Министерство образования Республики Беларусь  
Частное учреждение образования  
«Гродненский колледж бизнеса и права»

**Реферат**

По дисциплине:  
«Защита компьютерной информации»  
Тема: Ассиметричные криптоалгоритмы.

Выполнил:  
Учащийся 25–ПО группы  
Олишкевич И.Р.

## 

## Асимметричные криптоалгоритмы

Асимметричные алгоритмы шифрования (или алгоритмы с открытым ключом) – криптографические алгоритмы, в которых один ключ используется для шифрования, а другой, отличный от первого, – для расшифрования. Алгоритмы называются асимметричными, так как ключи шифрования и расшифрования разные, следовательно, отсутствует симметрия основных криптографических процессов. Один из двух ключей является открытым (public key) и может быть объявлен всем, а второй – закрытым (private key) и должен держаться в секрете. Какой из ключей, открытый или закрытый, используется для шифрования, а какой для расшифрования, определяется назначением криптографической системы.

Все алгоритмы шифрования с открытым ключом основаны на использовании односторонних функций. Односторонней функцией называется математическая функция, которую относительно легко вычислить, но трудно найти по значению функции соответствующее значение аргумента. Использовать односторонние функции для шифрования сообщений с целью их защиты не имеет смысла, так как обратно расшифровать зашифрованное сообщение уже не получится. Для целей шифрования используются односторонние функции с люком (или с секретом) – особый вид односторонних функций, имеющих некоторый секрет (люк), позволяющий относительно быстро вычислить обратное значение функции.

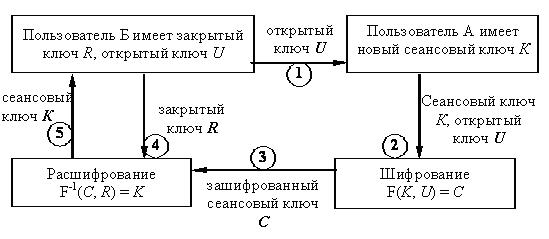
Алгоритмы шифрования с открытым ключом можно использовать для решения следующих задач:

1. для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа;
2. для формирования цифровой подписи под электронными документами;
3. для распределения секретных ключей, используемых потом при шифровании документов симметричными методами.

Простейший протокол формирования секретного ключа сессии может выглядеть следующим образом (если пользователи некоторой системы связи имеют доступ к базе данных открытых ключей абонентов системы, предоставляемой центром распределения ключей, то они могут получать из нее открытые ключи друг друга):

1. пользователь А получает открытый ключ пользователя Б из центра распределения ключей или непосредственно от пользователя Б;
2. пользователь А генерирует случайный сеансовый ключ и зашифровывает его полученным открытым ключом;
3. зашифрованный сеансовый ключ пересылается пользователю Б;
4. пользователь Б расшифровывает полученный пакет своим закрытым ключом;
5. пользователи А и Б используют согласованный сеансовый ключ для обмена шифрованными сообщениями.

Схему формирования парой пользователей А и В общего секретного ключа К для шифрования - расшифрования можно изобразить следующим образом, как показано на рисунке 1.

  
Рисунок 1 –Схема формирования общего секретного ключа

Существуют и более сложные протоколы распределения ключей, обеспечивающие взаимное подтверждение подлинности участников сеанса связи, подтверждение достоверности сеанса механизмом запроса-ответа или другие требования.

Рассмотрев основные способы применения алгоритмов шифрования с открытым ключом, изучим требования, которым должен, по мнению основоположников теории шифрования с открытым ключом Диффи и Хеллмана, удовлетворять алгоритм шифрования с открытым ключом. Эти требования следующие:

1. Вычислительно легко создавать пару (открытый ключ, закрытый ключ);
2. Вычислительно легко зашифровать сообщение открытым ключом;
3. Вычислительно легко расшифровать сообщение, используя закрытый ключ;
4. Вычислительно невозможно, зная открытый ключ, определить соответствующий закрытый ключ;
5. Вычислительно невозможно, зная только открытый ключ и зашифрованное сообщение, восстановить исходное сообщение.

Из этих общих требований видно, что реализация конкретного алгоритма с открытым ключом зависит от соответствующей односторонней функции.

Цифровая (электронная) подпись – уникальное числовое дополнение к передаваемой информации, позволяющее проверить ее авторство. Электронная (цифровая) подпись (ЭЦП) представляет собой последовательность бит фиксированной длины, которая вычисляется определенным образом с помощью содержимого подписываемой информации и секретного ключа. Различают присоединяемые цифровые подписи и цифровые подписи с восстановлением документа. Присоединяемые цифровые подписи – подписи, вычисленные по хеш-коду документа. Такие цифровые подписи представляют собой некоторый числовой код, который необходимо пристыковывать к подписываемому документу. Само сообщение при этом не шифруется и передается в открытом виде вместе с цифровой подписью отправителя. Цифровые подписи с восстановлением документа – подписи, которые как бы содержат в себе подписываемый документ: в процессе проверки подписи автоматически вычисляется и тело документа. Если при расшифровывании сообщение восстановилось правильно, значит, подпись была верной.

Алгоритм RSA стоит у истоков асимметричной криптографии. Он был предложен тремя исседователями-математиками Рональдом Ривестом (R.Rivest), Ади Шамиром (A.Shamir) и Леонардом Адльманом (L.Adleman) в 1977-78 годах.

Первым этапом любого асимметричного алгоритма является создание пары ключей: открытого и закрытого и распространение открытого ключа "по всему миру". Для алгоритма RSA этап создания ключей состоит из следующих операций:

1. выбираются два простых (!) числа p и q;
2. вычисляется их произведение n(=p\*q);
3. выбирается произвольное число e (e<n), такое, что НОД(e,(p-1)(q-1))=1, то есть e должно быть взаимно простым с числом (p-1)(q-1);
4. методом Евклида решается в целых числах (!) уравнение e\*d+(p-1)(q-1)\*y=1. Здесь неизвестными являются переменные d и y – метод Евклида как раз и находит множество пар (d,y), каждая из которых является решением уравнения в целых числах;
5. два числа (e,n) – публикуются как открытый ключ;
6. число d хранится в строжайшем секрете – это и есть закрытый ключ, который позволит читать все послания, зашифрованные с помощью пары чисел (e,n).

Как же производится собственно шифрование с помощью этих чисел:

1. отправитель разбивает свое сообщение на блоки, равные k=[log2(n)] бит, где квадратные скобки обозначают взятие целой части от дробного числа;
2. подобный блок, как Вы знаете, может быть интерпретирован как число из диапазона (0;2k-1). Для каждого такого числа (назовем его mi) вычисляется выражение ci=((mi)e)mod n. Блоки ci и есть зашифрованное сообщение Их можно спокойно передавать по открытому каналу, поскольку.операция возведения в степень по модулю простого числа, является необратимой математической задачей. Обратная ей задача носит название "логарифмирование в конечном поле" и является на несколько порядков более сложной задачей. То есть даже если злоумышленник знает числа e и n, то по ci прочесть исходные сообщения mi он не может никак, кроме как полным перебором mi.

А вот на приемной стороне процесс дешифрования все же возможен, и поможет нам в этом хранимое в секрете число d. Достаточно давно была доказана теорема Эйлера, частный случай которой утвержает, что если число n представимо в виде двух простых чисел p и q, то для любого x имеет место равенство (x(p-1)(q-1))mod n = 1. Для дешифрования RSA-сообщений воспользуемся этой формулой. Возведем обе ее части в степень (-y): (x(-y)(p-1)(q-1))mod n = 1(-y) = 1. Теперь умножим обе ее части на x: (x(-y)(p-1)(q-1)+1)mod n = 1\*x = x.

А теперь вспомним как мы создавали открытый и закрытый ключи. Мы подбирали с помощью алгоритма Евклида d такое, что e\*d+(p-1)(q-1)\*y=1, то есть e\*d=(-y)(p-1)(q-1)+1. А следовательно в последнем выражении предыдущего абзаца мы можем заменить показатель степени на число (e\*d). Получаем (xe\*d)mod n = x. То есть для того чтобы прочесть сообщение ci=((mi)e)mod n достаточно возвести его в степень d по модулю m: ((ci)d)mod n = ((mi)e\*d)mod n = mi.

На самом деле операции возведения в степень больших чисел достаточно трудоемки для современных процессоров, даже если они производятся по оптимизированным по времени алгоритмам. Поэтому обычно весь текст сообщения кодируется обычным блочным шифром (намного более быстрым), но с использованием ключа сеанса, а вот сам ключ сеанса шифруется как раз асимметричным алгоритмом с помощью открытого ключа получателя и помещается в начало файла.

Алгоритм открытого распределения ключей Диффи-Хеллмана был предложен в 1976 году. В этом криптоалгоритме используются свойства однонаправленных функций, предложенных У. Диффи и М. Хеллманом. Уникальность алгоритма Диффи-Хеллмана заключается в том, что пара абонентов сети имеет возможность получить известное только им секретное число, передавая по открытой сети открытые ключи. После этого абоненты могут приступить к защите сообщений уже известными проверенными способами – применяя электронную цифровую подпись и симметричное шифрование с использованием полученного разделяемого секрета. Алгоритм Диффи-Хеллмана посвящен, прежде всего, решению проблемы распределения ключей.

Алгоритм асимметричного шифрования Эль Гамаля был предложен в 1985 году. Безопасность его работы обусловлена сложностью вычисления дискретных логарифмов в конечном поле. Длина шифртекста, формируемого алгоритмом Эль Гамаля, вдвое больше длины исходного открытого текста. Схема Эль Гамаля может быть использована как для шифрования, так и для электронной цифровой подписи.

Криптосистема ЕСС на основе эллиптических кривых реализует асимметричный алгоритм шифрования.

Она использует алгебраическую систему, которая описывается в терминах точек эллиптических кривых. Криптосистема ЕСС является конкурентом по отношению к другим асимметричным алгоритмам шифрования, так как при эквивалентной стойкости использует ключи меньшей длины и имеет большую производительность. Современные ее реализации показывают, что эта система гораздо более эффективна, чем другие системы с открытыми ключами. Ее производительность приблизительно на порядок выше, чем у криптосистемы RSA.

Асимметричные криптосистемы обладают неоспоримым достоинством по сравнению с симметричными: они позволяют динамически передавать открытые ключи, тогда как при использовании симметричной криптосистемы необходим обмен секретными ключами до начала сеанса защищенной связи. Асимметричные криптоалгоритмы позволяют преодолеть недостатки, присущие системам симметричного шифрования:

* + не нужна секретная доставка ключей;
  + исчезает квадратическая зависимость числа ключей от числа пользователей.

Однако у асимметричных криптосистем имеются и недостатки:

* + на настоящий момент нет математического доказательства необратимости используемых в асимметричных алгоритмах однонаправленных функций;
  + по сравнению с симметричным асимметричное шифрование существенно медленнее, поскольку при зашифровании и расшифровании выполняются весьма трудоемкие операции (в частности, в RSA это возведение одного большого числа в степень, являющуюся другим большим числом). По этой же причине реализация аппаратного шифратора с асимметричным криптоалгоритмом существенно сложнее, чем аппаратная реализация симметричного криптоалгоритма;
  + необходимо защищать открытые ключи от подмены.

Поясним более подробно проблему защиты открытых ключей от подмены. Предположим, на компьютере абонента А хранится открытый ключ КВ абонента В. Пусть злоумышленник @ имеет доступ к открытым ключам, хранящимся у абонента А. Он генерирует свою пару ключей k@ и К@ и подменяет у абонента А открытый ключ КВ абонента В на свой открытый ключ К@. Для того чтобы отправить некую информацию абоненту В, абонент А зашифровывает ее на ключе К@, думая, что это ключ КВ. Соответственно, это сообщение не сможет прочитать абонент В, но зато легко расшифрует и прочитает злоумышленник @. Атаку подмены открытых ключей может предотвратить процедура сертификации открытых ключей.