Жукова М.В., Супруненко Д.В.
Понятие шифрование данных. Протокол Диффи-Хеллмана

РТУ МИРЭА
(Россия, Москва)

doi: 10.18411/lj-04-2019-229

idsp: ljjournal-04-2019-229

Аннотация

Статья посвящена ознакомлению с понятием «криптография» и его видами. Вниманию читателя представляется структура функционирования шифрования на примере общения нескольких абонентов по незащищенному каналу связи. Также приведен пример одного из криптографических алгоритмов (алгоритм Диффи-Хеллмана) с математическим обоснованием используемых процессов и с некоторыми особенностями программной реализации.

Ключевые слова: криптография, шифрование, асимметричное шифрование, симметричное шифрование, открытый ключ, закрытый ключ, алгоритм Диффи-Хеллмана, «атака среднего», модульная арифметика, односторонняя функция.

Abstract

This article devotes to reviewing the concept of cryptography with its types. Communication of two subscribers via insecure channels shows functioning of cryptography which introduces to readers' attention. Also this article gives the example of some encryption algorithm (Diffie–Hellman's algorithm) using some elements of the software and basing on mathematical foundations drawing encryption process.

Keywords: cryptography, encryption, asymmetric encryption, symmetrical encryption, public key, private key, Diffie–Hellman key exchange, «man in the middle» (MITM), modular arithmetic, one-way function.

1. Введение: о сложном просто.

Так или иначе люди испокон веков применяли различные способы сокрытия важной информации. Но только относительно недавно криптография – наука о способах защиты информации – действительно смогла добиться огромных успехов: «Цивилизация велит идти вперед: теперь прогресс с собой и черта двинул». Обусловлен этот баснословный прогресс двумя следующими факторами: повсеместное внедрение технологий в нашу повседневную жизнь и ее неукротимое развитие, а также «приоткрытие» завесы тайны на криптографические способы или алгоритмы, используемые для защиты информации. Как известно, использование шифрование решает одну из самых распространенных проблем и тех времен, и сегодняшнего дня – сохранение конфиденциальности информации. Посему стоит начать исследование вопроса криптографии с самого начала, а именно с определения.

Представим себе ситуацию, в которой два оппонента, Алиса и Боб, хотят передать на расстоянии друг другу некоторую важную приватную информацию (рис.1.1). Однако, их подслушивает некая Ева, которая не только жаждет получить это секретное сообщение, но и обладает возможностями для его перехвата. В сложившейся ситуации Алиса предпринимает следующий шаг: использование некоторого «секретного кода» для написания своего сообщения.

Очевидно, что логика такого вида общения заключена в обмене приватной информацией на дистанции с использованием некоторого «секрета» для того, чтобы данные не попали в чужие руки.

Следующая аналогия будет полезной для понимания логики такого рода обмена (рис.1.1): Алиса пишет исходное сообщение, запирает его с помощью такого замка, «ключ» к которому имели бы только она и Боб. Этот процесс называется шифрованием. Затем Алиса отправляет коробку с сообщением Бобу. Поскольку коробка с сообщением будет находиться в открытом доступе то ее также получит подслушивающая их Ева.

Поскольку Боб имеет «ключ» от замка на коробке, который получил заблаговременно от Алисы, поэтому он с легкостью получает исходное сообщение. Этот процесс называется дешифрованием.

Рис.1.1. Обобщённая схема передачи информации.

В свою очередь, Ева открыть коробку с данными не может, поскольку с ней никто не поделился необходимым для этого «ключом».

В общем случае, под *шифрованием* или *криптографией* подразумевают способ сокрытия данных, при котором информация преобразовывается в другую форму или код таким образом, что доступ к ней имеет только пользователь с секретным ключом (ключ дешифрования).

Криптография всегда шла бок о бок с развитием человечества, зачастую решая исход войны. До начала XVI века существовала наивная криптография, для которой характерно использование примитивных способов запутывания противника касательно содержания передаваемых сообщений (шифр Цезаря, полибианский квадрат, диск Энея и т.д.). По прошествии веков с развитием технологий шифрование приняло совсем другой вид, все яростнее и глубже интернируясь в жизнь современного человека, тем самым, становясь ядром всемирного общения и передачи данных посредством сети.

2. Виды шифрования данных. Ассиметричное шифрование.

На сегодняшний день шифрование данных значительно усложнилось и является одним из самых популярных и эффективных методов защиты. Существуют следующие два типа шифрования данных:

- *Ассиметричное* (с открытым ключом, «двухключевая») – два ключа: один для шифрования данных, другой – для дешифровки;
- *Симметричное* (с закрытым ключом, «одноключевая», классическая) – только один ключ: используется как для шифрования данных, так и для дешифровки.

Технология ассиметричного шифрования является более поздней и на данный момент встречается наиболее часто.

Общую схему шифрования с открытым ключом можно описать с помощью обмена сообщениями между уже знакомыми нам Алисой и Бобом (рис.1.2). И Алиса, и Боб должны иметь свой персональный ключ, который был бы связан с другим. Такие ключи называют *парой ключей*, основная особенность которой заключается в том, что информация, зашифрованная одним ключом (ключом Алисы), может быть расшифрована только с использованием второго ключа (ключа Боба) из этой пары. Обратное утверждение тоже верно: если данные зашифрованы посредством использования ключа Боба, то расшифровка информации возможна только с помощью ключа Алисы.

Рис.1.2. Обобщенная схема асимметричного шифрования.

На практике в такой паре один ключ именуют секретным или приватным, а другой – открытым или публичным. Если важно обеспечить конфиденциальность, шифрование выполняется с открытым ключом. Правильно и корректно расшифровать информацию можно только зная нужный открытый ключ, передаваемый в открытом виде, поэтому только владелец пары ключей может отправлять данные (сообщения).

Конечной целью шифрования является обеспечение конфиденциальности данных, в том числе цифровых. Рассмотрим один из самых часто встречаемых протоколов шифрования данных – протокол Диффи-Хеллмана.

3. Протокол Диффи-Хеллмана

Определение: Протокол Диффи-Хеллмана (DH) — криптографический протокол, позволяющий двум и более сторонам получить общий секретный ключ, используя незащищенный от прослушивания канал связи. Полученный ключ используется для шифрования дальнейшего обмена с помощью алгоритмов симметричного шифрования.

Передача ключа по открытым каналам была большой проблемой криптографии XX века. К решению данной проблемы наиболее близко удалось подойти британским математикам Уитфилду Диффи (англ. Whitfield Diffie) и Мартину Хеллману (англ. Martin Hellman), которые разработали свою систему шифрования (алгоритм) с открытым ключом в 1976 г. Данный алгоритм позволил дать ответ на главный вопрос: «Как при обмене зашифрованными сообщениями избежать необходимости передачи секретного кода расшифровки?»

Основная идея алгоритма заключалась в применении безопасного метода согласования секретного ключа без его передачи каким-либо другим способом. Следовательно, нужно найти безопасный способ получения секретного ключа с помощью того же метода связи, для которого разрабатывалась защита.

На уже знакомом нам примере эта идея выглядит следующим образом: Алиса и Боб обмениваются сообщениями по каналу, который прослушивается (каждое сообщение перехватывается Евой). Секрет состоит в выборе общего секретного ключа и в невозможности получения Евой его копии.

Чтобы воплотить эту идею с числами, требовалось найти такую численную процедуру, которая будет простой для вычисления в одну сторону и сложной в обратную. Это подводит нас к теме *модульной арифметики* или часовой арифметики и к понятию *односторонней функции*.

Рассмотрим следующее выражение (1), где « A » – генератор (число, которое в последствии будем возводить в степень), « P » – большое простое число, « mod » – оператор, возвращающий остаток от деления двух чисел (например, $15 \bmod 10 \equiv 5$, где 5 – остаток от деления 15 на 10), « N » – результат.

$$A \bmod P \equiv N \quad (1)$$

Чтобы вычисления были корректными, необходимо брать простое число для модуля (число, имеющее ровно два различных натуральных делителя — единицу и самого себя). Например, пусть $P=17$. Теперь возьмем первообразный корень этого простого числа – 3 ($A=3$). У числа «3» есть важное свойство: если возводить его в разные степени по модулю 17, то ответ равномерно распределится от 1 до 16, т.е. мы получим в результате числа 1, 2, 3, ..., 16 с равной вероятностью (2).

$$3^x \bmod 17 \equiv 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16 \quad (2)$$

Другими словами, вычислить выражение (2) легко, а произвести обратную процедуру очень сложно. Это и будет нашей односторонней функцией, т.е. математической функцией, которая легко вычисляется для любого входного значения, но трудно найти аргумент по заданному значению функции (рис.1.3). Уровень безопасности системы зависит от сложности нахождения «х», степени генератора «А». В этом и заключается проблема дискретного логарифмирования, которую с помощью современного вычислительного оборудования решить практически невозможно. Именно на этой идее основывается алгоритм Диффи-Хеллмана для обеспечения конфиденциальности.

Рис.1.3. Пример односторонней функции

Крепость односторонней функции выражается в количестве времени, которое требуется для обратного решения поставленной задачи.

Используя маленькие числа, подобрать «х» – легко, но, если использовать для модуля простое число длиной в сотни цифр – это становится по-настоящему сложно. Даже используя абсолютно весь созданный вычислительный потенциал, процесс вычисления может занять минимум десятки лет, а то и намного больше.

Перейдем к рассмотрению самого алгоритма и для начала ответим для себя на основные вопросы:

1. Кто обменивается? – **Алиса, Боб;**
2. Кто прослушивает? – **Ева;**
3. Что является публичными данными?
 - **A** – генератор;
 - **P** – большое простое число;
 - **Y1** и **Y2** – открытые ключи Алисы и Боба соответственно.
4. Что является секретными данными?
 - **x1** – приватное число Алисы;
 - **x2** – приватное число Боба;
 - **K** – общий секретный ключ Алисы и Боба.

Также при организации этого алгоритма нужно учесть следующие условия:

- $P = 2q + 1$, q – простое число;
- A и q – взаимнопростые числа (нет общих делителей, кроме 1);
- $x1, x2 < P$;
- Для $\forall A$ выполняется следующее: $1 < A < P - 1$ и $A^x \bmod P \neq 1$.

Общая схема и поэтапное описание алгоритма Диффи-Хеллмана представлена на рис.1.4.

Тем не менее, протокол Диффи-Хеллмана хоть и отлично выдерживает «пассивные атаки», но в случае реализации атаки «человек посередине» («атака среднего») он устоять не может (рис.1.5). В самом деле, в протоколе ни Алиса, ни Боб не могут достоверно установить, кем является их собеседник. Посему вполне возможна ситуация, при которой Алиса и Боб установили связь с неким Меллори, который представился Алисе Бобом, а Бобу выдает себя за Алису. И спустя некоторое время этот Меллори может получить общий ключ с Алисой, которая думает, что это Боб, и

общий ключ с Бобом, считаящий, что его собеседник – Алиса. Такая связь долгое время может оставаться незамеченной. Один из способов борьбы – использование ЭЦП (электронной цифровой подписи) или протокола MQV (модифицированный протокол Диффи-Хеллмана).

Рис.1.4. Общая схема алгоритма Диффи-Хеллмана.

Рис.1.5. Реализация атаки «человек посередине»

При программной реализации протокола Диффи-Хеллмана следует учесть следующие моменты:

- Для операций с большими числами в некоторых языках программирования требуются специальный формат (например, в Java используются классы BigInteger и BigDecimal);
- Проверка и выбор A будет занимать много времени, если решать задачу простым перебором. Для оптимизации можно использовать какие-либо алгоритмы, один из которых алгоритм Евклида;
- Необходимо организовать обмен между клиентом и сервером так, чтобы клиент и сервер могли обмениваться несколькими сообщениями (для этого в Java, например, можно использовать библиотеку «netty»). Для определения стадии алгоритма и того, какую информацию нужно обработать, можно в начало сообщения добавлять метки. По меткам же клиент и сервер будут определять, что именно нужно сделать.

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. A. 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.

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