Когда люди говорят про крипту вообще, есть несколько фундаментальных принципов. Один из них — принцип Керкгоффса, который говорит, что open source в криптографии очень важен. Если точнее, он дает общее знание об устройстве протоколов. Смысл очень простой: криптографические алгоритмы, которые используются в той или иной системе, не должны быть секретом, обеспечивающим ее устойчивость. В идеале необходимо строить системы так, чтобы их криптографическая сторона была полностью известна атакующему и единственным секретом являлся криптографический ключ, который в данной системе используется.

Современные и коммерчески доступные системы шифрования — все или почти все или лучшие из них — построены из компонент, устройство и принцип работы которых хорошо известны. Единственная секретная вещь в них — ключ шифрования. Есть только одно известное мне значимое исключение — набор секретных криптографических протоколов для всевозможных государственных организаций. В США это называется NSA suite B, а в России это всякие странные секретные алгоритмы шифрования, которые до определенной степени используются военными и государственными органами.

Не сказал бы, что такие алгоритмы приносят им большую пользу, за исключением того, что это примерно как атомная физика. Можно попытаться по пониманию дизайна протокола понять направление мысли людей, которые его разработали, и неким образом обогнать другую сторону. Не знаю, насколько такой принцип актуален по нынешним меркам, но люди, знающие про это больше меня, поступают именно так.