КЛАССИЧЕСКАЯ КРИПТОГРАФИЯ

Криптография как наука способна обеспечить конфиденциальность передачи данных, проверку целостности аутентификации пользователей. В качестве развлекательного примера можно рассмотреть протокол аутентификации.

Какой выбрать способ, чтобы узнать легален ли пользователь, ведь в мире компьютеров пароль можно вводить многократно.

Даже при ограниченном числе попыток, пользователь может прийти повторно с другого IP-адреса или представиться иным именем, попытаться взломать пароль путем многократных подборов.

Когда сервисы говорят, что пароль ненадежен, это неслучайно. Короткий шифр легко набирается путем перебора, поэтому рекомендуется создавать длинные пароли и использовать символы.

Насколько устойчив ваш пароль?



Выделяют две группы протоколов. Первая — протоколы симметричной криптографии, когда у двух участников есть секретный ключ и с его помощью они могут шифровать или дешифровать передаваемые сообщения.

Это надежная техника. Единственная проблема: ключ надо распределить каким-то образом, то есть обеспечить секретность ключа у участников обмена.

В асимметричной криптографии используют открытый и закрытый ключ. В этом случае в основе протоколов часто лежат задачи односторонней функции. Например, перемножить два простых числа легко, а вот обратная задача считается сложной, поскольку тяжело разложить произведение двух простых чисел на множители, которые заранее неизвестны.

Функции, лежащие в основе асимметричной криптографии, — это односторонние функции, которые легко вычислить и сложно обратить. Строго доказать существование односторонних функций пока не удается.

Предполагается, что они сложные, так как неизвестны эффективные способы их вычисления. Стойкость таких протоколов становится условной.

Либо мы верим, что такие алгоритмы не существуют, либо понимаем, что у атакующего не хватает вычислительных ресурсов, чтобы взломать протокол. Здесь уместно перейти к квантовой криптографии и квантовым вычислениям. Именно они могут взломать подобные протоколы.