Министерство образования Республики Беларусь

Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.55

Емельяненко
Александр Игоревич

# АЛГОРИТМЫ КРИПТОАНАЛИЗА ШИФРОВ

**АВТОРЕФЕРАТ**
на соискание степени магистра технических наук

по специальности 1-40 80 02 «Системный анализ, управление
и обработка информации»

Научный руководитель
Ломако Александр Викторович
доцент, кандидат технических наук

Минск 2021

# ВВЕДЕНИЕ

В современном мире информационный ресурс стал занимать одно из важнейших мест в экономическом развитии. Обладание информацией необходимого качества в нужном месте и в нужное время считается залогом успеха в различных видах хозяйственной деятельности. Монопольное владение конкретной информацией часто оказывается главным преимуществом в конкурентной борьбе и тем самым, предопределяет, высокую стоимость "информационного фактора», который просто катастрофически нуждается в своей защите.

Безопасность данных используют во многих сферах, начиная с небольших компаний, интернет-магазинов, заканчивая крупными корпорациями, банками, и государственными структурами. Поэтому методы защиты информации интенсивно совершенствуются. Появляются новые программы для сохранения и кодирования данных, для предупреждения вторжений и для исключения хищения данных, создаются новые алгоритмы шифрования и дешифрования данных для того, чтобы твои данные не смогли открыть нежелательные лица.

По мере совершенствования основных характеристик систем безопасности данных возникают новые возможности для решения задач все возрастающего объема и сложности. К их числу относится шифрование информации, требующее значительных объемов цифровой памяти и соответствующего количества арифметических операций, из-за чего шифрование информации получило развитие только в последнее время.

Для решения проблем в сфере информационной безопасности какого-либо одного средства или технического приема не существует. Однако, общим в решении большинства из таких проблем считается применение криптографии и крипто-подобных преобразований в системе.

Таким образом, актуальной является тема данной магистерской диссертации, ориентированной на решение задачи криптоанализа шифров.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

**Цель исследований.** Сравнение и анализ наиболее распространенных алгоритмов шифрования для повышения эффективности выбора наиболее подходящего алгоритма.

**Задачи исследования**. Для достижения поставленной цели необходимо выполнить следующие задачи:

1. Изучение предметной области, связанной с криптоанализом.

2. Разработка модифицированного алгоритма RC 6 для шифрования данных;

3. Разработка методов автоматизированного анализа шифрования данных;

4. Определение оптимальных стратегий при шифровании данных в вычислительных системах.

**Объект исследования**. Набор алгоритмов шифрования и методов криптоанализа.

**Предмет исследования**. Методы и программные средства, позволяющие автоматизировать процессы сравнительной оценки шифра на основе криптоанализа.

**Структура и объем диссертации.** Диссертационная работа состоит из введения, трёх глав, заключения, списка использованных источников и приложений. Работа содержит 96 страниц основного текста, 46 рисунков, 29 таблиц и три приложения. Список использованных источников содержит 39 наименований.

**Методы исследования**. Анализ, сравнение, обобщение, классификация, компьютерное моделирование.

**Научная новизна:**

– предложен модифицированный алгоритм RC 6;

– определены оптимальные стратегии программирования при реализации алгоритмов шифрования.

**Практические результаты работы;**

– создана программа для анализа шифрования данных;

– показана возможность использования полученных научно-технический результатов для выбора алгоритма шифрования.

## КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

В главе 1 «Анализ предметной области и постановка задачи» были проанализированы возможные векторы атак злоумышленников по преступному доступу к информации в компьютерных системах. Были исследованы возможные средства обнаружения атак. В частности, такими средствами являются сигнатурный и статистический анализ.

Определена общая классификация алгоритмов шифрования, в частности их разделение на симметричные и асимметричные. Было дано определение симметричных и асимметричных алгоритмов шифрования и рассмотрены все возможные на момент написания работы варианты реализации этих

алгоритмов. Был детально проанализирован механизм работы симметричных алгоритмов, в том числе была проанализирована сеть Фейстеля и механизмы шифрования DES и AES.

В главе 2 «Анализ показателей, влияющих на эффективность шифрования» был проведен детальный анализ симметричных и асимметричных алгоритмов шифрования. В частности, были проанализированы симметричные алгоритмы шифрования: MARS, Serpent, TwoFish, а также асимметричные алгоритмы: RSA, Эль-Гамаля и др. На основе проведения анализа алгоритмов была представлена их сравнительная характеристика, и были выделены наиболее устойчивые к взлому алгоритмы шифрования.

Также были проанализированы основные методы защиты информации и безопасного доступа пользователей компьютерной сети к данным, которые базируются на основе предварительно исследованных алгоритмов шифрования.

В частности, были проанализированы методы аутентификации пользователей во взаимодействии с алгоритмами шифрования. Были исследованы типы аутентификации и возможные векторы атак на них.

Отдельное внимание было уделено электронно-цифровой подписи, как современному способу защиты электронных документов. Был проанализирован механизм электронно-цифровой подписи, в частности проанализированы цифровые подписи на основе симметричных и асимметричных алгоритмов шифрования. В конце раздела внимание было уделено методам хеширования паролей, как одного из наиболее распространенных способов засекречивания и хранения паролей. Была рассмотрена роль алгоритмов шифрования в хешировании паролей.

В заключительной главе 3 «Реализация криптоанализа применительно к заданному набору шифров» проанализирован механизм работы алгоритма RC6. На его основе был разработан модифицированный вариант алгоритма RC6. В основе изменений модифицированного алгоритма лежит добавление двух новых регистров: E и F. Благодаря модификации алгоритма удалось достичь значительно большего быстродействия алгоритма и большей криптостойкости.

В главе был пошагово рассмотрен вариант реализации модифицированного алгоритма, таким образом, чтобы было возможно на основе детального анализа разработать программную реализацию этой модификации.

Проанализировано на языке программирования Java программное обеспечение «Scrambler» для осуществления шифрования, дешифрования файлов на основе 6 наиболее популярных алгоритмов шифрования с открытым ключом (RSA, ElGamal, Pohlig-Hellman, Rabin, модифицированный RC 6 и Williams). Данный программный продукт также предназначен для демонстрации процессов шифрования/дешифрования и анализа вышеперечисленных алгоритмов по

следующим параметрам: время шифрования и дешифрования, время генерации ключей, размер зашифрованных файлов и вычислительная сложность алгоритмов. Это стало возможным на основе полученных данных после использования различных методов класса BigInteger.

Диссертация выполнена самостоятельно, проверена в системе «Антиплагиат». Процент оригинальности соответствует норме, установленной кафедрой. Цитирования обозначены ссылками на публикации, указанные в «Списке использованных источников».

## ЗАКЛЮЧЕНИЕ

В ходе исследования на основе анализа предметной области были выявлены существующие подходы к организации шифра, определена общая классификация алгоритмов шифрования, в частности их разделение на симметричные и ассиметричные. На основе проведения анализа алгоритмов была представлена их сравнительная характеристика, и были выделены наиболее устойчивые к взлому алгоритмы шифрования

Произведен анализ наиболее популярных алгоритмов шифрования и решены следующие задачи:

− изучение предметной области, связанной с криптоанализом;

− разработка модифицированного алгоритма RC6 для шифрования данных;

− разработка методов автоматизированного анализа шифрования данных;

− определение оптимальных стратегий при шифровании данных в вычислительных системах.

В результате выполнения магистерской диссертации разработан модифицированный алгоритм RC6. Благодаря модификации алгоритма удалось достичь значительно большего быстродействия алгоритма и большей криптостойкости. Также результатом работы является программный продукт «Scrambler», предназначенный для шифрования/дешифрования файлов на основе шести алгоритмов шифрования с открытым ключом и пригодный для анализа алгоритмов шифрования по параметрам.

## СПИСОК ПУБЛИКАЦИЙ АВТОРА

[1–А.] Емельяненко А. И. Электронно-цифровая подпись с помощью симметричных криптосистем // А. И. Емельяненко // Студенческий. СибАК. – 2021. – №21(149) – URL: https://sibac.info/journal/student/149/217366.