АНАЛИЗ СИММЕТРИЧНЫХ И АСИММЕТРИЧНЫХ АЛГОРИТМОВ ШИФРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ДАННЫХ

Гришина С.А., Булатова А.Р.,

Поволжский государственный университет телекоммуникаций и информатики, г. Самара, Россия

Аннотация. В настоящее время в сетях цифровой связи одной из основных проблем является обеспечение информационной безопасности. Для того, чтобы предотвратить уязвимости, необходимо использовать шифрование данных. Данный метод позволяет обеспечить безопасность информации в современном информационном пространстве. В данной статье проводится анализ симметричных и асимметричных алгоритмов шифрования с целью обеспечения безопасности данных. Рассматриваются принципы работы каждого типа алгоритмов, их преимущества и недостатки.

Ключевые слова: шифрование, алгоритмы шифрования, дешифрование, безопасность данных, уязвимость.

Шифрование — это процесс кодирования информации, посредством преобразования ее

в недоступный для прочтения вид, с целью защиты данных и передачи их по каналу связи определенному получателю. Дешифрование — это метод декодирования зашифрованных данных в читаемую информацию.

В 1976 году Уитфилд Диффи и Мартин Хеллман представили концепцию криптографии с открытым ключом, которая позволяла использовать два ключа – открытый ключ для шифрования и закрытый ключ для процесса дешифрования. Этот метод устранил необходимость в безопасном обмене ключами, внедрив инфраструктуру открытых ключей [3].

Изобретение асимметричного шифрования кардинально изменило мир криптографии. Ранее все методы шифрования основывались только на одном ключе – симметричном шифровании, которым отправитель и получатель должны были обмениваться.

Симметричное шифрование — это метод шифрования, который использует один ключ для шифрования и дешифрования информации. Данный метод шифрования использует секретный или общий ключ, который пользователи должны хранить в тайне для поддержания безопасности зашифрованных данных.

Использование одного и того же ключа обеспечивает эффективную и быструю связь, что делает симметричное шифрование надежным решением для защиты данных.

Примеры симметричного шифрования:

1. При безопасном обмене сообщениями ключ используется как для шифрования, так и для дешифрования, обеспечивая конфиденциальность.

2. Виртуальные частные сети (VPN) используют симметричное шифрование для безопасного соединения с удаленным сервером.

3. При шифровании файлов на компьютере или в облаке используются алгоритмы симметричного шифрования для защиты доступа.

4. Протокол SSL/TLS использует симметричное шифрование для защиты онлайн-транзакций.

Преимуществами симметричного шифрования являются:

1. Простота и легкость реализации, так как требуется только один секретный ключ.

2. Высокая скорость и способность обрабатывать большие объемы данных, подходящая для сценариев реального времени и массовой передачи информации.

Однако у данного вида шифрования есть несколько недостатков. При потере ключа зашифрованные данные могут стать уязвимыми для злоумышленников, а безопасный обмен ключом с предполагаемым получателем не так прост. Все то, что отправляется через Интернет, может быть подвержено киберугрозам.

Несмотря на недостатки, алгоритмы симметричного шифрования остаются популярным выбором для большинства приложений из-за их простоты и эффективности.

Для повышения безопасности применяется алгоритм асимметричного шифрования. В данном методе шифрования используются два ключа – открытый ключ и закрытый ключ. Открытый ключ используется для шифрования, а закрытый ключ - для дешифрования. Данный метод шифрования предоставляет безопасную связь и аутентификацию пользователя, что гарантирует безопасную передачу информации, однако, он более медленный и ресурсоемкий по сравнению с симметричным шифрованием.

При генерации двух отдельных ключей создаются открытый и закрытый ключи. Открытый ключ предоставляется пользователям, а закрытый ключ не разглашается. Если сторона А хочет отправить стороне Б зашифрованные данные, то А использует открытый ключ Б для их шифрования. Только Б может расшифровать данные, используя свой закрытый ключ. Этот процесс гарантирует, что только предполагаемый получатель сможет получить доступ к расшифрованным данным.

С помощью алгоритма RSA, разработанного Ривест Шамиром и Адлманом, открытый ключ производит шифрование, а закрытый ключ - дешифрование информации.

Обмен ключами Диффи Хеллмана (DHKE), позволяет двум сторонам согласовать общий секретный ключ, путем обмена данными по общедоступному каналу связи [2]. Примером могут быть приложения для обмена сообщениями и виртуальные частные сети (VPN), использующие данный метод шифрования для установления безопасных каналов связи.

Алгоритм криптографии на эллиптических кривых (ECC), содержащий в себе математические уравнения на эллиптических кривых для генерации ключей шифрования, подходит для различных приложений, устройств Интернета вещей (IoT) и блокчейн-технологий.

К преимуществам асимметричного шифрования можно отнести:

1. Обеспечение более надежной защиты данных, так как закрытый ключ для расшифровки не передается по сети.

2. Нет необходимости обмениваться общим ключом при использовании асимметричных ключей.

3. Создание и проверка цифровых подписей для подлинности сообщений становится более простой.

4. Подходит для безопасного обмена информацией между несколькими сторонами, что делает это шифрование высоко масштабируемым.

К недостаткам асимметричного шифрования относят:

1. Использование шифрования требует больших вычислительных затрат, это может сказаться на скорости работы алгоритмов шифрования и дешифрования.

2. Управление двумя ключами при использовании асимметричного шифрования может быть сложным, особенно в крупномасштабных системах.

3. Алгоритмы асимметричного шифрования могут быть подвержены атакам метода перебора, хотя большая длина ключа снижает этот риск.

4. Реализация асимметричного шифрования требует хорошего понимания криптографических концепций, это может стать вызовом для неподготовленных пользователей.

Комбинирование асимметричного и симметричного шифрования способствует повышению уровня безопасной и эффективной системы связи Примерами такого подхода являются: протокол безопасности транспортного уровня (TLS) и протокол защищённых конечных точек соединения (SSL).

Данные протоколы безопасности сочетают в себе симметричное и асимметричное шифрование для обеспечения безопасности и эффективности защиты онлайн-коммуникаций. Асимметричное шифрование позволяет безопасно обмениваться ключами, а симметричное шифрование обеспечивает быстрое и простое шифрование данных.

TLS/SSL шифруют данные при передаче, однако, из-за необходимости установить безопасное соединение с использованием асимметричного шифрования перед обменом симметричным ключом, в данных протоколах есть дополнительный уровень сложности [1].

Симметричное и асимметричное шифрование играют важную роль в обеспечении безопасности конфиденциальной информации и коммуникаций в современном мире. Каждый из них имеет свои преимущества и недостатки, и при правильном их использовании эти алгоритмы гарантируют, что наша информация останется в безопасности. Наука криптографии продолжает развиваться для защиты информационной безопасности, от новых, все более сложных угроз, именно поэтому симметричные и асимметричные криптографические системы будут оставаться

актуальными на протяжении многих лет.

Литература

1. Балакирев П.А. Анализ алгоритмов асимметричного шифрования // Вестник науки. 2020. №4 (25). URL: https://cyberleninka.ru/article/n/analiz-algoritmov-asimmetrichnogo-shifrovaniya

2. Муратов Г.А. ОСОБЕННОСТИ РАБОТЫ ПРОТОКОЛА TLS/SSL // Молодой исследователь Дона. 2021. №3 (30). URL: https://cyberleninka.ru/article/n/osobennosti-raboty-protokola-tls-ssl

3. Чичикин Гордей Ярославович, Семёнов Дмитрий Андреевич Криптосистема RSA // Наука, образование и культура. 2019. №5 (39). URL: https://cyberleninka.ru/article/n/kriptosistema-rsa