УДК 004.056.55

Абдрахманова Н.Ж.

Магистрант

Научный руководитель: Кузенбаев Б.А. доктор PhD,зав. Кафедрой

Костанайский Региональный Университет

ИССЛЕДОВАНИЕ И АНАЛИЗ СОВРЕМЕННЫХ КРИПТОСИСТЕМ ДЛЯ ЗАЩИТЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Аннотация*: Данное исследование представляет собой анализ современных криптосистем, используемых для обеспечения безопасности в информационных технологиях. В работе рассмотрены такие криптосистемы, как AES, RSA и ECC, описаны их принципы работы, особенности и степень защищенности от криптоанализа и квантовых атак. В результате анализа были выявлены преимущества и недостатки каждой криптосистемы, а также рекомендации по выбору наиболее подходящей системы в зависимости от конкретной задачи и требований к безопасности данных. Исследование может быть полезным для специалистов в области информационной безопасности, а также для людей, работающих в области разработки и реализации криптосистем.*

Ключевые слова: *криптография, шифрование, дешифрование, симметричный ключ, ассиметричный ключ.*

Abdrakhmanova N.Zh.

Master's student

Scientific supervisor: Kuzenbaev B.A. Doctor PhD, Head Department

Kostanay Regional University

RESEARCH AND ANALYSIS OF MODERN CRYPTOSYSTEMS TO PROTECT COMPUTER SECURITY

Abstract: *This study is an analysis of modern cryptosystems used to ensure security in information technology. The work examines such cryptosystems as AES, RSA and ECC, describes their operating principles, features and degree of security against cryptanalysis and quantum attacks. As a result of the analysis, the advantages and disadvantages of each cryptosystem were identified, as well as recommendations for choosing the most suitable system depending on the specific task and data security requirements. The study may be useful for specialists in the field of information security, as well as for people working in the field of development and implementation of cryptosystems.*

Keywords: *cryptography, encryption, decryption, symmetric key, asymmetric key.*

1.Введение.

Сейчас, в дни очень быстрого роста электронного обмена данными, все мы общаемся в киберпространстве без какой-либо защиты. Мы передаем друг другу большую часть нашей конфиденциальной и наиболее приватной информации и данных. Поэтому в целях безопасности мы используем криптографические методы. По сути, криптография – это техника секретного письма и чтения. Это процесс преобразования и хранения информации или данных в определенном формате , поэтому понять и обработать эту информацию могут только те, для кого она предназначена. Криптография включает в себя различные технологии, такие как:

-объединение писем с изображениями и многие другие способы защиты данных для целей передачи.

-криптографические технологии, используемые в информационной безопасности для защиты личных данных от кибер-хакеров и неавторизованных сторон.

Существует также другое название криптографии – криптология, которая помогает пользователям шифровать и расшифровывать скрытые тексты в различных нечитаемых кодах с целью безопасной передачи частной информации

2.Методы

В этой статье опишем информационную безопасность в терминах криптографии. В наши дни этот глобальный мир использует интернет сайты и их реализации в любой ситуации своей жизни. Следовательно, для этих современных реализаций существует некоторая необходимость в защите их информации с помощью криптографических процедур. Хотя криптография допускает множество методов защиты информации, а также предоставляет несколько целей для алгоритмов шифрования и алгоритмов дескрипции. Благодаря этим целям мы можем легко закодировать наши информационные средства в неразборчивом формате, чтобы никто не мог понять это без какого-либо разрешения.

Симметричная криптография основана на алгоритмических методах. Этот метод использует один и тот же цифровой ключ как для шифрования, так и для дешифрования. Отправитель и получатель выделяют один и тот же закрытый ключ. Через этот секретный ключ отправителя, через средство связи зашифрованное сообщение отправляется получателю. Получатель может расшифровать зашифрованный текст в удобночитаемый формат с помощью того же ключа. В симметричной криптографии есть слабое место, поскольку она может быть легко расшифрована благодаря

одному и тому же ключу. Таким образом, киберпреступникам и хакерам очень легко подвергнуться атаке.

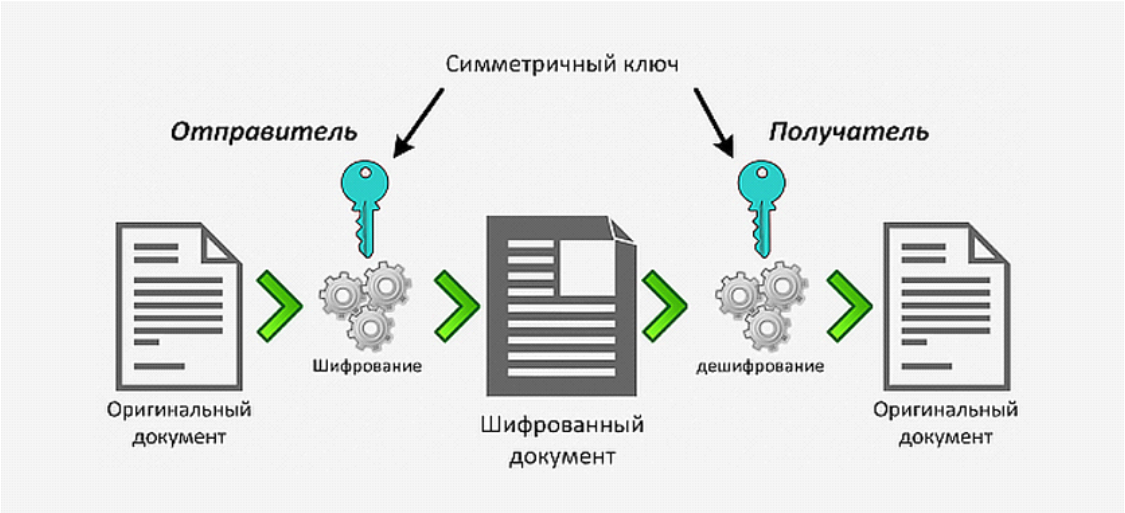

Рисунок 1. Пример симметричного ключа

Один из наиболее распространенных алгоритмов с симметричным ключом является — AES (Advanced Encryption Standard), который использует 128-битные, 192-битные или 256-битные ключи для шифрования данных. AES принимает широкое участие среди многих пользователей безопасности. Преимущества использования ключа AES заключаются в его высокой скорости работы и надежности. Этот алгоритм шифрования используется во многих сферах, таких как финансы, правительственные структуры, здравоохранение и другие, для защиты данных от несанкционированного доступа.

В информационной безопасности с использованием криптографии идея криптографии с асимметричным ключом заключается в том, что она использует пару ключей или означает два ключа – 1-й один открытый ключ и 2-й один закрытый или секретный ключ как для процесса шифрования, так и для процесса дешифрования с целью защиты конфиденциальных данных от третьих неавторизованных сторон . Мы

можем назвать асимметричную криптологию криптографией с открытым ключом. Использование и основная цель этой криптографии – решить еще много проблем, потому что с помощью криптографии с симметричным ключом мы не можем этого сделать.

Рисунок 2. Пример ассиметричного ключа

(RSA) Криптотехника (Ривеста – Шамира – Адельмана) –это система асимметричных ключей, которая основана на лежащих в основе наиболее сложных проблемах и устранении неполадок, возникающих в системе. Поэтому эти три инвестора изобрели алгоритм, названный RSA, примерно в 1978 году . Основная идея алгоритма RSA в том, что трудно разложить на множители наибольшее количество целых чисел за весь жизненный цикл информационной безопасности. Асимметричный ключ содержит два числа, из двух чисел одно число является умножением двух простых чисел, а секретный ключ также состоит из одной и той же пары простых чисел. Поэтому, если кто-то захочет разложить на множители эти два больших простых числа, секретный ключ будет скомпрометирован. Таким образом, надежность шифрования полностью зависит от размера используемого ключа. И если мы увеличим двойной или тройной размер

ключа, то автоматически надежность шифрования возрастет в геометрической прогрессии. Длина ключа RSA составляет от 1024 бит до 1048 бит.RSA используется для шифрования и дешифрования данных, а также для создания цифровых подписок.

SHA (алгоритм безопасного хеширования) — это семейство алгоритмов хеширования, требующее обеспечения безопасности и соблюдения безопасности паролей и других конфиденциальных данных. SHA-1, SHA-2 и SHA-3 являются наиболее распространенными алгоритмами хеширования.

Три основных хэш функции:

- Детерминировано шифровать данные (такой вид шифрования всегда создает одно и то же зашифрованное значение для одного и того же текстового значения);
- Принимать ввод любой длины, а выводить результат фиксированной длины;
- Изменять данные необратимо. Ввод нельзя получить из вывода.

Шифрование SHA и безопасность:

Что такое «потенциал безопасности»? Данное выражение означает, что в ближайшие несколько лет не появится доступное устройство, которое сможет расшифровывать алгоритм шифрования. Например:

1. Зашифрованную информацию с помощью SHA0 можно расшифровать, так как устройства для этого есть в наличии, поэтому этот алгоритм шифрования вообще не безопасен.
2. Расшифровка SHA1 практически невозможна на рядовом устройстве. Однако, если воспользоваться более мощными устройствами, тогда за огромное количество операций этот алгоритм можно расшифровать. Число требуемых операций для расшифровки SHA1 очень большое и составляет

252. Повторимся, расшифровать SHA1 абы кому не получится, но раз есть такая вероятность, значит, алгоритм перешел в статус «условно не безопасного». Из-за этого многие компании и приложения отказались от его использования, но какая-то часть использует до сих пор.

3. На сегодняшний день алгоритм SHA2 невозможно расшифровать. И такая ситуация продержится еще несколько лет, до тех пор, пока не будет доступно устройство, расшифровывающее SHA2.
4. Алгоритм SHA3 невозможно расшифровать. Также пока неизвестно, когда появится устройство, умеющее это делать, поэтому он считается самым надежным на сегодня, хоть и не самым популярным.

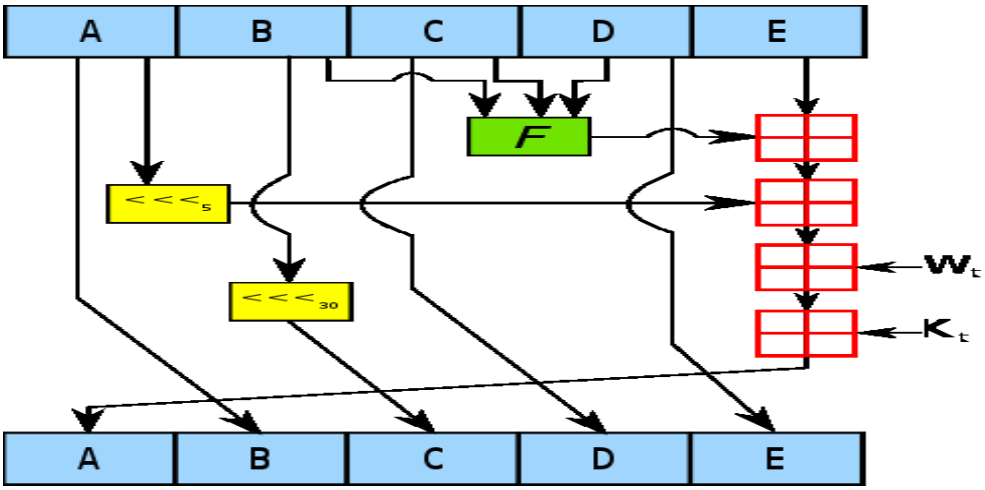

Рисунок 3. Пример шифрования SHA

Для защиты данных на более высоком уровне многие системы безопасности используют криптографические протоколы, такие как SSL (Secure Sockets Layer) и TLS (Transport Layer Security). Эти протоколы используются для шифрования данных, защищенных между клиентом и сервером.

3.Результаты и обсуждения.

В ходе исследования были проанализированы различные криптосистемы, такие как AES, RSA, SHA и другие. Были выявлены их преимущества и недостатки, а также возможные уязвимости и способы атак.

В результате исследования было установлено, что криптосистема AES является наиболее надежной для защиты данных. Она обладает высокой скоростью работы, а также высокой стойкостью к атакам.

Однако, необходимо отметить, что выбор криптосистемы зависит от конкретного случая и требований к безопасности. Не все криптосистемы подходят для защиты конкретных данных.

Таким образом, можно сделать вывод, что правильный выбор криптосистемы является важным фактором для обеспечения компьютерной безопасности.

Во всем мире крупные государства регулируют применение средств защиты информации правовыми методами. Государство может запрещать или ограничивать использование криптографических систем частными лицами, при этом некоторые документы и другая секретная информация государственной важности хранятся в зашифрованном виде.Так, в Великобритании человек обязан выдать пароль от своего компьютера или телефона правоохранительным органам, в том случае, если проводится судебное расследование. Отказ выдать средство дешифрования является уголовным преступлением. В Казахстане использование криптографии ограничено для компаний и индивидуальных предпринимателей. Любая деятельность по выпуску и продаже шифровальных программ должна лицензироваться.В США действует стандарт AES, согласно которому важная государственная информация должна храниться в зашифрованном виде. Спецслужбы (АНБ, ЦРУ) могут требовать от производителей устройств и разработчиков ПО выдачу ключей дешифрования.Наука о криптографических методах сокрытия

информации – одна из самых актуальных в наше время. Она занимает большую нишу в области информационной безопасности и широко используется не только государствами, но и крупными компаниями, бизнесом, частными лицами.

4.Выводы

В заключение можно сказать, что криптография в информационной безопасности - лучшее решение многих сложных задач. Криптографическая технология - это способ, с помощью которого могут быть решены проблемы безопасности. Безопасность данных - это способ изучения, с помощью которого мы можем защитить нашу информацию. Этот метод наиболее важен, потому что несколько государственных структур хотят обезопасить своих граждан. День ото дня наблюдается стремительный рост электронной коммуникации и обмена ею между народами без какой-либо безопасности в киберцикле. Люди обмениваются своими личными данными и делятся друг с другом деликатными мыслями. Когда люди пользуются интернет сайтами, многие киберпреступники ждут, когда они обменяются данными. Во время преобразования информации хакеры атакуют информацию и легко крадут информацию, после кражи информации эти хакеры злоупотребляют этими данными. Криптография - это лучший технический термин для обозначения безопасности, но с помощью той же техники информационные хакеры могут взломать информацию. Сейчас, в мире компьютеризации, мы решаем различные вопросы безопасности. Наиболее важной целью криптографических методов в жизненном цикле информационной безопасности является то, что должны существовать наиболее надежные алгоритмы обеспечения секретности. Целью этих алгоритмов будет обеспечение конфиденциальности и других методов информационной

безопасности. Поэтому правительственная организация будет использовать эти приложения (алгоритмы) для защиты информации.

Использованная литература:

1. Applied Cryptography: Protocols, Algorithms, and Source Code in C" Bruce Schneier
2. Cryptography and Network Security: Principles and Practice" William Stallings
3. "Introduction to Modern Cryptography" Jonathan Katz and Yehuda Lindell
4. "Cryptography Engineering: Design Principles and Practical Applications" by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno
5. Senstar Symphony Common Operating Platform [Electronic resource]. URL: https://senstar.com/products/video-management/senstar-symphony-common-operating-platform/ (accessed February 10, 2023)
6. VIDEO ANALYTICS INNOVATION UNLEASHED [Electronic resource] URL: https://www.briefcam .com/ (accessed 02/13/2023)
7. Irisity - Security beyond human intelligence. [Electronic resource]. URL: https://irisity.com/ (accessed 12/15/2022)
8. Dmitriev D.V. Explanatory dictionary of the Russian language Dmitriev, 2003, - 228 p.