6. <https://ru.bmstu.wiki/>
7. <https://ru.wikipedia.org/wiki/>
8. <https://www.securitylab.ru/analytics/>
9. <https://habr.com/ru/post/151599/>
10. Панасенко, С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ – Петербург, 2009. – 576 с.
11. Наумов Р. В. Информационная безопасность. Методы шифрования // I Международная научно-практическая конференция «Научные исследования: ключевые проблемы III тысячелетия» 1(1), 2016.

Жукова М.В., Супруненко Д.В.

Понятие асимметричного шифрования. Протокол RSA

РТУ МИРЭА

(Россия, Москва)

doi: 10.18411/lj-04-2019-230

idsp: ljjournal-04-2019-230

Аннотация

Искомая статья дает свое представление об понятии асимметричного шифрования, а также рассматривает его использование на примере протокола RSA. Здесь представлена общая структура алгоритма, включающая в себя математическое описание и особенности программной реализации. Также статья рассказывает о поэтапном «математическом» создании алгоритма RSA.

Ключевые слова: шифрование, асимметричное шифрование, открытый ключ, закрытый ключ, протокол RSA, «атака среднего», модульная арифметика, односторонняя функция с секретом, теорема Эйлера, алгоритм разложения больших чисел на простые множители.

Abstract

This article gives understanding about concept of asymmetric encryption and considers the use of this term taking RSA key exchange as an example. Its overall structure, including background of math description and specificities of the software, is represented here. Also article tells to readers about mathematical process of establishing the RSA key exchange step by step.

Keywords: encryption, asymmetric encryption, public key, private key, RSA key exchange, «man in the middle» (MITM), modular arithmetic, trapdoor function (TDF), Euler's Theorem, factorization algorithm.

1. Немного об асимметричном шифровании

До начала 1970 года криптография основывалась на симметричных ключах, то есть отправитель (Алиса) шифровал свои сообщения, используя при этом специальный ключ, а получатель (Боб), в свою очередь, расшифровывал послание с помощью идентичного ключа.

Как уже было сказано ранее, шифрование – процесс сопоставления сообщения зашифрованному сообщению с применением определенного ключа. Чтобы расшифровка текста сообщения стала возможной, необходимо использовать тот же самый ключ, которым было произведено шифрование. То есть для ведения защищенной приватной беседы между знакомой нам парой, Алиса и Боб должны изначально договориться об общих одинаковых ключах. Такая договоренность на практике зачастую невозможна, если собеседники не могут физически встретиться, или же необходимы некоторые дополнительные затраты на связь, как, например, при использовании обмена по Диффи-Хеллману.

В дополнение ко всему, если отправителю (Алисе) необходимо вести диалог с несколькими собеседниками, как если бы он был нечто *вроде банка ключей*, то ему бы

пришлось обмениваться отдельными ключами каждым из них (рис.1.1). Поэтому возникает необходимость каким-либо образом управлять этим набором ключей, например, с помощью упаковки сообщений для определения принадлежности ключа адресату. Основной недостаток такого подхода заключается в том, что собеседников может быть более 1000, и, соответственно, сообщений нужно будет отправить не меньшее количество исключительно ради идентификации.

Рис.1.1. Обмен с помощью «закрытого шифрования»

Более простой способ придумал британский инженер и математик Джеймс Эллис (англ. James Ellis). Он подал идею открытого шифрования, о которой уже говорилось ранее. Эта идея была основана на следующем подходе (рис.1.2): пусть отправитель (Алиса) имеет некоторое количество абсолютно одинаковых замков. Очевидно, что ко всему множеству идентичных замков одинаково точно подойдет один единственный ключ, который бы хранился у отправителя (Алисы). Алиса отправляет первый открытый замок адресату, например, Бобу. Получатель, в свою очередь, записывает сообщение, закрывает замок и отправляет его обратно Алисе, которая спустя некоторое время будет иметь некоторое множество закрытых замков. В таком случае, отправитель будет собой являть не банк ключей, а *банк замков*, открыть которые можно только тем самым единственным ключом. Следовательно, что никакого обмена ключами происходит не будет, а также можно позволить кому угодно в мире распространять сам замок и позволить отправлять сообщения.

Рис.1.2. Обмен с помощью «открытого шифрования»

Применение шифрования с помощью открытого ключа позволяет следующее:

- избавиться от необходимости использования секретных каналов связи для предварительного обмена ключами;
- свести проблему взлома к решению сложных задач (например, проблема дискретного логарифмирования), т.е. создать новое течение в вопросе стойкости криптосистемы;
- создать возможность для решения не только задачи по шифрованию данных, но и для, например, обеспечения юридической значимости документов (подтверждение авторства сообщений с помощью ЭЦП – электронно-цифровая подпись).

Последнее означает, что возможно использовать криптосистемы с совершенно другой целью. Это является необходимостью для лиц, управляющими дистанционно некоторыми видами ресурсов хозяина имущества. Сейчас данная задача стала еще более актуальной в виду развития электронной коммерции.

2. Реализация алгоритма. Математическая подоплека.

К сожалению, Эллис не предоставил физической реализации подхода, описанного выше, но внес интуитивное понимание основных принципов его работы. Сама идея основывается на разделении ключа на две составные и взаимозависимые части: *ключ шифрования* и *ключ дешифрования*.

Математическое решение было предложено другим британским математиком и шифровальщиком Клиффордом Коксом (англ. Clifford Cocks). Он поставил во главе стола следующую задачу: спроектировать особый вид односторонней функции – *односторонняя функция с секретом*. Она представляет из себя функцию, которая легко вычисляется в одном направлении и сложно в другом *при незнании специальной информации* – секрета (рис.1.3).

Рис.1.3. Пример односторонней функции с секретом.

Такую функцию возможно реализовать при использовании следующей математической операции: возведение в степень по модулю, представленное выражением (3). Здесь « m » – исходное сообщение, « e » – степень, « mod » – оператор, возвращающий остаток от деления двух чисел, « N » – большое простое число, « c » – полученное зашифрованное сообщение.

$$m^e \bmod N \equiv c \quad (3)$$

В данном случае $m^e \bmod N$ – пример математического замка, которой используется всеми, кто хочет отправить сообщение Алисе.

Если есть типовой замок, то в соответствии с алгоритмом требуется разработать пару ключей: ключ шифрования и ключ расшифровки. Для этого Кокс предложил возвести « c » в некоторую другую степень « d », которая бы отменяла действия, произведенные над « m » (4). Если совместить выражения (3) и (4), то получим следующее (5):

$$c^d \bmod N \equiv m \quad (4)$$

$$m^{ed} \bmod N \equiv m \leftrightarrow m^{ed} \bmod N \equiv m \quad (5)$$

Тем самым, мы получили *ключ шифрования* – « e » и *ключ расшифровки* « d ». Тогда встает следующий вопрос: каким образом выбрать « c » и « d », чтобы злоумышленникам было сложно подобрать « d ». Кокс предположил, что ответом на данный вопрос будет являться другая *односторонняя функция*, которая бы генерировала это « d ». Для этого он обратился к Евклиду и его основополагающей идее о том, что *любое число единственным образом раскладывается на простые множители*, которые можно взять за основу секретных ключей. Поскольку сама по себе операция разложения на простые множители очень больших чисел фундаментально сложна.

Этот метод был немедленно засекречен после публикации и повторно независимо открыт в 1978 году Рональдом Ривестом (англ. *Ronald Rivest*), Ади Шамиром (англ. *Adi Shamir*) и Леном Адельманом (англ. *Len Adleman*). На данный момент RSA является самым широко используемым алгоритмом шифрования данных с открытым ключом в мире.

В отличие от Диффи-Хеллмана, безопасность алгоритма RSA базируется на разложении больших чисел на простые множители. Безопасность обеспечивается сложностью вычисления « d » при наличии известных « e » и « N ». Подразумевается, что владелец пары ключей сохраняет секретный ключ в тайне, а открытый ключ передается публично. Следовательно, если информация зашифрована с помощью открытого ключа, дешифровать ее может только владелец ключевой пары.

Алгоритм RSA, также, как и протокол Диффи-Хеллмана, подвержен «атаке среднего» (рис.1.5). В случае с RSA ключом, который перехватывает злоумышленник является открытый ключ « e ». Меллори получает блок сообщений « m » и ключ « e », и отправляет Бобу уже свой блок сообщений « m_2 » и ключ « e ». Аналогичная ситуация и в обратную сторону. Получается, человек в середине, Меллори, может принимать и отправлять сообщения и Алисе, и Бобу, и те, в свою очередь, ничего не заподозрят. Одним из способов борьбы с эти являются следующие процедуры: пусть Алиса и Боб пересылают друг другу открытые ключи, затем шифруют все сообщения открытыми ключами (Алиса шифрует для Боба) и пересылают половину зашифрованного сообщения. Боб шифрует для Алисы и пересылает половину сообщения. Пересылается вторая половина сообщения, соединяется и получается сообщения для расшифровки закрытым ключом.

Рис.1.5. Общая схема «атаки среднего» для RSA

При программной реализации RSA следует учесть следующее:

- Для операций с большими числами в некоторых языках программирования требуются специальный формат (например, в Java используются классы `BigInteger` и `BigDecimal`);
- Такие части алгоритма, как выбор « d » или вычисление « e », занимают очень много времени при решении задачи простым перебором. Для определения взаимно простых чисел можно использовать алгоритм Евклида;
- При шифровании блока сообщений необходимо создать алгоритм. Например, преобразовать биты строки в какое-либо число. Очевидно, что для этого необходимы операторы и библиотеки работы с битами. В Python есть библиотека `bitarray`, а в Java - метод класса `String` - `getBytes()`;
- Необходимо организовать обмен между клиентом и сервером, причём передавать данные друг другу лучше в строковом типе (который потом конвертируется в биты) для удобной конкатенации блоков сообщений впоследствии.

1. <https://www.khanacademy.org/>
2. <https://progress.online/>
3. <https://www.intuit.ru/>

4. <https://ssd.eff.org/ru/>
5. Computer security and cryptography/ Под ред. А. Conheim. - М., WILEY, 2007. – 45 с.
6. <https://ru.bmstu.wiki/>
7. <https://ru.wikipedia.org/wiki/>
8. <https://www.securitylab.ru/analytics/>
9. <https://habr.com/ru/post/151599/>
10. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ – Петербург, 2009. – 576 с.
11. Наумов Р. В. Информационная безопасность. Методы шифрования // I Международная научно-практическая конференция «Научные исследования: ключевые проблемы III тысячелетия» 1(1), 2016.
12. Авдошин С.М., Савельева А.А. Криптографические методы защиты информационных систем. – 2007. – УДК 004.056.55 – С. 91-99.

Запылихин Ю.С., Андрианова Л.П.

Гибридная электростанция на базе возобновляемой энергии ветра и солнца для энергоснабжения децентрализованных потребителей

*ФГБОУ ВО «Уфимский государственный
нефтяной технический университет»
(Россия, Уфа)*

doi: 10.18411/lj-04-2019-231

ids: lj-04-2019-231

Аннотация

В статье приведены результаты исследований гибридной электростанции для децентрализованного энергоснабжения удаленных потребителей, в состав которой входят ветровая, солнечная и дизельная установки. Основными источниками электроэнергии являются ветровая и солнечная установки, а дизельная установка используется в качестве резервного источника.

Ключевые слова: децентрализованное энергоснабжение, удаленный потребитель, гибридная электростанция, возобновляемые источники энергии, ветрогенератор, фотоэлектрический модуль, инвертор

Abstract

The article presents the results of studies of a hybrid power plant for decentralized power supply to remote consumers, which includes wind, solar and diesel installations. The main sources of electricity are wind and solar installations, and the diesel installation is used as a backup source.

Keywords: decentralized power supply, remote consumer, hybrid power plant, renewable energy sources, wind generator, photovoltaic panel, inverter

К децентрализованным потребителям электроэнергии относятся объекты, имеющие малую потребляемую мощность и (или) находящиеся на значительном удалении от централизованной (национально/региональной) электрической сети, и подключение к ней экономически невыгодно [1].

Для энергоснабжения таких потребителей перспективным является создание гибридных электростанций на основе возобновляемых источников энергии (ветра и солнца), производство которых не требует высокотехнологического оборудования.

Для энергоснабжения децентрализованных потребителей предлагается гибридная электростанция малой мощности, состоящая из ветровой, дизельной и солнечной установок. Дизельная установка может подключаться напрямую к нагрузке или к локальной сети постоянного тока при отсутствии благоприятных погодных условий для работы ветровой и солнечной установок, что обеспечивает энергетическую безопасность потребителей.

Гибридная электростанция на базе возобновляемых источников энергии ветра и солнца благодаря инвертору на выходе электроустановки обеспечивает требуемое качество электрической энергии и легко масштабируется. [2]