате на своём сайте, я решил провести полноценное тестирование самостоятельно. Для того чтобы тесты были действительно полноценны и всесторонне описывали алгоритм, я ознакомился с основами криптографии и криптоанализа при помощи замечательной книги Брюса Шнайера, «Прикладная криптография».

Если понимание некоторых терминов вызвало у вас затруднение, то милости прошу в приложение 2. В первом приложении вы найдёте информацию о работе элементарных клеточных автоматов. В третьем описана работа самого алгоритма. Четвёртое содержит список всех литературных источников.

Для полноценного понимания хода исследования рекомендуется читать текст работы последовательно, от начала до конца. Приятного чтения.

# Критерии оценки

Как понять, что работа выполнена успешно? Что для нас есть успех? Нужно дать определение.

Моя работа считается успешно выполненной, когда в её итоге выбранный мною алгоритм шифрования будет использован на сайте. То есть я собираюсь не только протестировать его, но и при необходимости модифицировать.

При криптоанализе стоит считать, что злоумышленнику известен наш алгоритм. Поэтому в программе-тестировщике я допускаю использование своей реализации алгоритма. Но имеются и другие данные: открытый текст и шифротекст. В соответствии с известными данными выделяют 4 основных метода криптоанализа:

1. Атака на основе шифротекста
2. Атака на основе открытых текстов и соответствующих шифротекстов
3. Атака на основе подобранного открытого текста
4. Атака на основе адаптивно подобранного открытого текста

Моя реализация должна быть подвергнута всем этим видам атак. На основе результатов попыток взлома я решу, что стоит переделать, а что добавить. Криптостойкость конечной версии я сравню с криптостойкостью других аналогичных алгоритмов шифрования.

Так же реализация должна быть переносимой и производительной. Производительность конечной версии будет сравнена как с производительностью других алгоритмов, так и с производительностью предыдущих версий. Переносимости я добьюсь при помощи использования лишь стандартных средств, поддерживаемых на всех устройствах, от умных утюгов до персональных компьютеров.

# Концепция