***Защита от атаки человек посередине путем применения алгоритма RSA.***

Автор: Гладков Никита Николаевич.

Россия, Екатеринбург, Уральский государственный университет путей сообщения.

e-mail: nekitgladkov@gmail.ru

Краткие сведения из теории.

Алгоритм Диффи-Хеллмана был изобретен в 1976 году. Этот алгоритм позволяет двум сторонам получить общий секретный ключ, используя открытый канал связи. Отсюда выходит проблема атаки, называемой «человек посередине». Суть ее заключается в том, что криптоаналитик, прослушивающий канал связи, может различными методами расшифровать информацию, передаваемую по каналу.

Моя идея состоит в том, что при шифровании сообщения, закодированного при помощи алгоритма Диффи-Хеллмана, алгоритмом RSA, можно будет защитить информацию от взлома.

Рассмотрим данный вариант. Мы знаем, что шифрование RSA, основывается на вычислительной сложности задачи факторизации больших чисел и использует публичные и приватные ключи. Так как криптоаналитик, имеющий доступ к каналу связи не может узнать секретный ключ, он не сможет расшифровать посланные сообщения.

В данном случае общение по открытому каналу будет более безопасно, чем при шифровании с помощью алгоритма Диффи-Хеллмана.

Приведем пример.

Есть две стороны. Назовем их Алиса и Боб. Есть криптоаналитик – злоумышленник.

Алиса и Боб хотят обменяться информацией по открытому каналу. При этом они используют шифрование Диффи-Хеллмана. Алиса придумывает публичные p – случайное простое число и g – первообразный корень по модулю p. Также она придумывает случайное натуральное число a —закрытый ключ. А Боб в свою очередь придумывает случайное натуральное число – закрытый ключ. Затем Алиса вычисляет открытый ключ .



Если отправить этот ключ Бобу, то есть вариант, что злоумышленник может высчитать a.

Поэтому предлагается ключ зашифровать при помощи алгоритма RSA.



Тогда Боб генерирует два различных случайных простых числа и , вычисляет их произведение , которое называется модулем. Вычисляет значение функции Эйлера от числа : . Затем выбирает целое число , удовлетворяющую условию . И вычисляет число .



Пара публикуется в качестве открытого ключа RSA, а пара является закрытым ключом RSA и держится в секрете.



Алиса узнает и , и шифрует . Получается сообщение . Сообщение отправляется Бобу.



Злоумышленник, прослушивающий канал связи не может расшифровать сообщение , не зная ключа . Информация доходит до Боба. При помощи ключа Боб узнает содержимое сообщения , а при помощи узнает секретный ключ . Теперь остается, чтобы Алиса узнала этот секретный ключ. Получается ситуация, аналогичная предыдущей. Боб, используя публичные и , получает . В свою очередь Алиса придумывает новые , и , получает и . Используя и , полученные от Алисы, Боб получает сообщение



Алиса получив это сообщение, аналогично получает секретный ключ. Теперь Алиса и Боб могут обмениваться сообщениями по данному каналу, не опасаясь атаки.

В общем получается, что при использовании дополнительного шифрования алгоритмом RSA, злоумышленник не может взломать сообщение с секретным ключом и информация передаваемая Алисой и Бобом будет защищена.

Приведем пример, взяв небольшие числа для простоты решения.

Алиса генерирует



Получает



Отправляет Бобу



Боб, в свою очередь, используя получает .



Затем для шифрования с помощью алгоритма RSA, Боб генерирует



Из них он получает:



Боб отправляет пару Алисе. С помощью этой пары, Алиса зашифровывает и отправляет его в виде сообщения *.*



.



И отправляет его обратно Бобу.

Боб при помощи получает .



Далее Алиса генерирует



Из них он получает:



Алиса отправляет пару Бобу. С помощью этой пары, Боб зашифровывает и отправляет его в виде сообщения *.*



.



Аналогично Алиса при помощи получает .



В зависимости от полученного результата следует вывод, что при использовании в алгоритме RSA более длинных значений , можно без опаски обменяться данными для получения общего ключа.



Список литературы:

1. Венбо Мао, Современная криптография. Теория и практика. Вильямс, 2005.
2. Википедия, свободная энциклопедия / RSA. 15.11.2012. URL: <http://ru.wikipedia.org/wiki/RSA> (дата обращения: 20.10.2012)
3. Википедия, свободная энциклопедия / Алгоритм Диффи-Хеллмана. 9.10.2012. URL: [http://ru.wikipedia.org/wiki/Алгоритм\_Диффи - Хеллмана](http://ru.wikipedia.org/wiki/Алгоритм_Диффи%20-%20Хеллмана) (дата обращения: 20.10.2012)
4. Сайт «Информационная безопасность: практика информационной безопасности». Домен 6. Криптография. Часть 4. URL: <http://dorlov.blogspot.ru/2010/09/issp-06-4.html> (дата обращения: 22.10.2012)
5. Сайт e-nigma. Алгоритм шифрования RSA. 2006-2012. URL: <http://www.e-nigma.ru/stat/rsa> (дата обращения: 3.11.2012)