



Понятие шифрования пришло до нас еще с древних времен. Его использовали на протяжении многих столетий. Даже сам Юлий Цезарь пользовался небольшим шифрованием в своих письмах. Он немного сдвигал каждую букву в своем письме на три позиции в левую сторону, сегодня это так же используется и называется Шифр Цезаря. На сегодняшний день существует много принципов шифрования. Рассмотрим историю и основные стандарты шифрования.

Одним из стандартов, которым начали пользоваться с 1970-х годов, является DES (Стандарт шифрования данных). Стандарт разработан IBM, но в дальнейшем его стало улучшать Агенство национальной безопасности. В то время, стандарт DES стал, практически не уязвим. Длина ключа составляла 56 бит, его и можно было взломать, но за определенное время, просто методом подбора, было под силу не каждому. В конце 90-х годов все изменилось, и DES могли взломать в течении нескольких дней, этому способствовало наличие новых технологий. Причина быстрого взлома таилась в маленьком размере ключа и блока. Именно в это время DES признали непригодным для защиты информации.

В январе 1997 года Национальным институтом стандартов и технологий, был объявлен конкурс, чтобы заменить DES. Принять участие в конкурсе мог кто угодно, но при этом он должен был понимать, что его творение будет бесплатным для всех. В условиях конкурса были прописаны такие правила, что разработчик должен был придумать, как создать устойчивость шифра к линейному и дифференциальному криптоанализу, но при этом шифр не становился сложным в реализации. Победителями стали Йоан Даймен и Винсент Рэймен.

Сегодня используется Продвинутый стандарт шифрования (AES), он имеет блоки по 128 бит, это не дает его так просто взломать. В AES нет слабых ключей, в отличие от DES, в котором 16 слабых ключей.

Шифрование имеет длинную историю, но его назначение не изменяется и сегодня. Как оно использовалось для разнообразной защиты информации, так и используется до сегодняшнего дня.

Автор: Administrator

12.12.2012 00:00 - Обновлено 10.01.2013 17:09

---