ОБМЕН СЕКРЕТНЫМ КЛЮЧОМ ПО ОТКРЫТОМУ КАНАЛУ СВЯЗИ

Прудковский Н. С.

Прудковский Николай Сергеевич / Prudkovskiy Nikolay Sergeevich – студент,
кафедра ИУ8 информационной безопасности, факультет информатики и систем управления,
Московский государственный технический университет им. Н. Э. Баумана, г. Москва

Аннотация: *в данной статье описывается алгоритм обмена ключом по открытому каналу связи (именно благодаря этой идее возник целый класс криптографии – асимметричное шифрование, являющийся фундаментальной частью современной криптографии). Объясняется принцип работы такого алгоритма на примере алгоритма Диффи-Хеллмана. Также выявляются положительные и отрицательные стороны асимметричного шифрования. Для простоты понимания сами алгоритмы шифрования не приводятся, разбирается только последовательность обмена ключом. Эта статья будет полезна читателям, которым непонятен принцип работы обмена секретным ключом по открытому каналу связи.*
Ключевые слова: *криптография, асимметричность, обмен ключом.*

Введение

Безопасное общение пользователей по открытому каналу всегда являлось одной из фундаментальных проблем криптографии. Чтобы сообщения можно было зашифровать и расшифровать, необходимо обеим сторонам иметь общий ключ. Если ключ передавать по открытому каналу, то прослушивающая сторона тоже получит доступ к зашифрованной информации и смысл шифрования пропадает.

Постановка задачи

Итак. Допустим, нам требуется от кого-то получить некие данные. Мы с вами не хотим, чтобы эти данные узнало какое-то третье лицо. И у нас нет никакой уверенности в том, что канал передачи данных не прослушивается. Приступим.

Немного истории

Криптография прошлых веков имела одну огромную проблему — проблема передачи ключей. В те времена существовали только так называемые «симметричные» шифры — шифры, при котором данные шифруются и расшифровываются одним и тем же ключом.

До 70-х годов, эта проблема настолько стала привычной, что считался аксиомой тот факт, что для передачи сообщения нужно передавать и сам ключ, которым расшифровывается сообщение.

Исторически первой системой с открытым ключом стал метод экспоненциального ключевого обмена Диффи-Хеллмана, разработанный в 1976 году. Метод предназначен для передачи секретного ключа симметричного шифрования. Именно Диффи и Хеллман опровергли устоявшуюся аксиому о невозможности передачи шифрованных сообщений через открытый канал, и с этого момента началось развитие асимметричных криптосистем.

Асимметрическое шифрование в реальной жизни

Давайте представим, как работает алгоритм подобного шифрования на простом жизненном примере [1, 291].

1. *Алиса кладет свое письмо в ящик и, заперев его на замок, отправляет Бобу.*
2. *Боб получает ящик, берет свой замок и, дополнительно заперев им ящик, отправляет обратно.*
3. *Алисе приходит ящик с двумя замками (с первым замком Алисы, от которого у нее есть ключ, и со вторым — Боба, от которого ключ есть только у Боба).*
4. *Алиса снимает свой замок, и отправляет ящик обратно Бобу.*
5. *Бобу приходит ящик с уже одним его замком, от которого у него есть ключ.*
6. *Боб отпирает оставшийся его замок своим ключом и читает сообщение.*

Вернемся к криптографии

Казалось бы, решение найдено. Отправитель и принимающий шифруют свое сообщение, и затем собеседники поочередно снимают свой шифр.

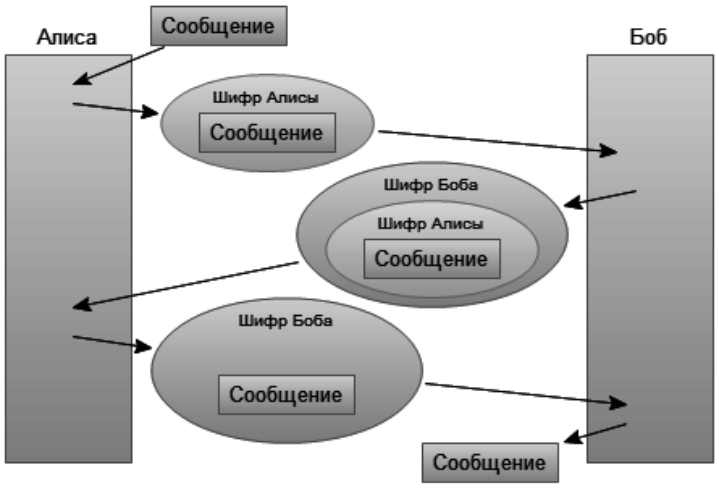

Рис 1. Пример с ящиком в реальности

Но суть в том, что не существуют таких шифров, которые бы позволили снять шифр из-под другого шифра. То есть этап, где Алиса снимает свой шифр, невозможен:

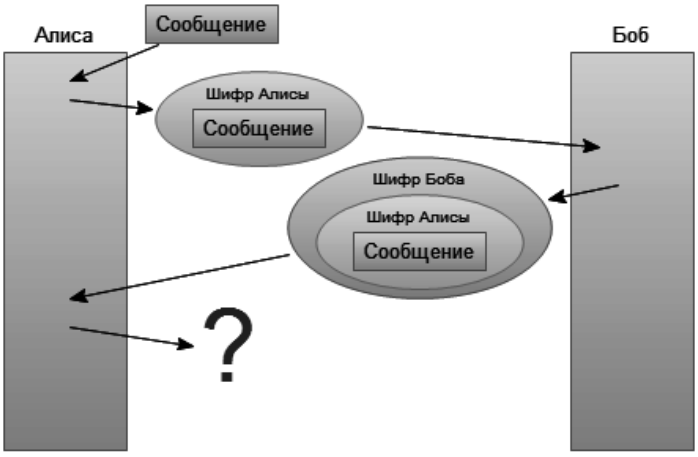

Рис 2. Как на самом деле при шифровании

Алгоритм Диффи-Хеллмана [1, 274]

Идея с ящиком вдохновили Диффи и Хеллмана искать способ передачи подобного вида сообщения. В итоге они пришли к использованию односторонних функций.

Объясню на примере. Имеется функция удвоение, т.е. **удвоить(5)=10**, она двухсторонняя, т.к. из результата 10 легко получить исходное значение 5. Односторонняя функция — та функция, после применения которой практически невозможно получить исходное значение. К примеру, смешивание желтой и синей краски — пример односторонней функции. Смешать их **легко**, а вот получить обратно исходные компоненты **невозможно**. Одна из таких функций в математике — **вычисление по модулю.**

За основу алгоритма Хеллман предложил функцию $\boldsymbol{Y^x(mod\ P)}$. Обратное преобразование для такой функции очень сложно, и можно сказать что, заключается в полном переборе исходных значений.

К примеру вам сказали, что$\boldsymbol{7^x(mod\ 11) = 2}$. Найдите **x**. Как видите, вы начинаете перебирать варианты. А теперь представьте что за Y и P взяты числа порядка $\boldsymbol{10^{200}}$.

Стоит добавить, что для повышения стойкости, число P должно быть простым, а Y - являться первообразным корнем по модулю P.

Теперь пошагово приведу сам алгоритм опять же на примере Алисы и Боба:

Таблица 1. Алгоритм Диффи-Хеллмана

	Алиса	**Боб**
Этап 1	Оба участника договариваются о значениях **Y** и **P** для общей односторонней функции. Эта информация не является секретной. Допустим, были выбраны значения **7** и **11**. Общая функция будет выглядеть следующим образом: **7x (mod 11)**	

Этап 2	Алиса выбирает случайное число, например **3**, хранит его в секрете, обозначим его как число **A**	Боб выбирает случайное число, например **6**, хранит его в секрете, обозначим его как число **B**
Этап 3	Алиса подставляет число **A** в общую функцию и вычисляет результат $\mathbf{7^3(mod\ 11) = 343(mod\ 11) = 2}$, обозначает результат как **a**	Боб подставляет число **B** в общую функцию и вычисляет результат $\mathbf{7^6(mod\ 11) = 117649(mod\ 11) = 4}$, обозначает результат как **b**
Этап 4	Алиса передает число **a** Бобу	Боб передает число **b** Алисе
Этап 5	Алиса получает **b** от Боба и вычисляет значение $\boldsymbol{b^A(mod\ 11) = 4^3(mod\ 11) = = 64(mod\ 11) = 9}$	Боб получает **a** от Алисы и вычисляет значение $\boldsymbol{a^B(mod\ 11) = 2^6(mod\ 11) == 64(mod\ 11) = 9}$
Этап 6	Оба участника в итоге получили число 9. Это и будет являться ключом.	

Хотел бы обратить ваше внимание, что для получения ключа в конечной формуле любому человеку нужно иметь три значения:

- Значения **a** и **P**, и секретное число Боба **B.**
- Или же значения **b** и **P**, и секретное число Алисы A.

Но секретные числа по каналу не передаются! Еве не получится восстановить ключ, не имея чьего-нибудь секретного числа.

Плюсы и минусы асимметрического шифрования

Криптостойкость этого шифрования определяется трудоемкостью вычисления дискретного логарифма в конечном поле. Действительно, злоумышленник может узнать такие параметры алгоритма, как a, b, Y и P, но вычислить по ним значения x или y (секретные ключи Боба и Алисы) – задача, требующая очень больших вычислительных мощностей и времени.

Недостатков у этого метода немного (в отличие от симметричного шифрования [**Ошибка! Источник ссылки не найден.**, 163]), но все же стоит о них упомянуть.

Первый недостаток ассиметричного шифрования заключается в низкой скорости выполнения операций зашифровки и расшифровки, что обусловлено необходимостью обработки ресурсоемких операций. Как следствие, требования к аппаратной составляющей такой системы часто бывают неприемлемы.

Другой недостаток – уже чисто теоретический, и заключается он в том, что математически криптостойкость алгоритмов асимметричного шифрования пока еще не доказана.

Дополнительные проблемы возникают и при защите открытых ключей от подмены, ведь достаточно просто подменить открытый ключ легального пользователя, чтобы впоследствии легко расшифровать его своим секретным ключом [2, 388].

Заключение

В конце статьи хотелось бы добавить, что алгоритм шифрования считается стойким до тех пор, пока не будет доказано обратное. Поэтому все алгоритмы с ростом вычислительных мощностей устаревают и заменяются новыми. Однако на сегодняшний день асимметрическое шифрование не потеряло своей актуальности (до сих пор не было найдено серьезных уязвимостей) и пользуется большим спросом в IT-сфере.

Литература

1. *Сингх С.* Книга шифров. Тайная история шифров и их расшифровки. М.: Аст, Астрель, 2006. 447 с.
2. *Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В.* Основы криптографии. М.: Гелиос АРВ, 2001. 479 с.
3. *Шнайер Б.* Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2003. 806 с