Universitatea Tehnică a Moldovei

ANALIZA COMPARACTIVA A METODELOR CRIPTOGRAFICE DE PRELUCRARE A INFORMAȚIEI PENTRU TRANSMISIA PRIN DIFERITE CANALE DE COMUNICAȚII

Student: Ceavdari Vadim

Coordonator: Ciclicci Vladimir

conf. univ., dr.

Chişinău 2022

REZUMAT

Autorul: Ceavdari Vadim, gr. SCE-211M

Titlul tezei de master: Analiza comparativă a metodelor criptografice de prelucrare a informaţiei pentru transmisia prin diferite canale de comunicaţii

Structura lucrării: constă din pagini de titlu, aviz, rezumat, introducere, 3 capitoli, concluzii, bibliografie.

Cuvinte cheie: criptografie; cifru; cheie publică; cheie privată; algoritm simetric; algoritm asimetric.

Problematica studiului: Analiza imunității la viteză și la zgomot a sistemelor de transmisie a datelor în funcție de metodele de criptare și de tipul canalului de comunicație.

Scopul lucrării: Analiza comparativă a metodelor criptografice de prelucrare a informațiilor în timpul transmiterii pe diverse canale de comunicație pe baza studiului modelelor matematice ale sistemelor de transmisie a datelor cu criptare a datelor folosind metoda RSA și metoda formantului, care au cea mai bună imunitate la viteză și la zgomot.

Obiectivele:

1. Examinați metodele existente de criptare a datelor.
2. Luați în considerare algoritmul de criptare RSA.
3. Dezvoltarea în mediul Matlab a modelelor unui sistem de transmisie a informațiilor cu algoritmul de criptare RSA pentru o linie de comunicație prin cablu și pentru transmisia de date pe un canal radio.
4. Luați în considerare un algoritm pentru criptarea datelor folosind metoda formantului.
5. Dezvoltarea în mediul Matlab a modelelor unui sistem de transmisie a informațiilor cu un algoritm de criptare a datelor folosind o metodă formantului pentru o linie de comunicație prin cablu și pentru transmisia de date pe un canal radio.
6. Efectuați o analiză comparativă a modelelor dezvoltate.

Metode aplicate: Metodele de criptare studiate pentru sistemele de transmisie de date au fost analitic și modelate în mediul Matlab folosind biblioteca de blocuri Simulink.

Rezultatele obținute: Este demonstrat că sistemele de transmisie de date cu algoritmul de criptare formanților au cea mai bună performanță și imunitate la zgomot.

Se remarcă faptul că, în funcție de parametrii canalului de transmisie, de exemplu, cu o lățime de bandă mare a canalului de comunicație, este mai bine să utilizați metoda de criptare a datelor formante sau algoritmul de criptare RSA în combinație cu alte metode de criptare (de exemplu, metode de criptare simetrică).

SUMMARY

Author: Ceavdari Vadim, gr. SCE-211M

Title: Comparative analysis of cryptographic methods of information processing for transmission over diferent communication channels

Thesis structure: consists of title pages, Review, Summary, Introduction, Conclusions, Bibliography.

Key words: cryptography; cipher; public key; private key; symmetric algorithm; asymmetric algorithm.

Research problem: Analysis of the speed and noise immunity of data transmission systems depending on encryption methods and the type of communication channel.

Thesis purpose: Noise Comparative analysis of cryptographic methods of information processing during transmission in various communication channels based on the study of mathematical models of data transmission systems with data encryption using the RSA method and the formant method, which have the best speed and noise immunity.

Objectives:

1. Examine existing data encryption methods.
2. Studying of Consider the RSA encryption algorithm.
3. To develop in the Matlab environment models of an information transmission system with the RSA encryption algorithm for a cable communication line and for data transmission over a radio channel.
4. Consider an algorithm for encrypting data using the formant method.
5. Modeling To develop in the Matlab environment models of an information transmission system with a data encryption algorithm using a formant method for a cable communication line and for data transmission over a radio channel.
6. Perform a comparative analysis of the developed models.

Applied methods: The studied encryption methods for data transmission systems were investigated analytically and modeled in the Matlab environment using the Simulink block library.

The obtained results: It is shown that data transmission systems with the formant encryption algorithm have the best performance and noise immunity.

It is noted that depending on the parameters of the transmission channel, for example, with a large bandwidth of the communication channel, it is better to use the formant data encryption method or the RSA encryption algorithm in combination with other encryption methods (for example, symmetric encryption methods).

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном обществе успех любого вида деятельности сильно зависит от обладания определенными сведениями (информацией) и от отсутствия их (её) у конкурентов. Чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере и тем больше потребность в защите информации. Одним словом, возникновение индустрии обработки информации привело к возникновению индустрии средств её защиты и к актуализации самой проблемы защиты информации, проблемы информационной безопасности. Одна из наиболее важных задач (всего общества) – задача кодирования сообщений и шифрования информации. Что общего и что различает эти процессы и процедуры?

Вопросами защиты информации занимается наука криптология (*криптос*– тайный, *логос*– наука). Криптография является одной из трех составных частей криптологии – науки о передаче информации в виде, защищенном от несанкционированного доступа. Криптография, как было сказано, занимается шифрованием и дешифрованием сообщений с помощью секретных ключей. Другая часть криптологии – криптоанализ – представляет собой теорию и практику извлечения информации из криптограммы без использования ключа. Основной принцип криптоанализа сформулировал один из его основоположников бельгийский криптолог Огюст Керкхофс (1835-1903) в 1883 году в книге «Военная криптография»: «При оценке надежности шифра следует допустить, что противнику известно о нем все, кроме ключа». Третья часть криптологии – аутентификация – объединяет в себе совокупность приемов, позволяющих проверять подлинность источника информации и полученных сообщений.

В результате использования обществом автоматизированных систем, образовалось немалое количество проблем, как у пользователей, так и у разработчиков. Основной из них является проблема информационной безопасности. Ее влияние велико, поэтому оставлять ее в бесконтрольном состоянии нельзя. Она требует постоянного сосредоточения, решения проблем и поиска новых путей совершенствования существующих методов. Особенно ввиду того, что практически вся современная информация может легко преобразоваться в машиночитаемую форму. А это значит, ее можно легко исказить, скопировать, либо уничтожить. Что, весьма, нежелательно. В совокупности с этим, развитие информационных технологий, присущее нашей современности, способствует распространению негативных явлений, таких как несанкционированный доступ к секретной информации, промышленный шпионаж. [6, 23] Подобные действия представляют собой серьезную опасность для современных организаций. Поэтому вопросы защиты информации, на сегодняшний день, имеют большую актуальность. Термин "криптография" происходит от двух греческих слов:

криптос и графейн – писать. Таким образом, это тайнопись, т.е. система изменения исходного сообщения с целью сделать его непонятным для непосвященных лиц и дисциплина, изучающая общие свойства и принципы систем тайнописи.

Основные цели криптографии:

- Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к данным). Это одна из основных задач криптографии, для ее решения применяется шифрование данных, т.е. такое их преобразование, при котором прочитать их могут только законные пользователи, обладающие соответствующим ключом.
- Обеспечение целостности данных — гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Под модификацией понимается вставка, удаление или подмена информации, а также повторная пересылка перехваченного ранее текста.
- Обеспечение аутентификации. Под аутентификацией понимается проверка подлинности субъектов (сторон при обмене данными, автора документов, и т.д.) или подлинности самой информации. Частным случаем аутентификации является идентификация — процедура доказательства субъектом того, что он действительно является именно тем, за кого себя выдает. Во многих случаях субъект X должен не просто доказать свои права, но сделать это так, чтобы проверяющий субъект (Y) не смог впоследствии сам использовать полученную информацию для того, чтобы выдать себя за X. Подобные доказательства называются «доказательствами с нулевым разглашением».
- Обеспечение невозможности отказа от авторства — предотвращение возможности отказа субъектов от совершенных ими действий (обычно — невозможности отказа от подписи под документом). Эта задача неотделима от двойственной — обеспечение невозможности приписывания авторства. Наиболее яркий пример ситуации, в которой стоит такая задача — подписание договора двумя или большим количеством лиц, не доверяющих друг другу. В такой ситуации все подписывающие стороны должны быть уверены в том, что в будущем, во-первых, ни один из подписавших не сможет отказаться от своей подписи и, во-вторых, никто не сможет модифицировать, подменить или создать новый документ (договор) и утверждать, что именно этот документ был подписан.

Введём некоторые понятия кодирования и декодирования информации.

Чем шифрование отличается от кодирования? Слова «кодирование» и «шифрование» часто используются как синонимы. Однако в современной прикладной математике (к которой можно отнести и криптографию) эти термины разделяются. Под шифрованием понимается такое преобразование текста (сообщения), в результате которого прочитать преобразованный текст может только тот, кто обладает специальным ключом. Кодированием называется любое преобразование данных из одной формы представления в другую. Таким образом, кроме шифрования, термин «кодирование» включает в себя также так называемое «помехоустойчивое кодирование» (преобразование текста, позволяющее восстанавливать его в случае сбоя при передаче или хранении), сжатие данных и т.п. В широком смысле, кодированием можно назвать также сканирование текста или изображения (информация преобразуется из визуального представления в цифровое), и даже ввод текстов с клавиатуры.

Кодирование – процедура преднамеренного замещения (подстановки и т.п.) символов, знаков, изображений и т.д. одного множества, элементами другого множества. Основным «действующим лицом» здесь является код! Код – это правило соответствия совокупности знаков одного множества X знакам другого множества Y. Если каждому символу X при кодировании соответствует отдельный знак Y, то это кодирование. Если для каждого символа из Y однозначно отыщется по некоторому правилу его прообраз в X, то это правило называется декодированием. Кодирование – процесс преобразования букв (слов) алфавита X в буквы (слова) алфавита Y. При представлении информации в ЭВМ, символы кодируются байтами двоичных чисел. Байты в свою очередь состоят из 8 битов. При этом используются следующие способы.

1. ***Переход от естественных обозначений к более компактным.*** Этот способ подготовки данных для кодирования применяется для сжатия записи дат, номеров изделий, уличных адресов и т.д. Идея способа показана на примере сжатия записи даты. Обычно мы записываем дату в виде 10. 05. 01., что требует 6 байтов памяти ЭВМ. Однако ясно, что для представления дня достаточно 5 битов, месяца- 4, года - не более 7, т.е. вся дата может быть записана в 16 битах или в 2-х байтах.

2. ***Подавление повторяющихся символов.*** В различных текстах часто встречаются цепочки повторяющихся символов, пробелы или нули в числовых полях. Если имеется группа повторяющихся символов длиной более 3, то ее длину можно сократить до трех символов. Сжатая таким образом группа повторяющихся символов представляет собой триграф S P N, в котором S – символ повторения; P – признак повторения; N - количество символов повторения, закодированных в триграфе. В других схемах подавления повторяющихся символов используют особенность кодов ДКОИ, КОИ-7, КОИ-8,

заключающуюся в том, что большинство допустимых в них битовых комбинаций не используется для представления символьных данных.

3. ***Кодирование часто используемых элементов данных.*** Этот способ уплотнения данных также основан на употреблении неиспользуемых комбинаций кода ДКОИ. Для кодирования, например, имен людей можно использовать комбинации из двух байтов дикраф P N, где P – признак кодирования имени, N – номер имени. Таким образом может быть закодировано 256 имен людей, чего обычно бывает достаточно в информационных системах.

Определим ряд основных терминов, используемых в криптографии.

В соответствии с общепринятым под **шифром** понимают совокупность обратимых

преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом криптографического преобразования.

Ключ - это конкретное (секретное или открытое) состояние некоторых параметров алгоритма криптографического преобразования данных, которое обеспечивает выбор только одного варианта из всех возможных для данного алгоритма.

Основной характеристикой шифра является **криптостойкость**, которая определяет его стойкость к раскрытию методами криптоанализа. Обычно эта характеристика определяется интервалом времени, необходимым для раскрытия шифра.

Гаммирование - процесс наложения по определенному закону гаммы шифра на открытые данные.

Под **гаммой** шифра понимается псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму, для шифрования открытых данных и расшифровывания зашифрованных данных.

Имиттозащита – это защита системы шифрованной связи от навязывания ложных данных.

Имитовставка – это блок из *m* бит, который вырабатывается по определенному правилу из открытых данных с использованием ключа и затем добавляется к зашифрованным данным для обеспечения их имитозащиты.

К шифрам, используемым для криптографической защиты информации, предъявляется ряд требований:

- достаточная криптостойкость (надежность закрытия данных);
- простота процедур шифрования и расшифрования;
- незначительная избыточность информации за счет шифрования;
- нечувствительность к небольшим ошибкам шифрования и др.

ЗАКЛЮЧЕНИЕ

В данной мастеранской работе выполнялся сравнительный анализ криптографических алгоритмов обработки информации в линии передачи в среде Matlab. В результате проделанной работы можно сделать следующие выводы:

1. Одни шифры (перестановочные, шифры замены) обладают недостаточной криптостойкостью. Другие – поточные (шифр Виженера, шифр Вернама) обладают высокой криптостойкостью, но мало пригодны для повседневной практики.
2. Для коротких сообщений шифр RSA почти идеален, но при передаче информации большого объема он сильно уступает по скорости симметричным алгоритмам шифрования.
3. Разработанная в среде Matlab математическая модель системы с алгоритмом шифрования RSA показала, что данный алгоритм шифрования обладает хорошей криптостойкостью, но требует определенных процедур (помехоустойчивого кодирования) при наличии помех в канале передачи.
4. Формантный метод обладает лучшими качествами по быстродействию так как оперирует при шифровании с небольшими по величине простыми числами: основанием, ядром и остатком формант.
5. Разработанная в среде Matlab математическая модель системы с алгоритмом шифрования на основе формантного метода показала, что данный алгоритм шифрования обладает хорошей криптостойкостью, хорошим быстродействием и помехоустойчивостью.
6. Все математические модели систем передачи данных с обоими алгоритмами шифрования дали примерно одинаковые результаты как при передаче данных по кабельным каналам связи, так и по радиоканалу. Это говорит о правильных выбранных параметрах всех блоков разработанных математических моделей систем передачи данных.

В зависимости от параметров канала передачи, например, при большой пропускной способности канала связи лучше использовать формантный метод шифрования данных или алгоритм шифрования RSA в сочетании с другими методами шифрования (например, симметричными методами шифрования).

БИБЛИОГРАФИЯ

1. Рябко Б. Я., Фионов А. Н Криптографические методы защиты информации: учебное пособие. — М.: Горячая линия. — Телеком, 2005 — 229 с. ISBN: 5-89176-233-1
2. Введение в криптографию / Под общ. ред. В. В. Ященко. — 4-е изд., доп. М.: МЦНМО, 2012 — 348 с. ISBN: 978-5-4439-0026-1
3. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. университета, 2006 – 140 с. – 100 экз. – ISBN: 5-8265-0503-6.
4. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Ţurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.
5. А. Балабанов, А. Агафонов. Сопоставительный анализ и его приложения. Современные и классические задачи теории чисел и криптографии. Lap Lambert Academic Publishing, 2016, ISBN: 978-3-659-92621-1.
6. Петров А. А. Компьютерная безопасность. Криптографические методы защиты. – М.: ДМК Пресс, 2008 – 448 с. ISBN: 5-89818-064-8.
7. Глухов М. М. Круглов И. А., Пичкур А. Б., Черемушкин А. В. Введение в теоретико-числовые методы криптографии. – СПб.:"Лань", 2011 - 400 стр.ISBN: 978-5-8114-1116-0.
8. Романьков В.А. Введение в криптографию. Курс лекций / В.А. Романьков. М.: ФОРУМ, 2012 - 240 с., ISBN: 978-5-91134-573-0.
9. Криптографическая защита информации: учебное пособие / А.В.Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006 – 140 с. – ISBN: 5-8265-0503-6.
10. Гультяева Т.А. Основы теории информации и криптографии. – Новосибирск: Изд-во НГТУ, 2010 – 88 с. – ISBN: 978-5-7782-1425-5.
11. Бабенко Л.К., Ищукова Е.А. Криптографическая защита информации: симметричное шифрование: учебное пособие. - Таганрог: Изд-во ЮФУ, 2015 - 219 с. УДК 004.056.55(075.8).
12. Салий В.Н. Криптографические методы и средства защиты информации: учебное пособие. – Саратов – 43с. - ISBN: 978-5-7788-1125-1.
13. Бескид П.П., Тагарникова Т.М. Криптографические методы защиты информации. Ч.1. Основы криптографии. Учебное пособие – СПб., Изд-во РГГМУ, 2010 – 95 с. УДК 621.391.037.372.

14. Калмыков И.А. К 24 Криптографические методы защиты информации: Учебное пособие (лабораторный практикум). - Ставрополь: СКФУ, 2012. - 91 с. УДК 34.028 (075) ББК 67.404.3.
15. Ludmila Peca, Dinu Ţurcanu. Computer networks: Practical examples solved to be introduced in computer networks. ISBN 978-9975-45-812-2. Chișinău, Publisher „Tehnica-UTM”, 2022.
16. POPA, Cristina. Tehnici de modelare şi simulare: Aplicații MATLAB / Cristina Popa, Bogdan Doicin. - Ploieşti: Editura Universitatii PetrolGaze din Ploieşti, 2018. - 161 p; fig., tab. - Bibliogr.: p. 161. ISBN: 978-973-719-729-0.