УДК 004.056.55

ОБЗОР МЕТОДОВ И АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ

Т.Ю. Голиков

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: И.Н. Тонкович, канд.хим.наук, доцент

Аннотация. Постоянно растущий объем конфиденциальных данных, отправленных через email, делает опасность утечки информации актуальной задачей. Технология шифрования с открытым и закрытым ключом обеспечивает безопасность и целостность данных от большинства злоумышленников. Однако таких мер защиты в полной мере оказывается недостаточно. В данной работе проведено исследование «узких» мест данной технологии.

Ключевые слова: защита данных, электронная почта, криптография, методы и алгоритмы шифрования сообщений, ассимметричное шифрование, симметричное шифрование

Введение. Сервис электронной почты на сегодняшний день является старейшим и наиболее востребованным средством коммуникации. Длительное и активное развитие не могло не сказаться на безопасности этого сервиса. Эксперты в области информационной безопасности среди потенциальных угроз, характерных для систем электронной почты, выделяют следующие: уязвимость как самой электронной почты так и ее компонентов. передачу вредоносных файлов, утечку информации, XSS-атаки, Анти-APT. Постоянно растущий объем конфиденциальных корпоративных и пользовательских данных, отправленных через email, делает опасность утечки информации актуальной задачей.

Решение данной задачи обеспечивают технологии, использующие средства шифрования и предотвращения утечки данных.

По данным Google количество шифруемых сообщений на сегодняшний день составляет более 90%: шифрование исходящих электронных сообщений – 92%, шифрование входящих электронных сообщений – 94% [1].

Статистика шифруемых данных исходящих и входящих сообщений за период с 01 января 2021 года по 12 марта 2021 года приведена на рисунке 1.

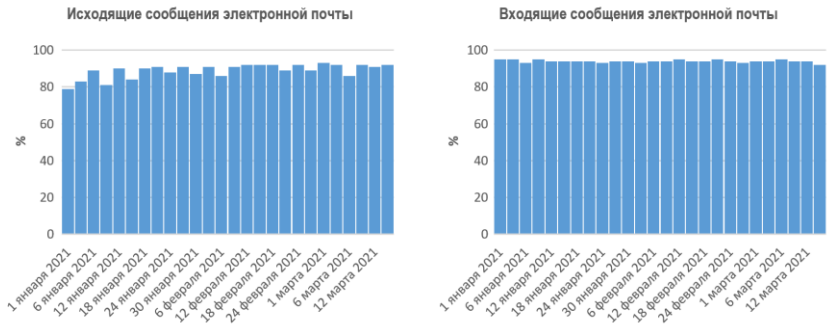

Рисунок 1 – Статистика шифруемых данных

Шифрование позволяет передавать информацию в защищенной форме, обеспечивая безопасность, конфиденциальность и целостность данных. При защите конфиденциальной информации используемые криптографические технологии способствуют, как правило, высокому уровню безопасности персональных данных отдельных людей и групп. Криптография с открытым ключом с цифровыми подписями обеспечивает в целом безопасность и целостность. Однако таких мер защиты оказывается недостаточно.

Данное исследование посвящено выявлению «узких» мест технологии шифрования с открытым и закрытым ключом.

Основная часть. В настоящее время в сфере информационной безопасности выделяют две группы методов шифрования электронных сообщений: с симметрическим и асимметрическим шифрованием.

Симметрическое шифрование – это способ шифрования данных, при котором для шифрования и восстановления зашифрованных сообщений используется один ключ.

Асимметрическое шифрование – это криптографическая система, использующая открытые и закрытые ключи для шифрования и восстановления сообщений.

Выделим преимущества и недостатки алгоритмов симметрического и асимметрического шифрования.

Наиболее известными криптографическими алгоритмами симметрического шифрования являются: DES, AES, IDEA, Blowfish. Рассмотрим их.

Data Encryption Standard (DES). Алгоритм DES, разработанный фирмой IBM, использует комбинацию нелинейных и линейных преобразований для шифрования сообщений. Преимуществом данного алгоритма является высокая стойкость и скорость работы алгоритма за счет его простоты и, зашифровав сообщение с помощью одного пакета программ, для расшифровки можно использовать любой другой пакет. Недостатком данного алгоритма считают ограниченное количество ключей, из-за чего появляется возможность их полного перебора на быстродействующей вычислительной технике.

Advanced Encryption Standard (AES). Алгоритм AES – это блочный шифр, который может шифровать и расшифровывать информацию. Шифрование преобразует данные в неразборчивую форму, называемую зашифрованным текстом. Расшифровка зашифрованного текста преобразует данные обратно в исходную форму, называемую открытым текстом. Алгоритм AES может использовать криптографические ключи 128, 192 и 256 бит для шифрования и дешифрования данных блоками по 128 бит. При разработке алгоритм был ориентирован на аппаратную реализацию и содержал операции, выполняемые на универсальных микропроцессорах не слишком эффективно, что является его недостатком.

Blowfish. Алгоритм Blowfish реализует блочное симметрическое шифрование с переменной длинной ключа. Алгоритм состоит из двух частей: расширение ключа и шифрование данных. Данный алгоритм обладает высокой скоростью шифрования на развернутом ключе, низкой вероятностью ошибок, за счет простоты алгоритма и отсутствием известных успешных атак на полно раундовую версию алгоритма. Хотя Blowfish по скорости опережает некоторые свои аналоги, но при увеличении частоты смены ключа основное время работы уходит на подготовительный этап, что в сотни раз уменьшает его эффективность [2].

International Data Encryption Algorithm (IDEA). IDEA известен тем, что применялся в пакете программ шифрования Pretty Good Privacy. Данный алгоритм использует 128-битный ключ и 64-битный размер блока, для шифрования фрагментов сообщения. Свободное пространство последнего 64-битного блока заполняется определённой последовательностью бит. Позже происходит разбиение этих блоков на блоки в 16 бит, над которыми и совершаются манипуляции с данными. Главными недостатками являются непредусмотренное увеличение ключа и медленная обработка сообщений по сравнению с другими аналогами.

Наиболее известными криптографическими алгоритмами асимметрического шифрования являются: RSA, DSA, ECDSA, McEliece.

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman). Это криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Преимущества данного алгоритма – это возможность открытого распространения ключей в сети Интернет и линейная зависимость между числом занятых ключей и количеством подписчиков. Недостатки реализации криптографического алгоритма шифрования RSA на практике делают его менее безопасным, чем отмечалось в теории.

Digital Signature Algorithm (DSA). DSA – это криптографический алгоритм с использованием пары ключей, для создания электронной подписи, но не для шифрования. Подпись создается секретно (закрытым ключом), но может быть публично проверена (открытым клю-

чом). Это означает, что только один субъект может создать подпись сообщения, но любой может проверить её корректность. К недостаткам данного алгоритма можно отнести временные затраты на проверку и отсутствие шифрования в электронной подписи [3].

Elliptic Curve Digital Signature Algorithm (ECDSA). Это алгоритм с открытым ключом для создания цифровой подписи, определённый в группе точек эллиптической кривой. Основная особенность ECDSA по сравнению с другим популярным алгоритмом RSA заключается в том, что ECDSA обеспечивает более высокую степень безопасности с меньшей длиной ключа. Недостатком данного алгоритма является большой массив данных, необходимый для обработки [4].

McEliece. McEliece криптографический алгоритм с использованием алгебраического кодирования. Одно из преимуществ данного алгоритма состоит в том, что криптосистема включает элемент случайности в каждое шифрование для повышения безопасности. Это является случайно сгенерированным вектором ошибок. RSA и другие современные криптосистемы не включают такую случайность в процесс шифрования.

Заключение. Преимущества асимметрических алгоритмов заключаются в отсутствии необходимости передачи секретного ключа по надёжному каналу, меньшем количестве ключей в больших сетях, чем при использовании симметрического шифрования, повышенной степени защиты, поскольку ключ дешифрования, который нужно держать в секрете, известен только одной стороне. Однако в алгоритмы асимметрического шифрования трудно внести изменения, шифрование и расшифровывание происходит медленнее, вычислительные системы требуют больше ресурсов для работы и по сравнению с симметрическим шифрованием, более длинные ключи.

Главный недостаток ассиметричных алгоритмов шифрования сообщений заключается в медленном исполнении. Из-за того, что симметричные алгоритмы работают в 1 000 раз быстрее, чем асимметричные алгоритмы шифрования, их используют для шифрования сообщений, а ассиметричные используются для засекречивания и распространения сеансовых ключей. Указанные недостатки требуют разработки новых подходов и приемов выполнения данных алгоритмов.

Список литературы

1. *Отчет Google о доступности сервисов и данных. Шифрование электронных сообщений [Электронный ресурс] – Режим доступа: https://transparencyreport.google.com/safer-email/overview?hl=ru/.*

2. *Криптографический алгоритм Blowfish [Электронный ресурс] – Режим доступа: http://cryptowiki.net/index.php?title=. Криптографический_алгоритм_Blowfish.*

3. *Алгоритм DSA [Электронный ресурс] – Режим доступа: http://solutionmes.wikidot.com/crypto-dsa.*

4. *Vaudenay, Serge: The Security of DSA and ECDSA. In Desmedt, Yvo (editor): Public Key Cryptography, volume 2567 of Lecture Notes in Computer Science, pp 309–323.*

UDC 004.056.55

OVERVIEW OF DATA ENCRYPTION METHODS AND ALGORITHMS

T.Y. Holikau

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

I.N. Tonkavich – PhD, associate professor

Annotation. The ever-growing volume of sensitive data sent via email makes the danger of information leakage a topical issue. Public and private key encryption technology ensures data security and integrity from most attackers. However, such protection measures are fully insufficient. In this paper, a study of the «bottlenecks» of this technology is carried out.

Keywords: data protection, email, cryptography, message encryption methods and algorithms, asymmetric encryption, symmetric encryption, information security