ТЕМА 4 Криптография с открытым ключом

4.1 Основные требования к алгоритмам асимметричного шифрования

Алгоритмы шифрования с *открытым ключом* разрабатывались для того, чтобы решить две наиболее трудные задачи, возникшие при использовании симметричного шифрования: распределение ключа и цифровая подпись.

При описании симметричного шифрования и шифрования с *открытым ключом* будем использовать следующую терминологию. Ключ, используемый в симметричном шифровании, будем называть секретным ключом. Два ключа, используемые при шифровании с *открытым ключом*, будем называть *открытым ключом* и *закрытым ключом*. *Закрытый ключ* держится в секрете, но называть его будем *закрытым ключом*, а не секретным, чтобы избежать путаницы с ключом, используемым в симметричном шифровании. *Закрытый ключ* будем обозначать KR, *открытый ключ* - KU.

Будем предполагать, что все участники имеют доступ к *открытым ключам* друг друга, а *закрытые ключи* создаются локально каждым участником и, следовательно, распределяться не должны.

Диффи и Хеллман описывают требования, которым должен удовлетворять алгоритм шифрования с *открытым ключом*.

1. Вычислительно легко создавать пару *KU, KR*.
2. Вычислительно легко, имея *открытый ключ* и незашифрованное сообщение *M*, создать соответствующее зашифрованное сообщение:
   $C = E_{KU}[M]$
3. Вычислительно легко дешифровать сообщение, используя *закрытый ключ*:
   $M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$
4. Вычислительно невозможно, зная *открытый ключ KU*, определить *закрытый ключ KR*.
5. Вычислительно невозможно, зная *открытый ключ KU* и зашифрованное сообщение C, восстановить исходное сообщение *M*.

Можно добавить шестое требование, хотя оно не выполняется для всех алгоритмов с *открытым ключом*:

6. Шифрующие и дешифрующие функции могут применяться в любом порядке:
   $M = E_{KU}[D_{KR}[M]]$

Это достаточно сильные требования, которые вводят понятие *односторонней функции с люком*. ***Односторонней функцией*** называется такая функция, у которой каждый аргумент имеет единственное обратное

значение, при этом вычислить саму функцию легко, а вычислить обратную функцию трудно.

$Y = f(X)$ - легко

$X = f^{-1}(Y)$ - трудно

Вернемся к определению *односторонней функции с люком*, которую, подобно *односторонней функции*, легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация. При наличии этой дополнительной информации инверсию можно вычислить за полиномиальное время. Таким образом, *односторонняя функция* с люком принадлежит семейству *односторонних функций* f_k таких, что

$Y = f_k(X)$ - легко, если k и X известны

$X = f_k^{-1}(Y)$ - легко, если k и Y известны

$X = f_k^{-1}(Y)$ - трудно, если Y известно, но k неизвестно

.