Симметричное шифрование

Симметричное шифрование

Для работы применяется всего один пароль. Происходит всё следующим образом:

1. Существует некий математический алгоритм шифрования.
2. На его вход подаётся текст и пароль.
3. На выходе получаем зашифрованный текст.
4. Если хотим получить исходный текст, применяется тот же самый пароль, но с алгоритмом дешифрования.

Особенности симметричного шифрования

Говоря простым языком, если кто-то узнает наш пароль, безопасность криптосистемы тут же нарушится. Именно поэтому, используя подходы симметричного шифрования, мы должны особое внимание уделять **вопросам создания и сохранения конфиденциальности пароля**. Он должен быть сложным, что исключит подбор программным перебором значений. И не должен передаваться кому-нибудь в открытом виде как в сети, так и на физических носителях информации. Очевидно, что листочек, прикреплённый к монитору — явно не лучший вариант)).

Плюсы симметричного шифрования

Несмотря на свои ограничения и угрозу безопасности, подход до сих пор широко распространён в криптографии. Дело в том, что он очень прост в работе и понимании. И техническая нагрузка на железо невелика (как правило, всё работает очень быстро).

Благодарю за внимание