ТЕМА 6. Коды аутентификации сообщений - MAC

6.1. Требования к MAC

Один из способов обеспечения целостности - это вычисление *MAC* (Message Authentication Code). Под *MAC* понимается некоторый аутентификатор, являющийся определенным способом вычисленным блоком данных, с помощью которого можно проверить целостность сообщения. В некоторой степени симметричное шифрование всего сообщения может выполнять функцию аутентификации этого сообщения. Но в таком случае сообщение должно содержать достаточную избыточность, которая позволяла бы проверить, что сообщение не было изменено. Избыточность может быть в виде определенным образом отформатированного сообщения, текста на конкретном языке и т.п. Если сообщение допускает произвольную последовательность битов (например, зашифрован ключ сессии), то симметричное шифрование всего сообщения не может обеспечивать его целостность, так как при дешифровании в любом случае получится последовательность битов, правильность которой проверить нельзя. Поэтому гораздо чаще используется критографически созданный небольшой блок данных фиксированного размера, так называемый аутентификатор или имитовставка, с помощью которого проверяется целостность сообщения. Этот блок данных может создаваться с помощью секретного ключа, который разделяют отправитель и получатель. *MAC* вычисляется в тот момент, когда известно, что сообщение корректно. После этого *MAC* присоединяется к сообщению и передается вместе с ним получателю. Получатель вычисляет *MAC*, используя тот же самый секретный ключ, и сравнивает вычисленное значение с полученным. Если эти значения совпадают, то с большой долей вероятности можно считать, что при пересылке изменения сообщения не произошло.

$MAC = C_K(M)$

Предположим, что конфиденциальности сообщения нет, т.е. оппонент имеет доступ к открытому сообщению и соответствующему ему значению *MAC*. Определим усилия, необходимые оппоненту для нахождения ключа *MAC*. Предположим, что $k > n$, т.е. длина ключа больше длины *MAC*. Тогда, зная M_1 и $MAC_1 = C_K(M_1)$, оппонент может вычислить $MAC_1 = C_{K_i}(M_1)$ для всех возможных ключей K_i. При этом, по крайней мере, для одного из ключей будет получено совпадение $MAC_i = MAC_1$. Оппонент вычислит 2^k значений *MAC*, тогда как при длине *MAC* n битов существует всего 2^n значений *MAC*. Мы предположили, что $k > n$, т.е. $2^k > 2^n$. Таким образом, правильное значение *MAC* будет получено для нескольких значений ключей. В среднем совпадение будет иметь место для $2^k / 2^n = 2^{(k-n)}$ ключей. Поэтому для вычисления единственного ключа оппоненту требуется знать несколько пар сообщение и соответствующий ему *MAC*.

Таким образом, простой перебор всех ключей требует не меньше, а больше усилий, чем поиск ключа симметричного шифрования той же длины.

Функция вычисления *MAC* должна обладать следующими свойствами:

1. Должно быть вычислительно трудно, зная M и C_K (M), найти сообщение M′, такое, что $C_K(M) = C_K(M')$.
2. Значения $C_K(M)$ должны быть равномерно распределенными в том смысле, что для любых сообщений M и M′ вероятность того, что $C_K(M) = C_K(M')$, должна быть равна 2^{-n}, где n - длина значения MAC.