Операции с большими числами и информационная безопасность облачных технологий

Operations with large numbers and information security of the cloud computing

Гринюк О.Н.
канд. техн. наук, доцент кафедры «Автоматизация производственных процессов», НИ РХТУ им. Д.И. Менделеева, г. Новомосковск
e-mail: olgrinyuk@mail.ru

Grinyuk O.N.
Candidate of Technical Sciences, Associate professor "Automation of productions", NI RHTU of D.I. Mendeleyev, Novomoskovsk
e-mail: olgrinyuk@mail.ru

Алексашина О.В.
канд. техн. наук, доцент кафедры «Стандартизация, метрология и сертификация», Московский политехнический университет, г. Москва
e-mail: svirukova@ya.ru

Aleksashina O.V.
Candidate of Technical Sciences, Associate Professor of the Department "Standardization, Metrology and certification", Moscow Polytechnic University, Moscow
e-mail: svirukova@ya.ru

Санаева Г.Н.
Старший преподаватель кафедры «Вычислительная техника и информационные технологии», НИ РХТУ им. Д.И. Менделеева, г. Новомосковск
e-mail: gn_san@mail.ru

Sanayeva G.N.
Senior teacher "Computer facilities and information technologies", NI RHTU of D.I. Mendeleyev, Novomoskovsk
e-mail: gn_san@mail.ru

Аннотация
Информационная безопасность облачных технологий на сегодня является актуальным вопросом. Приводятся методики защиты облачных данных и популярных инструментов для шифрования файлов для облачных данных. Рассматриваются особенности одного из наиболее успешных асимметричных алгоритмов шифрования на сегодняшний день – алгоритма RSA. Приводятся перспективы использования данного алгоритма.
Ключевые слова: информационная безопасность облачных технологий, асимметричный алгоритм шифрования, алгоритм RSA.

Abstract
The information security of a cloud computing, is so topical issue for today. Techniques of protection of cloudy data and popular tools for enciphering of files for cloudy data are given. Is

considered features of one of the most successful asymmetric algorithm of enciphering today - RSA algorithm. The prospects of use of this algorithm are given.
Keywords: Information security of a cloud computing, asymmetric algorithm of enciphering, RSA algorithm.

Информационная безопасность облачных технологий на сегодня является настолько актуальным вопросом, что от его решения зависит развитие в целом индустрии средств защиты информации в перспективных информационно-телекоммуникационных системах.

С точки зрения обеспечения безопасности, «облака» представляют собой лишь одну из разновидностей инфраструктурных платформ, пусть даже с высокой степенью автоматизации. Разумеется, и в облаке не обойтись без процессов, которые хорошо зарекомендовали себя в традиционных физических системах. Такие основополагающие функции, как межсетевой экран, IDS/IPS, виртуальное закрытие уязвимостей (Virtual Patching) и антивирусы, являются обязательными элементами любой концепции безопасности, будь то физические, виртуальные или облачные системы. А вот задачи, возникающие при управлении этими функциями, в различных инфраструктурах отличаются [1].

Предлагаемые решения представляют собой широкий спектр реализаций от продуктов с многофункциональным набором средств защиты от различных типов угроз до узконаправленных решений для отражения конкретных атак.

Однако пользователям «облаков» важно понимать, что массовое применение виртуализации не предлагает в настоящее время универсального решения вопроса защиты. Каждой компании со своей собственной ИТ-средой при вхождении в «облако» стоит задуматься над применением технологий защиты, сопоставимых с ее функциональными задачами и рисками.

Поэтому, вероятно, самым простым и надёжным способом защиты данных от просмотра третьей стороной является их ручное шифрование непосредственно перед отправкой в «облако». В принципе для этого подойдёт любой шифровальщик с поддержкой алгоритма AES. В конце концов, файлы можно запаковать архиватором WinRAR и установить на архив достаточно сложный пароль. Оба эти варианта просты, надёжны, но не слишком удобны. Если файлов много, а доступ к ним нужно иметь постоянный, процедуру шифрования можно попробовать автоматизировать. Для этого используются приложения, которые служат своего рода посредниками между компьютером пользователя и облачным хранилищем. Принцип их работы довольно прост. Они перехватывают отправляемые в «облако» файлы и автоматически шифруют их, так что на сервер они попадают уже в зашифрованном виде. При этом ключи шифрования хранятся только у пользователя и возможность того, что к корпоративным данным получат доступ злоумышленники извне либо сотрудники самого облачного сервиса исключается. Примерно та же самая процедура выполняется при скачивании зашифрованных файлов на компьютер пользователя. Шифрование же и дешифрование производится на клиентской машине [4].

Сегодня одним из наиболее популярных инструментов для шифрования файлов является приложение Boxcryptor. Boxcryptor – сервис, предназначенный для защиты данных частных пользователей и компаний при их размещении в облачных хранилищах Яндекс.Диск, Dropbox, Google Drive, Box, OneDrive, Amazon Cloud Drive, Amazon S3, CloudMe, Cloudwatt, Cubby, Egnyte, GMX, iCloud Drive, livedrive, Orange, SDS, SpiderOak, storegate, Strato HiDrive, SygarSync, Telekom, WEB.de, а также в системе для самостоятельного облачного хранения (ownCloud) и на локальном хранилище (Local Storage). Метод, используемый Boxcryptor для шифрования, – алгоритмы шифрования AES-256 и RSA [6] .

Другой вариант обеспечения защиты личных файлов в «облаке» основывается

исключительно на доверии к разработчикам хранилища. Есть сервисы, отличающиеся более высоким уровнем безопасности, чем их популярные конкуренты. Таковыми являются SpiderOak и Tresorit. Первый позиционируется как сервис для резервного копирования. Для защиты данных в SpiderOak применяется комбинация алгоритмов 2048 RSA и 256 AES [5].

Выбор криптографического алгоритма и режима его использования зависит от особенностей передаваемой информации (ее ценности, объема, способа представления, необходимой скорости передачи и т.д.), а также возможностей владельцев по защите своей информации. Все это существенным образом влияет на выбор криптографического алгоритма и организацию защиты данных. Анализ литературных источников показывает, что каждый из наиболее распространенных типов симметричных и асимметричных алгоритмов шифрования имеет свои преимущества и недостатки. Поэтому при выборе того или иного алгоритма шифрования или их сочетания, необходимо учитывать в какой ситуации, какой из алгоритмов работает лучше. При этом при выборе того или иного алгоритма шифрования могут учитываться такие показатели, как: длина ключа, затраты на подбор, производительность, совместимость [3].

Одним из наиболее успешных асимметричных алгоритмов шифрования на сегодняшний день является алгоритм RSA. В противоположность традиционным симметричным системам шифрования, RSA работает с двумя различными ключами: «открытым» и «закрытым» ключом. Оба работают совместно друг с другом и сообщение, зашифрованное одним из них, может быть расшифровано только вторым. Так как закрытый ключ не может быть вычислен из открытого ключа, последний может храниться в открытом доступе. Безопасность RSA основана на математической проблеме факторизации произведения двух больших целых чисел. Шифруемое сообщение рассматривается как одно большое число. Во время шифрования оно возводится в степень ключа и делится с остатком на произведение первых двух. Повторяя процесс с другим ключом, можно получить исходный текст [2].

Чтобы построить пару ключей для RSA, надо сделать следующее:

1. Взять два больших простых числа p и q.
2. Вычислить $n = pq$.
3. Взять небольшое нечетное число e, взаимно простое с $\varphi(n) = (p-1)(q-1)$.
4. Вычислить $d = e^{-1} \pmod{\varphi(n)}$.
5. Пара $P = (e, n)$ — открытый RSA-ключ.
6. Пара $S = (d, n)$ — секретный RSA-ключ.

Шифром сообщения m будет $m^e \pmod n$. Для дешифровки сообщения x надо вычислить $x^d \pmod n$. Надежность криптосистемы RSA основывается на трудности задачи разложения составных чисел на множители: если враг разложит (открыто опубликованное) число n на множители p и q, он сможет найти d тем же способом, что и создатель ключа.

Конечно же, большие простые числа можно строить сравнительно быстро. В противном случае теряла бы всякий практический смысл система шифрования RSA. Наиболее эффективным средством построения простых чисел является несколько модифицированная малая теорема Ферма. На практике для ускорения вычислений криптосистему RSA часто используют вместе с какой-то традиционной системой шифрования, в которой ключ необходимо хранить в секрете. Выбрав такую систему, мы используем для шифрования ее, а система RSA используется только для передачи секретного ключа.

На конференции по развитию RSA Константинос Карагианнис (Konstantinos Karagiannis), технический директор по кибербезопасности BT Americas, высказал мнение, что симметричные алгоритмы (DES, AES) с 512-значными ключами будут расколоты первыми. Как только количество кубитов превысит 100, квантовые компьютеры начнут подбирать 512-значные ключи за считанные минуты. А вот асимметричные алгоритмы

(например, RSA) с 4096-значными ключами можно будет расшифровать за аналогичный срок только с помощью 1000-кубитных компьютеров. В этом случае асимметричное шифрование с 4096-значными ключами останется надежным еще лет шесть до 2025 г., в котором может появиться компьютер мощностью примерно 1152 кубитов. Данный прогноз является условным, так как не учитывает, что новые технологии далеко не сразу начинают широко использоваться [7].

Литература

1. *Новиков А.* Сегодня в «облаках» уже вовсю гремит гром/ БИТ. Бизнес&Информационные технологии// http://bit.samag.ru/archive/article/1224 доступ 01.03.2019
2. *Лукин М., Сатюков Р.* Система шифрования RSA/Дискретная математика: Алгоритмы //http://rain.ifmo.ru/cat/view.php/theory/coding/rsa-2005.
3. Введение в криптографию, 2-е изд., испр. / Под общ. ред. В.В.Ященко. — М.: МЦНМО-«ЧеРо», 1999.
4. *Гридасов В.* Boxcryptor — шифрование данных в облачных сервисах https://www.anti-malware.ru/reviews/Boxcryptor_encrypted_data_in_the_cloud доступ 20.02.2019
5. Как обеспечить безопасность файлов в облаке https://www.xelent.ru/blog/kak-obespechit-bezopasnost-faylov-v-oblake/ доступ 03.03.2019
6. Популярное решение для шифрования файлов Boxcryptor стало доступно на русском языке https://www.macdigger.ru/news/post/populyarnoe-reshenie-dlya-shifrovaniya-fajlov-boxcryptor-stalo-dostupno-na-russkom-yazyke доступ 05.03.2019
7. Через неопределенность к квантовому превосходству: заметки с конференции RSA https://www.kaspersky.ru/blog/quantum-supremacy-rsa/20553/ доступ 03.03.2019