Обмен ключами

Важно иметь ключ шифрования, который известен только тому, кто шифрует данные, и тому, кто их расшифровывает. Но здесь возникает логистическая проблема, особенно когда нам нужно зашифровать большой объём данных в интернете: как передать ключ шифрования между этими двумя людьми, не передавая его физически через небезопасную среду, такую как интернет?

Один из способов сделать это — передать ключ вне сети, то есть мы не будем использовать сеть. Это значит, что нам нужно найти другой способ передачи ключа из одного места в другое. Представьте себе человека с чемоданом, на котором надеты наручники. Он садится в поезд. Он едет через всю страну. Он передаёт чемодан кому-то другому. И теперь у обеих сторон разговора будет один и тот же ключ.

Конечно, вы могли бы сделать то же самое с помощью курьера, позвонив кому-то по телефону или просто обменявшись ключами лично. Но в интернете мы не можем позволить себе такую роскошь, как время. Нам нужно иметь возможность мгновенно зашифровать одно сообщение в нашем браузере. Поэтому нам нужно использовать какой-то способ обмена ключами в пределах полосы пропускания, то есть отправлять по сети какой-то тип информации.

Иногда это можно сделать с помощью дополнительных механизмов шифрования. Например, можно использовать асимметричное шифрование для шифрования симметричного ключа, отправить этот ключ в асимметричном шифровании третьей стороне, и она сможет расшифровать его и получить симметричный ключ. Это позволяет безопасно передавать ключи шифрования по сети. И всё это происходит относительно быстро.

Обычно так поступают с ключами, которые могут использоваться только в течение короткого периода времени. Например, сеансовые ключи используются временно. Затем мы удаляем эти сеансовые ключи и используем новый сеансовый ключ для следующего сеанса. Например, клиент может зашифровать случайный или симметричный ключ, который будет использоваться в течение сеанса, с помощью открытого ключа сервера. Затем клиент отправляет эту зашифрованную информацию на сервер. А сервер использует свой закрытый ключ для расшифровки этого сеансового ключа.

Существует ещё один способ создания симметричного ключа между двумя устройствами с помощью криптографии с открытым ключом. Это позволит нам создать один и тот же симметричный ключ на обоих устройствах без необходимости отправлять его по сети. Вот как это работает.

Начнём со стороны Боба. У Боба, очевидно, есть закрытый ключ, который есть только у Боба. У Алисы тоже есть закрытый ключ. Её закрытый ключ известен только ей. Затем мы объединим закрытый ключ Боба с открытым ключом Алисы. Открытый ключ Алисы, очевидно, известен всем. Таким образом, Боб легко получит доступ к этой информации.

И наоборот, Алиса может объединить свой закрытый ключ с открытым ключом Боба. Поскольку и Боб, и Алиса используют математически связанные ключи, они создают один и тот же симметричный ключ с помощью этого алгоритма.

Мы называем их алгоритмами обмена ключами. Мы не используем шифрование или хеширование. Вместо этого мы генерируем один и тот же симметричный ключ на обеих сторонах канала, хотя и не передаём этот симметричный ключ по сети.