Теоретические основы криптосистем с открытым ключом

Главная проблема использования одноключевых (симметричных) криптосистем заключается в распределении ключей. Для того, чтобы был возможен обмен информацией между двумя сторонами, ключ должен быть сгенерирован одной из них, а затем в конфиденциальном порядке передан другой.

Суть шифрования с открытым ключом заключается в том, что для шифрования данных используется один ключ, а для расшифрования другой (поэтому такие системы часто называют ассиметричными).

Первый ключ, которым шифруется исходное сообщение, называется открытым и может быть опубликован для использования всеми пользователями системы. Расшифрование с помощью этого ключа невозможно. Второй ключ, с помощью которого дешифруется сообщение, называется секретным (закрытым) и должен быть известен только законному получателю закрытого сообщения.

Алгоритмы шифрования с открытым ключом используют так называемые необратимые или односторонние функции. Эти функции обладают следующим свойством: при заданном значении аргумента $\boldsymbol{x}$ относительно просто вычислить значение функции $f(x)$, однако, если известно значение функции $\boldsymbol{y = f(x)}$, то нет простого пути для вычисления значения аргумента **x**.

Система открытого распространения ключей позволяет двум сторонам сформировать совместную часть некоторой распределенной секретной информации. Однако, ни одна из сторон не имеет никакого непосредственного влияния на то, какой окажется эта информация.

Криптосистема RSA

RSA – криптографическая система с открытым ключем, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности).

Алгоритм RSA работает следующим образом:

Пусть p и q - два больших различных простых числа, и пусть $n = p \times q$ и e некоторое целое, взаимно простое с $(p-1)\times(q-1)$.

Пространства открытых текстов M_k и зашифрованных сообщений C_k представляют собой множество неотрицательных целых чисел Z_n, меньших n. Если исходное сообщение окажется слишком длинным, чтобы принадлежать Z_n, его необходимо разбить на части, равные m.

Соответствующая ключу k функция шифрования E_k: M_k -> C_k определяется как $E_k(m) = m^e \bmod(n)$. Для того, чтобы полностью определить алгоритм ее вычисления, достаточно записать e и n в открытый справочник. Такая пара называется открытым ключом.

E_k является кандидатом на однонаправленную функцию с потайным ходом, и хотя существует эффективный алгоритм вычисления обратной ей функции D_k, мы не знаем, как получить его на основании алгоритма E_k (т.е. только для заданных n и e).