ВШЭ БЭАД223

Танирберегнова Аружан

Обзор литературы по теме "Криптография в информационной безопасности"

Содержание

1 Вступление

1.1 Что такое криптография и какова ее роль в информационной безопасности

В наши дни криптография играет важную роль в обеспечении информационной безопасности, так как она позволяет защитить данные от несанкционированного доступа, изменения и уничтожения. Основная цель криптографии - обеспечить конфиденциальность, целостность и аутентичность информации.

Основные принципы криптографии включают в себя использование математических алгоритмов для шифрования данных, создание ключей доступа к зашифрованным данным, а также аутентификацию пользователей. Криптографические методы включают в себя симметричное и асимметричное шифрование, хэширование, электронную подпись и другие техники.

Однако с развитием технологий и появлением новых угроз, криптография также сталкивается с вызовами. Например, увеличение вычислительной мощности компьютеров делает классические методы шифрования уязвимыми к взлому. Также существует угроза квантовых компьютеров, которые могут взламывать современные криптографические алгоритмы.

Для борьбы с этими угрозами проводятся исследования и разработки новых методов криптографии, таких как квантовая криптография, многофакторная аутентификация, использование блокчейн-технологий и другие инновационные подходы.

Криптография, как наука об защите информации, становится все более важной в контексте растущих угроз кибербезопасности. В данной работе будет проанализированы статьи о ее значении в обеспечении информационной безопасности, ее основные принципы и методы, а также возможные угрозы и вызовы, с которыми она сталкивается в современном мире. Работа также будет посвящена изучению последних тенденций и разработок в области криптографии, направленных на повышение уровня защиты информации.

В данном обзоре литературы будут рассматриваться более подробно роль криптографии, а также последние тенденций и разработоки в области криптографии, направленные на повышение уровня защиты информации.

2 Обзор литературы

2.1 Analysis of Cryptography Encryption for Network Security.[1]

Авторы данной статьи рассказывают долгую и разнообразную историю криптографии. Подробнее описаны ее методы - шифры и коды. Описана важность атак, механизмов и услуг безопасности для оценки и преодоления угроз безопасности. Эта статья выделяет ключевые концепции, такие как симметричное и асимметричное шифрование, а также подчеркивает важность использования криптографических систем для защиты конфиденциальной информации и обеспечения безопасности передачи данных между сетями. В заключении этой статьи говорится о том что шифрование играет ключевую роль в обеспечении безопасности передачи данных между сетями, защищая информацию от несанкционированного доступа и обеспечивая безопасную передачу ключей между отправителем и получателем. Использование криптографии, водяных знаков, цифровых подписей и других методов значительно увеличивает безопасность коммуникаций и подчеркивает важность криптографических систем для защиты конфиденциальной информации.

Можно сделать вывод, что данная статья играет важную роль в исследовании информационной безопасности, поскольку она помогает понять и оценить методы защиты информации, подчеркивает значение шифрования для обеспечения безопасности передачи данных и важность соблюдения криптографических стандартов для защиты конфиденциальной информации в сети.

2.2 Importance of Cryptography in Network Security.[2]

Эта статья предоставляет обширный обзор сетевой безопасности и криптографии, в частности, цифровых подписей. В ней отмечается что безопасность и криптография - это слишком обширная тема, чтобы охватить все аспекты защиты информации в цифровой форме и предоставления служб безопасности. Однако, в работе предоставлен общий обзор сетевой безопасности и криптографии, а также обсуждаются различные алгоритмы. Затем представлен детальный обзор сетевой безопасности и криптографии в цифровых подписях. Целью цифровой подписи является обеспечение средства для сущности привязать свою идентичность к определенной информации. Далее рассмот-

рены типичные атаки на цифровые подписи. Первый метод - схема цифровой подписи RSA, которая до сих пор остается одним из наиболее практичных и универсальных методов. Схемы цифровой подписи Fiat-Shamir, DSA и смежные схемы также были рассмотрены. Цифровые подписи имеют множество применений в области информационной безопасности, включая аутентификацию, целостность данных и невозможность отказа от подписи. Эта статья кратко описывает, как работает криптография. И что читатели должны быть осторожны, поскольку существует множество способов атаки каждой из этих систем; криптоанализ и атаки на криптосистемы, однако, выходят за пределы этой статьи.

2.3 Analysis of Cryptographic Algorithms for Network Security.[3]

Здесь авторы рассматривают шифрование и его ключевую роль в обеспечении безопасности данных. Как оно используется для обеспечения конфиденциальности содержания сообщения при передаче и защиты от изменения. Сетевая безопасность является ключевым компонентом информационной безопасности, так как она относится ко всем аппаратным и программным функциям, характеристикам, операционным процедурам, учету, контролю доступа, административной и управленческой политике. Шифрование занимает центральное место в проблемах безопасности IT, так как оно лежит в основе конфиденциальности, конфиденциальности и идентичности, которые вместе обеспечивают основу для доверенной электронной коммерции и безопасной связи. Существует широкий спектр криптографических алгоритмов, которые используются для обеспечения безопасности сетей, и в настоящее время ведутся постоянные исследования новых криптографических алгоритмов для разработки более продвинутых техник безопасной связи. Эта статья играет важную роль в исследовании криптографии, так как она предоставляет обзор ключевых аспектов шифрования и его значимости для обеспечения безопасности данных. Она описывает широкий спектр криптографических алгоритмов, используемых для обеспечения безопасности сетей, и подчеркивает важность постоянных исследований новых криптографических методов для разработки более продвинутых техник безопасной связи. Эта статья также выделяет роль сетевой безопасности как ключевого компонента информационной безопасности и обозначает, что шифрование занимает центральное

место в проблемах безопасности информационных технологий. Все это делает данную статью важным вкладом в исследование криптографии, так как она обобщает актуальные аспекты и направления развития этой области.

2.4 Cryptography and Security in Internet of Things (IoTs): Models, Schemes, and Implementations.[4]

В этой статье описывается как интернет вещей (IoT) привлек внимание исследовательского сообщества в последние годы. Это одна из самых актуальных тем для текущих и будущих исследований, вовлекая как академическую, так и промышленную сферы. Проблемы безопасности и конфиденциальности для IoT являются приоритетными задачами. Эта статья объединяет модели, схемы и аспекты реализации альтернативных технологий и устройств IoT. Она фокусируется на знании эффективности реализации, в основном в аппаратных аспектах, конфиденциальности коммуникаций, аутентификации пользователей, целостности данных и доступности услуг. Рассматриваются атаки и современные угрозы, а также контрмеры против них. Представлены различные инфраструктуры IoT и альтернативные модели доверия. Обсуждаются также вопросы политики. Кроме того, IoT охватывает аспекты связанные с облачными вычислениями, аналитикой данных, машинным обучением и другими технологиями, что делает его одной из ключевых областей развития информационных технологий.

2.5 A Review of Information Security using Cryptography Technique.[5]

В данной статье описывается как защита данных стала крайне важным аспектом в наше время во всех сферах. Какие для этого были разработаны различные методы и алгоритмы. Они обеспечивают доступность, конфиденциальность и целостность данных. Все больше компаний хранят информацию о своем бизнесе и частных лицах на компьютерах. Большая часть хранящейся информации является высоко конфиденциальной и не предназначена для публичного просмотра. В этой статье я рассмотрены алгоритмы криптографии, основанные на концепции блочного шифра. Для написания этой

статьи я изучил информационную безопасность с использованием техники криптографии. После подробного изучения сетевой безопасности с использованием криптографии, эта статья делится на три раздела. Представляют только базовое введение в информационную безопасность с использованием криптографии, а также подробное описание алгоритмов криптографии, таких как симметричные алгоритмы ключа, такие как DES, AES, блокфиш и асимметричные алгоритмы ключа, такие как RSA, алгоритм обмена ключами Диффи-Хеллмана.

2.6 Role of Cryptography in Network Security.[6]

Сетевые администраторы используют несколько механизмов безопасности для защиты данных в сети от несанкционированного доступа и различных угроз. Эти механизмы безопасности повышают удобство использования и целостность сети. Аспекты проектирования механизмов безопасности сети включают как аппаратные, так и программные технологии. Области применения механизмов безопасности охватывают как общедоступные, так и частные компьютерные сети, используемые в повседневной работе для проведения транзакций и общения между деловыми партнерами, государственными учреждениями, предприятиями и частными лицами. Схемы безопасности сети различаются в зависимости от типов сети: публичной или частной, проводной или беспроводной. К защите данных во всех приложениях и платформах относится информационная безопасность, включающая шифрование, токенизацию и практики управления ключами. Антивирусное и анти-вредоносное программное обеспечение также являются частью сетевой безопасности для защиты от вредоносных программ, таких как шпионское ПО, вымогательство, трояны, черви и вирусы. Криптография является автоматизированным математическим инструментом, который играет важную роль в сетевой безопасности. Она обеспечивает конфиденциальность и целостность данных, а также обеспечивает аутентификацию и невозможность отказа пользователей. Статья фокусируется в первую очередь фокусируется на техниках криптографии и их роли в обеспечении безопасности сети. Техника криптографии состоит из алгоритмов шифрования и расшифрования. Алгоритмы шифрования выполняют перестановку обычного текста и генерацию непонятного формата для стороннего лица, известного как шифротекст. Исходные данные

расшифровываются посылателем с использованием алгоритмов расшифрования. Криптографические техники широко классифицируются на три категории: симметричная криптография, асимметричная криптография и аутентификация. Принятые широко криптографические алгоритмы описаны вместе со своими преимуществами и недостатками. Более того, в данной статье тщательно обсуждаются недавно разработанные эффективные криптографические алгоритмы, специфические для областей облачных вычислений, беспроводных сенсорных сетей и сетей на кристалле (on-chip), что дает ясное представление о возможности обеспечения безопасной коммуникации в сети с использованием криптографии.

Эта статья имеет существенное влияние на развитие криптографии, предоставляя полный обзор и последних достижений в этой области. Она подчеркивает необходимость разработки эффективных криптографических методов для защиты современных компьютерных сетей от постоянно развивающихся угроз. Кроме того, статья рассматривает специфические сценарии применения криптографии в облачных вычислениях, беспроводных сенсорных сетях и on-chip сетях, что является важным в контексте современных технологических тенденций и требований безопасности.

2.7 A review on network security and cryptography.[7]

В статье предоставляется обзор сетевой безопасности и различных техник, с помощью которых можно улучшить сетевую безопасность, то есть криптографию. Эта статья играет важную роль в исследовании важности криптографии, так как она предоставляет обзор сетевой безопасности и различных техник, которые могут улучшить безопасность передачи данных через интернет. Она также подчеркивает необходимость защиты компьютерной и сетевой безопасности в цифровую информационную эпоху, где кибератаки становятся все более распространенными. Такая статья помогает подчеркнуть важность криптографии в обеспечении безопасности передачи данных и защите от киберугроз.

2.8 Securing Network-on-Chip Using Incremental Cryptography.[8

Эта статья играет важную роль в изучении роли криптографии, так как она предлагает новую легкую схему шифрования для обеспечения безопасности сетевой коммуникации в системах на кристалле (SoC). В статье представлен подход, который улучшает производительность шифрования без ущерба для безопасности, используя инкрементальную криптографию, которая учитывает уникальные характеристики трафика в сети на кристалле. Экспериментальные результаты показывают, что предложенный подход значительно (до 57%, в среднем на 30%) сокращает время шифрования по сравнению с традиционными подходами при незначительном (менее 2%) влиянии на затраты ресурсов. Таким образом, данная статья помогает подчеркнуть важность развития криптографических методов для обеспечения безопасности передачи данных в сетевой коммуникации на кристалле. Сеть на кристалле (NoC) стала стандартной коммуникационной тканью для компонентов на кристалле в современных конструкциях систем на кристалле (SoC). Поскольку NoC имеет видимость всех коммуникаций в SoC, она стала одной из основных целей для атак на безопасность. Хотя шифрование пакетов может обеспечить безопасную связь, оно может привести к неприемлемым энергетическим и производительностным издержкам из-за ограниченных ресурсов конструкций SoC. В этой статье мы предлагаем легкую схему шифрования, реализованную на интерфейсе сети. Наш подход улучшает производительность шифрования без ущерба для безопасности, используя инкрементальную криптографию, которая использует уникальные характеристики трафика NoC. Экспериментальные результаты демонстрируют, что наш предложенный подход значительно (до 57%, в среднем на 30%) сокращает время шифрования по сравнению с традиционными подходами при незначительном (менее 2%) влиянии на издержки площади.

2.9 A review on lightweight cryptography algorithms for data security and authentication in IoTs.[9]

Роль криптографии в этой статье высоко оценивается, так как она предлагает обзор различных приложений и архитектур интернета вещей (IoTs) и выделяет проблемы безопасности информации и атаки, которые могут воз-

никнуть в связи с этим. Далее, в статье рассматриваются меры безопасности по защите данных и аутентификации, в результате чего используется криптография в качестве решения. Также проводится сравнительный анализ различных легких алгоритмов шифрования и аутентификации, который показывает их хорошую производительность по сравнению с традиционными криптографическими алгоритмами. Таким образом, данная статья помогает подчеркнуть важность развития легких криптографических методов для обеспечения безопасности в области интернета вещей.

2.10 A Review on Cryptography, Attacks and Cyber Security.[10]

Роль этой статьи в исследованиях криптографии, высока, так как она предоставляет обзор различных методов шифрования и их использование в сетевой безопасности. Она также помогает исследователям понять цели криптографии и различные алгоритмы, которые могут быть использованы для защиты информации. Также рассмотриваются типы атак, используемых для вторжения, и технологии кибербезопасности. Таким образом, эта статья оказывает влияние на развитие исследований в области криптографии и кибербезопасности.

2.11 Network Security and Cryptography.[11]

Суть данной статьи состоит в том, чтобы представить читателям ключевые принципы и техники криптографии и сетевой безопасности в компьютерных сетях. Она также ознакомляет читателей с основными концепциями, такими как классические шифровальные схемы, криптография с открытым ключом, схемы аутентификации, прекрасная конфиденциальность и интернет-безопасность. Кроме того, статья также предоставляет информацию о последних материалах и технологиях, связанных с интернетом вещей, облачными вычислениями, SCADA, блокчейном, умной сетью, аналитикой больших данных и другими современными тенденциями. Таким образом, статья играет важную роль в информировании читателей о последних тенденциях и технологиях в области криптографии и сетевой безопасности.

2.12 Cryptography: A Comparative Analysis for Modern Techniques.[12]

В статье рассказывается о важной роли шифрования в обеспечении безопасной связи между несколькими сторонами. Во многих современных исследованиях ученые вносят свой вклад в определение лучших методов шифрования с точки зрения их производительности. Выбор криптографической техники для конкретного контекста - большой вопрос; многие существующие исследования утверждают, что выбор техники зависит исключительно от желаемых качественных характеристик, таких как эффективность и безопасность. авторы статьи выяснили что существующие обзоры сосредоточены либо только на симметричных, либо асимметричных типах шифрования. Кроме того, обнаружено, что критерии сравнения производительности охватывают только общие параметры. В этой статье они также оценили производительность различных симметричных и асимметричных алгоритмов, охватывая множество параметров, таких как время шифрования/дешифрования, время генерации ключа и размер файла. В рамках оценки мы провели симуляции в примерном контексте, в котором были сравнены несколько криптографических алгоритмов. Результаты симуляции визуализированы таким образом, что ясно показывают, какой алгоритм наиболее подходит для достижения конкретной качественной характеристики. Имея такие исследования, значимые для развития криптографических методов, мы можем обеспечить более эффективную и безопасную защиту информации в различных областях, включая финансы, здравоохранение и коммуникации в целом. Такие исследования помогают определить оптимальные криптографические методы для различных применений, что важно для обеспечения безопасности в современном мире информационных технологий.

2.13 Summary по всем статьям

Таким образом, на основе анализа приведенных статьей можно сказать, что криптография играет критическую роль в обеспечении безопасности информации. Методы шифрования и дешифрования необходимы для защиты конфиденциальности данных, обеспечения целостности информации и аутентификации пользователей. С развитием технологий и вычислительной мощ-

ности появляются новые вызовы для криптографии. Например, квантовые компьютеры могут представлять угрозу для существующих криптографических методов, что требует разработки квантово-устойчивых шифров. Также во многих статьях упоминается необходимость постоянного обновления криптографических алгоритмов и протоколов. Уязвимости, обнаруженные в существующих методах, требуют постоянного анализа и улучшения стандартов шифрования. Авторы статей также подчеркивают важность обучения и осведомленности пользователей. Технические инновации могут быть бесполезны, если пользователи не следуют советам по безопасности и не используют средства шифрования правильным образом.

3 Вывод и ссылки на источники

В заключение стоит сказать, что криптография играет важную роль в защите конфиденциальности данных и обеспечении безопасности информационных систем. Криптографические методы и алгоритмы используются для защиты информации от несанкционированного доступа, подделки и изменения.

Также можно отметить, что с развитием технологий криптография стала все более сложной и требует усовершенствования и разработки новых методов защиты. Научные исследования в этой области позволяют улучшать алгоритмы шифрования, создавать более надежные системы безопасности и исследовать уязвимости текущих криптографических методов.

Таким образом, криптография остается актуальной и важной областью в информационной безопасности, и ее развитие и усовершенствование продолжаются благодаря научным исследованиям.

Список литературы

[1] V. E. Jyothi, D. B. Prasad, and D. R. K. Mojjada, “Analysis of cryptography encryption for network security,” https://iopscience.iop.org/article/10.1088/1757-899X/981/2/022028/meta, 2020.

[2] T. R. Devi, “Importance of cryptography in network security,” https://ieeexplore.ieee.org/abstract/document/6524439, 2013.

[3] K. Acharya, M. Sajwan, and S. Bhargava, "Analysis of cryptographic algorithms for network security," https://ijcatr.com/archives/volume3/issue2/ijcatr03021009.pdf, 2014.

[4] N. Sklavos and I. D. Zaharakis, "Cryptography and security in internet of things (iots): Models, schemes, and implementations," https://ieeexplore.ieee.org/abstract/document/7792443, 2016.

[5] Sharma, Neha, Prabhjot, and H. kaur, "A review of information security using cryptography technique," https://web.s.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=09765697&AN=132075850&h=kmlgcUwkLG5XTYeMteUvGY%2brjzeyZNXRrf0XvkbAwL%2bMytYKG0Q9B%2fVzLMlXcSVfcNKlwofRpOBeRN6IkIk75Q%3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%3dsite%26authtype%3dcrawler%26jrnl%3d09765697%26AN%3d132075850, 2017.

[6] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of cryptography in network security," https://link.springer.com/chapter/10.1007/978-981-15-9317-8_5, 2020.

[7] M. S. V. B. and M. K. R. D., "A review on network security and cryptography," https://www.indianjournals.com/ijor.aspx?target=ijor:rjet&volume=12&issue=4&article=004, 2022.

[8] S. Charles and P. Mishra, "Securing network-on-chip using incremental cryptography," https://ieeexplore.ieee.org/abstract/document/9154968, 2020.

[9] I. Bhardwaj, A. Kumar, and M. Bansal, "A review on lightweight cryptography algorithms for data security and authentication in iots." https://ieeexplore.ieee.org/abstract/document/8269731, 2017.

[10] A. S. Divya and A. Seema, "A review on cryptography, attacks and cyber security," https://web.s.ebscohost.com/abstract?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=09765697&AN=124636318&h=

2fP7I9ed4uBaSnUBRju9g1BIOxevueGBhu3IVsglg4tbGQVPc48lHnKlOf8iwCoxLW6F
3d%3d&crl=c&resultNs=AdminWebAuth&resultLocal=ErrCrlNotAuth&
crlhashurl=login.aspx%3fdirect%3dtrue%26profile%3dehost%26scope%
3dsite%26authtype%3dcrawler%26jrnl%3d09765697%26AN%3d124636318,
2017.

[11] S. M. Musa, "Network security and cryptography," https://books.google.
ru/books?hl=ru&lr=&id=WTtaDwAAQBAJ&oi=fnd&pg=PT21&dq=
related:-7TnHxGcgOEJ:scholar.google.com/&ots=3Ih-TzSjUd&sig=
WKbuVkiJ0HSJWBtehhHgy3bDwfI&redir_esc=y#v=onepage&q&f=false,
2018.

[12] F. Maqsood1, M. Ahmed, M. M. Ali, and M. A. Shah, "Cryptography: A
comparative analysis for modern techniques," https://pdfs.semanticscholar.
org/8331/4e07dfb9d15145fa79734f63e47932866101.pdf, 2017.