[ИНФОРМАЦИОННАЯ БЕЗОПАСТНОСТЬ]

[Институт ИИБС, Кафедра ИСКТ]

[Шумейко Е.В.]

Криптография с открытым ключом

Основные требования к алгоритмам асимметричного шифрования

Основные требования к алгоритмам асимметричного шифрования
Создание *алгоритмов асимметричного шифрования* является величайшим и, возможно, единственным революционным достижением в истории криптографии.
Алгоритмы шифрования с *открытым ключом* разрабатывались для того, чтобы решить две наиболее трудные задачи, возникшие при использовании симметричного шифрования.
Первой задачей является распределение ключа. При симметричном шифровании требуется, чтобы обе стороны уже имели общий ключ, который каким-то образом должен быть им заранее передан. Диффи, один из основоположников шифрования с *открытым ключом*, заметил, что это требование отрицает всю суть криптографии, а именно возможность поддерживать всеобщую секретность при коммуникациях.

Основные требования к алгоритмам асимметричного шифрования

Второй задачей является необходимость создания таких механизмов, при использовании которых невозможно было бы подменить кого-либо из участников, т.е. нужна *цифровая подпись*. При использовании коммуникаций для решения широкого круга задач, например в коммерческих и частных целях, электронные сообщения и документы должны иметь эквивалент подписи, содержащейся в бумажных документах. Необходимо создать метод, при использовании которого все участники будут убеждены, что электронное сообщение было послано конкретным участником. Это более сильное требование, чем аутентификация.

Диффи и Хеллман достигли значительных результатов, предложив способ решения обеих задач, который радикально отличается от всех предыдущих подходов к шифрованию.

Сначала рассмотрим общие черты алгоритмов шифрования с *открытым ключом* и требования к этим алгоритмам. Определим требования, которым должен соответствовать алгоритм, использующий один ключ для шифрования, другой ключ - для дешифрования, и при этом вычислительно невозможно определить дешифрующий ключ, зная только алгоритм шифрования и шифрующий ключ.

Основные требования к алгоритмам асимметричного шифрования

Кроме того, некоторые алгоритмы, например RSA, имеют следующую характеристику: каждый из двух ключей может использоваться как для шифрования, так и для дешифрования.

Сначала рассмотрим алгоритмы, обладающие обеими характеристиками, а затем перейдем к алгоритмам *открытого ключа*, которые не обладают вторым свойством.

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.

Основные требования к алгоритмам асимметричного шифрования

В любое время участник может изменить свой *закрытый ключ* и опубликовать составляющий пару *открытый ключ*, заменив им старый *открытый ключ*.

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

1. Вычислительно легко создавать пару (*открытый ключ* KU , *закрытый ключ* KR).
2. Вычислительно легко, имея *открытый ключ* и незашифрованное сообщение M, создать соответствующий зашифрованное сообщение:

   $C = E_{KU}[M]$

3. Вычислительно легко дешифровать сообщение, используя *закрытый клю*

   $M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$

4. Вычислительно невозможно, зная *открытый ключ* KU, определить *закрытый ключ* KR.

Основные требования к алгоритмам асимметричного шифрования

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