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

Анализ и сравнение блочных и поточных шифров

АВТОРЕФЕРАТ
дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Проданова Михаила Дмитриевича

Научный руководитель
доцент к. ф.-м. н. _____ А. В. Жаркова
21.01.2023 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
21.01.2023 г.

Саратов 2023

ВВЕДЕНИЕ

В современном мире в связи с распространением информационных технологий растет число потенциальных угроз информационной безопасности. Но также в наше время существует множество различных способов защиты информации путем шифрования. Одним из распространенных способов шифрования является симметричное шифрование, в частности блочные и поточные шифры. Принимая во внимание многообразие симметричных шифров, важной задачей становится выбор способа шифрования, а также анализ и сравнение параметров и уровня защиты алгоритмов шифрования.

Существует множество работ, анализирующих конкретные алгоритмы шифрования и сравнивающих некоторые из них. Однако работ, в которых проводится сравнение множества блочных и поточных шифров, не так много.

Целью данной работы является изучение различных блочных и поточных шифров, их достоинств и недостатков, а также последующее их сравнение и анализ. В том числе в данной работе будет разработана и реализована программа с использованием представителей блочных и поточных шифров. Данные шифры будут сравнены на практике. Для достижения поставленной цели требуется решить следующие задачи:

1) изучить принципы работы и особенности блочных шифров;

2) изучить принципы работы и особенности поточных шифров;

3) сравнить и проанализировать блочные и поточные шифры, выявить их преимущества и недостатки;

4) разработать и реализовать программный продукт, использующий блочные и поточные шифры, позволяющий проводить сравнение и анализ используемых шифров.

Материалы данной дипломной работы частично были представлены на IX Международной научной конференции «Компьютерные науки и

информационные технологии» памяти А. М. Богомолов и опубликованы в её материалах[1].

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 105 страниц, из них 53 страницы – основное содержание, включая 26 рисунков и 2 таблицы, список использованных источников из 27 наименований.

[1] Жаркова, А. В. О сравнении блочных и поточных шифров [Электронный ресурс] / А. В. Жаркова, М. Д. Проданов // Компьютерные науки и информационные технологии : Материалы Междунар. науч. конф. – Саратов : ООО Издательство «Научная книга», 2021. – С. 65–68.

КРАТКОЕ СОДЕРЖАНИЕ

В дипломной работе в разделе 1 «Необходимые определения» приводятся необходимые определения[2, 3, 4, 5, 6], которые используются в данной работе.

Алгоритм – это набор конечного числа правил, задающих последовательность выполнения операций для решения задач определенного типа[2].

Протокол – это набор соглашений и правил, который определяет обмен данными между различными программами[3].

Криптография (от греческого тайность) – это совокупность идей и методов, связанных с преобразованием информации с целью ее защиты от непредусмотренных пользователей.

Открытый текст – это информация, представленная в виде некоторого текста (сообщения).

Шифр – способ преобразования открытого текста в защищенную форму.

Шифрование – процесс применения шифра. *Криптограмма* (*шифртекст*) – полученный в результате шифрования измененный текст.

Дешифрование (*расшифрование*) – перевод криптограммы в исходный открытый текст.

Ключ – некоторая дополнительная информация, с помощью которой осуществляются взаимно обратные действия шифрования и расшифрования.

Симметричный шифр – это шифр, в котором для шифрования и расшифрования применяется один и тот же секретный ключ.

---

[2] Кнут, Д. Э. Искусство программирования. Том 1. Основные алгоритмы [Электронный ресурс] / Д. Э. Кнут. – Москва : Вильямс, 2001. – 682 с. – Загл. с экрана. – Яз. рус.

[3] Таненбаум, Э. Распределенные системы. Принципы и парадигмы [Электронный ресурс] / Э. Таненбаум, М. ван Стеен. – Санкт-Петербург : Питер, 2003. – 877 с. : ил. – Загл. с экрана. – Яз. рус.

[4] Салий, В. Н. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского [Электронный ресурс]. – Саратов, 2017. – 43 с. : ил., табл. – URL: http://elibrary.sgu.ru/uch_lit/622.pdf (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. рус.

[5] Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си [Электронный ресурс] / Б. Шнайер. – Москва : Издательство ТРИУМФ, 2002. – 610 с. – Загл. с экрана. – Яз. рус.

[6] Основы криптографии [Электронный ресурс] / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин. – 2-е изд., испр. и доп. – Москва : Гелиос АРВ, 2002. – 480 с. – Загл. с экрана. – Яз. рус.

Асимметричный шифр – это шифр, в котором процедуры шифрования и расшифрования осуществляются на разных ключах[4].

Раздел 2 работы «Блочные шифры» состоит из трех подразделов, первый из которых 2.1 «Принципы построения блочных шифров» посвящен описанию принципов построения алгоритмов блочного шифрования.

Блочные шифры работают с блоками открытого текста фиксированной длины. При шифровании блочными шифрами с одним и тем же ключом один и тот же блок открытого текста всегда преобразуется в один и тот же блок шифртекста.

Реализация блочных шифров основывается на многократном применении базовых преобразований к блокам открытого текста фиксированной длины. Данные преобразования должны удовлетворять двум основным требованиям:

1) преобразования должны быть просто реализуемыми, в том числе и программным способом;

2) при небольшом числе итераций базовых преобразований должны получаться аналитически сложные преобразования.

Существует два основных типа базовых преобразований:

1) перемешивающие – криптографически сложные локальные преобразования над отдельными частями входного блока;

2) рассеивающие – простые преобразования, использующиеся для перестановки частей входного блока между собой.

В подразделе 2.2 работы «Режимы работы блочных шифров» приводится определение режима работы блочных шифров, приводятся требования безопасности к режимам работы, а также подробно описываются основные пять режимов работы блочных шифров.

На режимы работы накладываются некоторые требования безопасности:

1) режим шифра не должен компрометировать безопасность используемого алгоритма;

2) должна быть скрыта структура открытого текста;

3) должен быть рандомизирован ввод шифра;

4) должно быть затруднено манипулирование открытым текстом посредством ввода ошибок в шифртекст;

5) должно быть возможно шифрование нескольких сообщений одним ключом;

6) по эффективности режим не должен быть сильно хуже используемого алгоритма шифрования;

7) режим должен быть устойчив к сбоям[5].

Согласно российскому стандарту ГОСТ Р 34.13–2015[7] существуют пять основных режимов работы:

1) режим простой замены (electronic codebook, ECB);

2) режим простой замены с зацеплением (cipher block chaining, CBC);

3) режим гаммирования с обратной связью по шифртексту (cipher-feedback, CFB);

4) режим выходной обратной связи (output-feedback, OFB);

5) режим гаммирования (counter, CTR).

В подразделе 2.3 работы «Примеры блочных шифров» приводятся примеры алгоритмов блочного шифрования и некоторые их характеристики. Далее подробно рассматривается алгоритм блочного шифрования AES.

Наиболее известными примерами блочных шифров являются американские стандарты: DES (Data Encryption Standard) и AES (Advanced Encryption Standard), а также российский стандарт ГОСТ Р 34.12–2015, содержащий шифры «Кузнечик» и «Магма». Также существуют и другие популярные блочные шифры, такие как Blowfish, который разрабатывался как альтернатива DES, XTEA, предназначенный для приложений, требующих высокую скорость работы, RC6, Serpant и другие[8].

---

[7] ГОСТ Р 34.13–2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» [Электронный ресурс]. – Москва. : Стандартинформ, 2015. – 30 с. – URL: https://tc26.ru/standard/gost/ GOST_R_3413-2015.pdf (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. рус.

[8] Arora, N. Block and Stream Cipher Based Cryptographic Algorithms: a Survey [Электронный ресурс] / N. Arora, Y. Gigras // Research India Publications [Электронный ресурс]. – 2014. – URL: https://www.ripublication.com/irph/ijict_spl/ijictv4n2spl_13.pdf (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. англ.

Раздел 3 работы «Поточные шифры» состоит из трех подразделов, первый из которых 3.1 «Принципы построения поточных шифров» посвящен описанию принципов построения алгоритмов поточного шифрования.

Поточные шифры преобразуют открытый текст в шифртекст не по блокам, а по одному биту (в программных реализациях – по одному байту).

В поточных шифрах используются генераторы потока ключей, которые создают последовательность бит k_1, k_2, k_3,…, k_i, к которым применяется операция XOR с битами открытого текста p_1, p_2, p_3,…, p_i, результатом которой являются биты шифртекста c_1, c_2, c_3,…, c_i.

Математически формулы шифрования и расшифрования записываются следующим образом:

$c_i = p_i \oplus k_i$ (9);

$p_i = c_i \oplus k_i$ (10)[5].

В подразделе 3.2 работы «Виды поточных шифров» подробно рассматриваются два вида поточных шифров – самосинхронизирующиеся поточные шифры и синхронные поточные шифры.

В самосинхронизирующихся поточных шифрах следующий бит потока ключей зависит от некоторого количества предыдущих бит шифртекста.

В синхронных поточных шифрах последовательность бит потока ключей не зависит от шифртекста. При шифровании и расшифровании должны использоваться генераторы потока ключей, создающие идентичные последовательности.

В подразделе 3.3 работы «Примеры поточных шифров» приводятся примеры алгоритмов поточного шифрования, а также подробно рассматривается алгоритм поточного шифрования RC4.

Одним из самых популярных поточных шифров является RC4. RC4 использует ключ переменной длины от 40 до 2048 бит. Он отличается высокой скоростью работы, а также достаточно высокой стойкостью при использовании

несвязанных случайных ключей. Он широко используется в современных протоколах, таких как SSL, TLS и многих других.

В разделе 4 работы «Сравнение блочных и поточных шифров» приводятся отличия блочных и поточных шифров, их основные достоинства и недостатки.

Основные плюсы блочных шифров:

1) простая программная реализация по сравнению с поточными шифрами;

2) большое количество режимов работы, позволяющих использовать блочные шифры в самых разных задачах;

3) широкое распространение.

К плюсам поточных шифров можно отнести следующие:

1) простая аппаратная реализация по сравнению с блочными шифрами;

2) высокая скорость работы;

3) требуют меньше ресурсов, чем блочные шифры[10].

Так же стоит отметить, что поточные шифры проще анализировать математически, нежели блочные. Из этого следует, что существует множество разнообразных методов взлома поточных шифров, например, линейный и дифференциальный анализ. При этом для поточных шифров проще определить четкие критерии их надежности.

Раздел 5 работы «Программная реализация» состоит из двух подразделов, первый из которых 5.1 «Работа программы» посвящен подробному описанию работы программного продукта, написанного на языке Java, реализующего многие из известных алгоритмов блочных и поточных шифров и выводящего таблицу, в которой сравниваются различные параметры работы данных алгоритмов. Также программный продукт позволяет генерировать отчет в формате .docx, содержащий сравнительную таблицу и обобщенный результат. Листинг программы приведен в приложении А.

[10] Салий, В. Н. Криптографические методы защиты информации : курс лекций / В. Н. Салий // Саратовский национальный исследовательский государственный университет имени Н. Г. Чернышевского. – Саратов, 2012.

В данной программе используется библиотека для языка программирования Java, предоставляющая набор криптографических компонентов – Bouncy Castle Crypto API. Данная библиотека также содержит реализации многих симметричных алгоритмов шифрования. Реализации библиотеки Bouncy Castle используются в данной программе. Для блочных шифров реализованы рассмотренные ранее режимы работы: ECB, CBC, CFB, OFB и CTR.

Помимо этого, для дополнительных экспериментов на языке Java были написаны собственные реализации алгоритмов шифрования AES и RC4. В реализованной программе данные реализации носят названия «My AES» и «My RC4», соответственно.

Основное окно программы содержит четыре обязательных поля ввода данных:

1) поле выбора алгоритма шифрования;

2) поле ввода пути к входному файлу;

3) поле ввода пути к выходному файлу;

4) поле ввода пути к файлу ключа шифрования.

Помимо этого, при выборе блочного шифра появляется поле выбора режима работы. А также, если алгоритму шифрования требуется вектор инициализации, появляется поле ввода пути к файлу вектора инициализации. Окно приложения представлено на рисунке 10.

Программа реализует окно выбора нужного файла, при этом программа обрабатывает ошибки, такие как отсутствие одного из файлов, пустоту файла ключа и прочие.

Программа реализует вкладку «Настройки», в которой можно настроить путь к папке по умолчанию для окна выбора файлов для шифрования и для сохранения отчетов, включить или отключить автоматическое дополнение ключа и вектора инициализации нулями при недостаточном размере. Также реализована вкладка «Вид», в которой можно отобразить таблицы результатов шифрования и расшифрования и сгенерировать отчет.

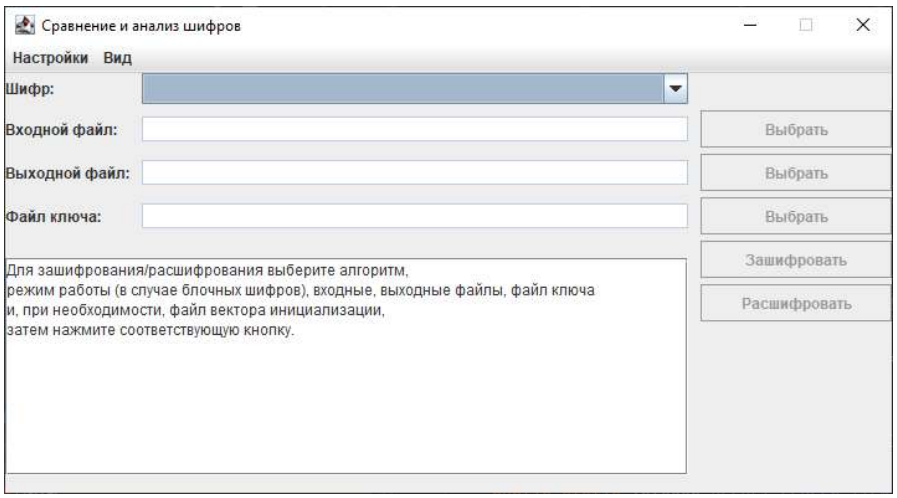

Рисунок 10 – Окно приложения

Все вычисления проводились на персональном компьютере с характеристиками: Windows 10 Pro x64; AMD Ryzen 5 3600 6-Core 3.59 GHz; 16 ГБ; Radeon RX 580 Series, 8 ГБ.

С помощью программного продукта была проведена оценка разницы собственных реализаций алгоритмов AES и RC4 с соответствующими реализациями библиотеки Bouncy Castle, оценка разницы в скорости работы блочных алгоритмов шифрования в разных режимах, а также оценка скорости шифрования и расшифрования всех рассматриваемых алгоритмов шифрования. Для получения результатов последней оценки был сгенерирован отчет в формате .docx. Фрагмент отчета представлен на рисунке 25.

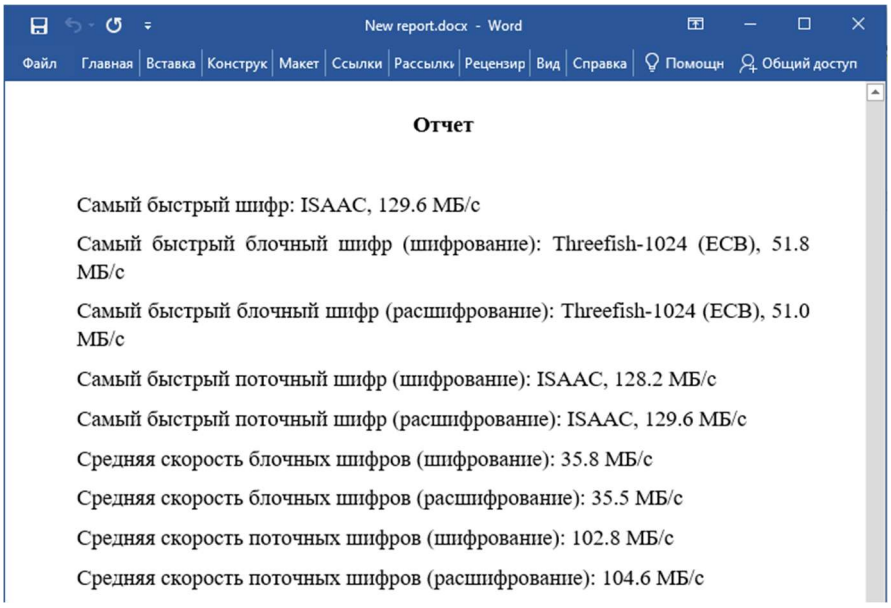

Рисунок 25 – Фрагмент отчета

В подразделе 5.2 работы «Анализ результатов» приводится анализ результатов, полученных в результате работы программного продукта. Также были подробно рассмотрены самые быстрые и медленные шифры: самый быстрый блочный шифр Threefish[19], самый медленный блочный шифр ГОСТ Р 34.12–2015 «Кузнечик»[21], самый быстрый поточный шифр ISAAC[23] и самый медленный поточный шифр Grain-v1[25].

В результате работы программы было получено, что в среднем скорость шифрования и расшифрования блочных алгоритмов составляет приблизительно 35 МБ/с. При этом скорость шифрования и расшифрования поточных алгоритмов в среднем составляет примерно 104 МБ/с.

Таким образом, сравнивая реализованные алгоритмы, можно сделать вывод, что, действительно, поточные шифры работают значительно быстрее блочных. В данном случае скорость работы поточных шифров превышает скорость работы блочных в среднем в 3 раза. При этом даже самый быстрый блочный шифр – Threefish (52 МБ/с) работает медленнее самого медленного поточного шифра – Grain-v1 (57 МБ/с).

В итоге имеем, что поточные шифры в целом работают гораздо производительнее блочных не только по времени, но и по остальным параметрам. Блочные шифры выигрывают в том, что они могут использоваться для различных ситуаций и задач, в том числе, например, в качестве основы для хэш-функций.

---

[19] The Skein Hash Function Family Version 1.3 [Электронный ресурс] / N. Ferguston, S. Lucks, B Schneier, D. Whiting, M. Bellare, T. Kohno, J. Callas, J. Walker // Schneier on Security [Электронный ресурс]. – 2010. – 100 с. – URL: https://www.schneier.com/wp-content/uploads/2015/01/skein.pdf (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. англ.

[21] ГОСТ Р 34.12–2015. Информационная технология. Криптографическая защита информации. Блочные шифры [Электронный ресурс] // Технический комитет по стандартизации «Криптографическая защита информации» [Электронный ресурс]. – Москва : Стандартинформ, 2015. – 30 с. – URL: https://tc26.ru/standard/gost/GOST_R_3412-2015.pdf (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. рус.

[23] Jenkins, J. R. ISAAC [Электронный ресурс] / J. R. Jenkins // Fast Software Encryption. FSE 1996. Lecture Notes in Computer Science, vol 1039. Springer [Электронный ресурс]. – Berlin, 1996. – 9 с. – URL: https://doi.org/10.1007/3-540-60865-6_41 (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. англ.

[25] Hell, M. Grain – A Stream Cipher for Constrained Environments [Электронный ресурс] / M. Hell, T. Johanson, W. Meier // Research Gate [Электронный ресурс]. – 2007. – 14 с. – URL: https://www.researchgate.net/publication/220141199_Grain_A_stream_cipher_for_constrained_environments (дата обращения: 28.11.2022). – Загл. с экрана. – Яз. англ.

ЗАКЛЮЧЕНИЕ

В данной работе было проведено ознакомление с научной литературой, изучены блочные и поточные шифры, а также разница между ними, разработано и реализовано приложение, реализующее алгоритмы блочных шифров в пяти основных режимах работы и алгоритмы поточных шифров. В реализованном приложении также выводится таблица сравнения различных параметров работы данных алгоритмов, на основе которой имеется возможность создания отчета в формате .docx.

При сравнении блочных и поточных шифров оказалось, что поточные шифры работают значительно эффективнее блочных, однако блочные шифры следует применять, когда скоростью шифрования можно пренебречь ради наибольшей надежности, а поточные – когда необходима высокая производительность и скорость работы.

Результаты, полученные в данной дипломной работе, могут быть применены при разработке блочных и поточных шифров, а также, если есть необходимость выбора между различными шифрами. Материалы данной дипломной работы частично были представлены на IX Международной научной конференции «Компьютерные науки и информационные технологии» памяти А. М. Богомолов и опубликованы в её материалах[1].

Таким образом, все поставленные задачи решены, цель работы достигнута.