УДК 004.7

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ ШИФРОВАНИЯ RSA В ОБЛАЧНЫХ СИСТЕМАХ

Банит В.В.
Национальный технический университет Украины
«Киевский политехнический институт»

Исследован метод повышения эффективности использования шифрова-ния RSA в облачных системах. Разработана тестирующая программа. Проведены экспериментальные исследования.
Ключевые слова: шифрование, RSA, облачные системы, криптография, защита информации.

Постановка проблемы. Облачные вычисления – программно-аппаратное обеспечение, доступное пользователю через Интернет или локальную сеть в виде сервиса, позволяющего использовать удобный интерфейс для удаленного доступа к выделенным ресурсам (вычислительным ресурсам, программам и данным) [1].

На данный момент большинство облачных инфраструктур развернуто на серверах датацентров, используя технологии виртуализации, что фактически позволяет любому пользовательскому приложению использовать вычислительные мощности, совершенно не задумываясь о технологических аспектах. Тогда можно понимать «облако» как единый доступ к вычислениям со стороны пользователя.

При работе с облачными системами главной проблемой остается безопасность информации передаваемой между облаком и пользователем, поддерживая соответствующую скорость работы.

Для безопасной передачи данных между пользователем и облачным сервисом можно использовать криптографию. В качестве криптографического алгоритма был выбран RSA. Именно этот алгоритм позволяет использовать шифрование с открытым ключом, но в качестве недостатка имеет низкую скорость шифрования и дешифрования, в связи с тем, что для этого алгоритма выбирается большая длина ключа.

В данной статье рассматривается метод повышения эффективности ис-пользования шифрования RSA в облачных системах путем определения длины ключа для требуемого времени отклика.

Анализ последних исследований и публикаций. Последние исследования в этой области проводили А. О. Жиров, О. В. Жирова, С. Ф. Кренделев в своей диссертации на тему: «Безопасные облачные вычисления с помощью гомоморфной криптографии». Но в этих работах не учитывается факт поддержания соответствующей скорости обмена данными между пользователем и облачным сервисом.

Безопасность данных теоретически может быть под угрозой. Не все данные можно доверить стороннему провайдеру в интернете, тем более, не только для хранения, но ещё и для обработки. Все зависит от того, кто предоставляет «облачные» услуги. Если данные надежно шифруются, постоянно делаются их резервные копии, и поставщик услуг уже не один год работает на рынке и имеет хорошую репутацию, то угрозы безопасности данных может никогда не случиться. У пользователя «облачных» бизнес приложений могут также возникнуть и юридические проблемы, например связанные с выполнением требований защиты персональных данных.

Государство, на территории которого размещен датацентр, может получить доступ к любой информации, которая в нем хранится. Например, по законам США, где находится самое большое количество датацентров, в этом случае компания-провайдер даже не имеет права разглашать факт передачи конфиденциальной информации кому-либо, кроме своих адвокатов [2].

Выделение нерешенных ранее частей общей проблемы. Нерешенной проблемой является проблема защищенной передачи информации между пользователем и облаком, при этом поддерживая нужную скорость работы.

Эта проблема является, наверное, одной из самых существенных в вопросе вывода конфиденциальной информации в облако. Путей ее решения может быть несколько. Во-первых, можно шифровать всю информацию, помещаемую на облако. Во-вторых, можно просто ее туда не помещать. Однако, во всяком случае, у компаний, пользующихся облачными вычислениями, это должно быть определенным пунктом в списке вопросов информационной безопасности. Кроме того, сами провайдеры должны улучшать свои технологии, предоставляя некоторые услуги по шифрованию.

Цель статьи. Главной целью статьи является повышения эффективности использования шифрования RSA в облачных системах путем определения длины ключа для требуемого времени отклика.

Описание метода. Идея состоит в том, что между пользователем и облаком создается шифрованное соединение RSA. На облаке есть песочница, которая содержит в себе статистику зависимости длины ключей от времени отклика. Песочница анализирует требуемую скорость работы и уровень безопасности передачи данных между пользователем и облачным сервисом. Если для данного соединения требуется высокий уровень безопасности, то длина ключа берется побольше, но при этом время, затрачиваемое на шифрование и дешифрование увеличивается, что снижает скорость работы всей системы.

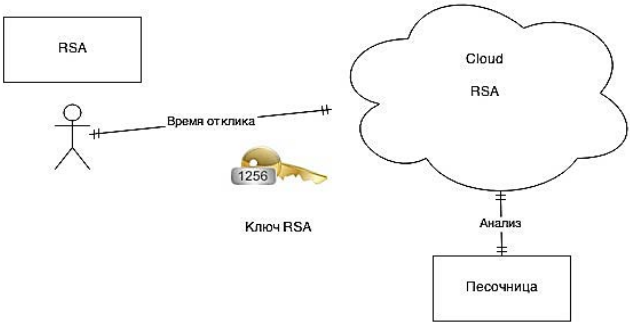

Рис. 1. Шифрованное взаимодействие с облаком

Алгоритм RSA

RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности).

Алгоритм RSA работает следующим образом: берутся два достаточно больших простых числа p и q и вычисляется их произведение n = p*q; n называется модулем.

Затем выбирается число e, удовлетворяющее 1< e < (p − 1)*(q − 1) и не имеющее общих делителей кроме 1 (взаимно простое) с числом (p − 1)*(q -1).

Затем вычисляется число d таким образом, что (e*d − 1) делится на (p − 1)*(q − 1).

e − открытый (public) показатель

d − частный (private) показатель.

(n; e) − открытый (public) ключ

(n; d) − частный (private) ключ.

Делители (факторы) p и q можно либо уничтожить либо сохранить вместе с частным (private) ключом.

Если бы существовали эффективные методы разложения на сомно-жители, то, разложив n на сомножители (факторы) p и q, можно было бы получить частный (private) ключ d. Таким образом надежность криптосистемы RSA основана на труднoразрешимой − практически неразрешимой − задаче разложения n на сомножители (то есть на невозможности факторинга n) так как в настоящее время эффективного способа поиска сомножителей не существует [3].

Практический пример необходимости шифрования. Приведем пример актуальности шифрования данных пользователя из области разработки программного обеспечения. Допустим существует облачный сервис для написания и сборки проектов, причем проект содержит не только файлы с исходным кодом, но и изображения, аудио и видео, созданные специ-ально для проекта (на данный момент действует сервис Ideone.com для компиляции только одиночных файлов с кодом).

Разработчик программного обеспечения заинтересован в безопасности и секретности хранения своих данных, дело в том что злоумышленник может перехватывать важные данные разработчика во время работы с сервисом. Что бы этого избежать данные нужно шифровать, но это в свою очередь снизит производительность, из-за того что информацию нужно постоянно кодировать и декодировать. Это негативно скажется на самой работе сервиса, так как время отклика системы значительно понижается. Что бы это исправить нужно создать систему реального времени, которая бы учитывала длину ключа, и скорость передачи пакета, так как они существенно влияют на обмен информацией между клиентом и облаком. То есть во время создания сессии между пользователем и сервисом, система анализирует время передачи пакета, его размер, и время на кодирование и декодирование, и выдает пользователю рекомендуемые параметры для данной сессии, а пользователь уже сам выбирает что ему важно на данное время: скорость работы, или безопасность.

Перед разработчиками сервиса стоит задача реализации системы шифрования которая позволит взаимодействовать с сервисом без ощутимых временных затрат.

В данной работе анализируется алгоритм шифрования RSA, а именно зависимость времени шифрования от размера пакета, величины ключа.

Описание разработанной программы. Программа состоит из 2 частей:

− первая часть представляет собой сбор статистики зависимости длины ключа от времени шифрования, учитывая также длину блока.

− вторая часть − это сама песочница, которая исходя из требуемого времени отклика, длины блока сообщения и используя выше собранную статистику, выдает рекомендуемое значение длины ключа.

Сбор статистики нужен для того что бы ускорить работу самой песочницы, когда наперед уже известны рекомендованы длины ключей, от требуемых параметров. Это позволяет не делать лишних операций, таких как генерация ключей для тестирования каждой длины ключа.

Исходный код программы находится в приложении А.

Снизу приведены графики демонтирующие результаты собранной статистики, зависимости длины ключей от времени отклика. Где на вертикальной оси − это длина ключа в битах, а на горизонтальной время шифрования и дешифрования блоков данных.

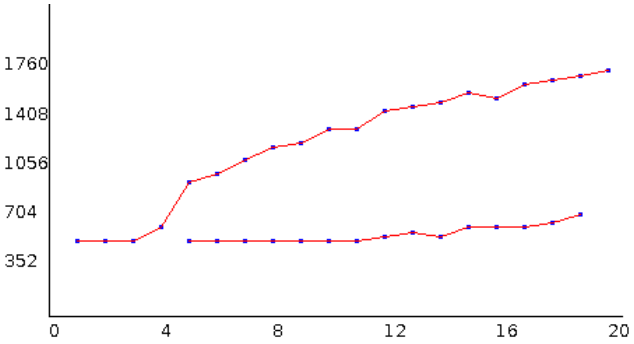

Рис. 2. График статистики для блока 5 и 40 байт

bits	data	time
544	40	1
544	40	2
608	40	3
832	40	4
960	40	5
1120	40	6
1152	40	7
1024	40	8
1312	40	9
1280	40	10
1376	40	11
1376	40	12
1504	40	13
1408	40	14
1568	40	15
1600	40	16
1632	40	17
1728	40	18
1664	40	19
1760	40	20

Табл. 1. Часть статистики

Ниже приведен второй график статистики для блока 5 Кбайт.

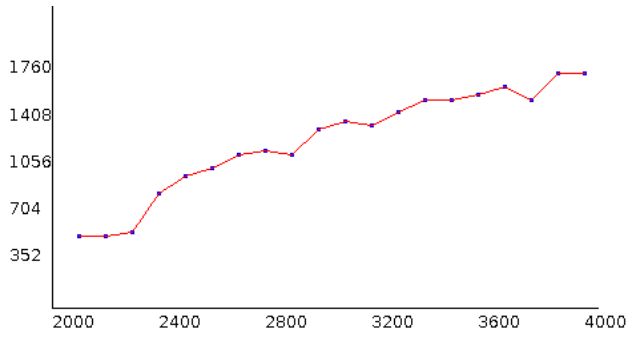

Рис. 3. График статистики для блока 5 Кбайт

Работа песочницы заключается в определении длины ключа по за-данным параметрам − размер блока и время шифрования. Например, для блока 10 байт и времени 11 мс программа выдаст 1280 бит. В программе для этого нужно ввести determineBits (11,10).

Выводы и предложения. В работе предложен способ повышения эффективности использования шифрования RSA путем определения длины ключа для требуемого времени отклика. Была

разработана соответствующая песочница. Собрана статистика зависимости длины ключа от времени шифрования, учитывая также длину блока. Проведены экспериментальные исследования. Дальнейшим перспективным развитием данной темы можно назвать улучшение работы самой криптографической системы, используя другие алгоритмы.

Список литературы:

1. В.А. Устинов, И.П. Клементьев. Введение в облачные вычисления / В.А. Устинов, И.П. Кле-ментьев // Облачные вычисления. – 2011. – № 1. – С. 1-4.
2. В.А. Устинов, И.П. Клементьев. Введение в облачные вычисления / В.А. Устинов, И.П. Кле-ментьев // Основы облачных вычислений. – 2011. – № 1. – С. 48-52.
3. J.R. Vic Winkler. Securing the Cloud: Cloud Computer Security Techniques and Tactics / J.R. Vic Winkler // Securing the Cloud– 2011. – № 1. – P. 32-43.

Баніт В.В.
Національний технічний університет України
«Київський політехнічний інститут»

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ШИФРУВАННЯ RSA В ХМАРНИХ СИСТЕМАХ

Анотація
Досліджено метод підвищення ефективності використання шифрування RSA в хмарних системах. Розроблена тестуюча програма. Проведено експериментальні дослідження.
Ключові слова: шифрування, RSA, хмарні системи, криптографія, захист інформації.

Banit V.V.
National Technical University of Ukraine
«Kyiv Polytechnic Institute»

IMPROVED UTILIZATION OF RSA ENCRYPTION IN THE CLOUD SYSTEMS

Summary
Studied a method for increasing the efficiency of use of RSA encryption in cloud systems. Designed test program. Experimental studies.
Key words: encryption, RSA, cloud systems, cryptography, information security.

УДК 534.14:535

ЗАЛЕЖНІСТЬ ПРУЖНИХ КОЛИВАНЬ ПАКЕТУ ВІД ОПТИЧНИХ ХАРАКТЕРИСТИК ВНУТРІШНЬОГО ШАРУ ПРИ ФТА ПЕРЕТВОРЕНІ

Богданов О.В.
Національний технічний університет України
«Київський політехнічний інститут»

Проведено аналіз залежності амплітуди та фази стаціонарного пружного коливання тонкого тришарового пакету. Фізичні властивості внутрішнього шару відрізняються від характеристик зовнішніх шарів лише значенням оптичного коефіцієнту поглинання. Зовнішні шари пакету виконані з однакового матеріалу. Постановка задачі виконана в рамках теорії незв'язаної термопружності.
Ключові слова: тришаровий пакет, фототермоакустичне (ФТА) перетворення, пружні коливання, оптичний коефіцієнт поглинання.

Вступ. Ефект фототермоакустичного (ФТА) перетворення знайшов застосування при дефектоскопії тонкошарових виробів, наприклад, в мікроелектроніці. З теоретичної сторони, на сучасному етапі існує велика кількість робіт, які присвячені питанню періодичного у часі ФТА перетворення [1, 2]. Слід також зауважити, що дослідники зазвичай цікавляться лише пружно-деформованим станом на «тіньовій» поверхні об'єкта (термооптична генерація звукових хвиль [3]).

Слід зазначити, що в присутніх, у відкритому доступі, дослідженнях відсутній аналіз параметрів пружних коливань від певних фізичних властивостей матеріалу. Цей недолік є дуже суттєвим для задач дефектоскопії, оскільки «дефектний» внутрішній шар може відрізнятися, від оточуючого матеріалу, лише певними параметрами. Тому, метою представленої роботи є аналіз залежності пружних коливань від фізичних властивостей внутрішнього шару. Зокрема, в рамках даної статті, розглянуто