Инфраструктура открытых ключей

Таким образом, если при симметричном шифровании для шифрования и дешифрования используется один и тот же ключ, то при асимметричном шифровании для шифрования и дешифрования используются два разных ключа. Эти два ключа, которые мы используем, — один для шифрования, а другой для дешифрования — математически связаны. На самом деле мы создаём оба ключа одновременно в рамках одного процесса. Это обеспечивает математическую связь между двумя ключами.

Это значит, что после создания этих двух математических ключей вы назначаете один из них закрытым ключом, а другой — открытым. Как следует из названия, закрытый ключ — это ключ, к которому есть доступ только у одного человека или устройства. Больше ни у кого нет доступа к этому закрытому ключу. Открытый ключ, как следует из названия, может видеть и использовать любой человек. Открытый ключ, как следует из названия, может быть доступен всем.

Если вы никогда раньше не использовали асимметричную криптографию, следующая часть может показаться вам нелогичной, но именно в этом и заключается сила и магия асимметричной криптографии. Любой, у кого есть открытый ключ, может зашифровать данные и отправить их вам с помощью этого открытого ключа. Закрытый ключ, который есть только у вас, — это единственный ключ, который может расшифровать любые данные, зашифрованные с помощью открытого ключа.

Например, несколько разных пользователей могут шифровать данные с помощью вашего открытого ключа и отправлять вам эту информацию. Если кто-то из этих пользователей получит доступ к зашифрованной информации, он не сможет расшифровать её с помощью открытого ключа, потому что единственный ключ, который может её расшифровать, — это закрытый ключ, а он есть только у вас.

Ещё один важный момент: хотя открытый и закрытый ключи математически связаны, вы не сможете получить один ключ, просто взглянув на другой или владея им. Из-за математических особенностей создания этих открытого и закрытого ключей невозможно восстановить закрытый ключ, даже если у вас есть открытый ключ. И это одно из главных преимуществ криптографии с открытым ключом.

Если вы когда-либо пользовались приложением, использующим асимметричное шифрование, например PGP или GPG, то вам приходилось создавать пару открытого и закрытого ключей. Этот процесс создания открытого и закрытого ключей происходит одновременно и обычно включает в себя множество случайных операций, комбинацию очень больших простых чисел и множество криптографических операций, выполняемых за кулисами.

Если вы создаёте эти ключи самостоятельно, то, как правило, вам нужно пройти через этот процесс только один раз в самом начале. После этого у вас будет закрытый и открытый ключи. В случае с Алисой она создаёт или генерирует новую пару ключей. Процесс генерации ключей обычно занимает всего несколько минут. В результате генерируются два отдельных ключа. Один из них определяется как открытый ключ. Другой ключ называется закрытым.

На этом этапе мы можем отправить открытый ключ нашим друзьям. Мы можем опубликовать его на нашем сайте или прикрепить к нашим страницам в социальных сетях. Затем мы берём закрытый ключ, сохраняем его локально и обеспечиваем его защиту. Очень часто мы присваиваем закрытому ключу пароль, чтобы для получения

доступа нужно было его знать. Это обеспечивает дополнительный уровень защиты на случай, если кто-то посторонний обнаружит наш закрытый ключ или получит к нему доступ.

Итак, теперь, когда Алиса создала открытый и закрытый ключи, она сделала открытый ключ доступным для всех. У неё есть друг по имени Боб, который хотел бы отправить Алисе зашифрованное сообщение. Боб начинает с того, что пишет на своём ноутбуке сообщение, которое мы будем называть открытым текстом. В нём говорится: «Привет, Алиса». У него есть открытый ключ Алисы, потому что, будучи открытым ключом, он доступен для всех.

Это данные для вашего программного обеспечения асимметричного шифрования, которое затем создает зашифрованный текст. Это комбинация открытого текста и открытого ключа Алисы. На этом этапе зашифрованный текст может быть отправлен Алисе и фактически доступен для просмотра любому пользователю. Расшифровать эту информацию без закрытого ключа невозможно. Даже если кто-то получит доступ к зашифрованному тексту и открытому ключу, он все равно не сможет каким-то образом восстановить открытый текст.

Теперь, когда Боб создал зашифрованный текст, он может отправить его Алисе. Алиса видит, что это зашифрованные данные, и использует свой закрытый ключ для расшифровки. В этот момент мы возвращаемся к исходному тексту. И, как вы можете видеть, он идентичен исходному тексту, который изначально отправил Боб. Когда вы имеете дело с одним человеком, у которого есть собственная пара открытого и закрытого ключей, он сам должен управлять ими. А в будущем, если вам понадобится расшифровать информацию, этот человек просто обратится к своему закрытому ключу и расшифрует всё, что ещё может быть зашифровано в его системе.

Но если вы работаете в среде с сотнями или тысячами пользователей и у каждого из них есть собственная пара открытого и закрытого ключей, вам может понадобиться какой-то способ управления таким большим объёмом данных. Это может быть сторонняя служба, которой вы передаёте закрытые ключи, и она хранит их до тех пор, пока они вам не понадобятся. Или, возможно, вы сами выполняете функцию условного депонирования ключей. После того как все создадут свои ключи, вы можете хранить их локально.

И если этот пользователь покинет компанию или перейдёт в другой отдел, у вас всё равно останутся приватные ключи, чтобы вы могли расшифровать всё, над чем он работал. Это часто встречается, когда нужно предоставить возможность расшифровать данные, даже если вы не тот, кто изначально их зашифровал. Например, как мы уже упоминали, пользователь может покинуть организацию, но нам всё равно нужен доступ ко всем его зашифрованным данным. Или это может быть государственное учреждение, которое работает с партнёром, и обеим организациям нужно расшифровать данные, которые могли быть зашифрованы в рамках этого проекта.

Передача закрытого ключа кому-то другому для управления процессом может показаться сомнительной. Но в некоторых случаях это необходимо для обеспечения бесперебойной работы и доступности всех данных вашей организации.