**Электронная подпись на основе алгоритма RSA**

Рассмотренная схема использования алгоритма *RSA* при большом модуле N практически не позволяет злоумышленнику получить закрытый *ключ* и прочитать зашифрованное сообщение. Однако она дает возможность злоумышленнику подменить сообщение от абонента А к абоненту Б, так как *абонент* А шифрует свое сообщение открытым ключом, полученным от Б по открытому каналу связи. А раз *открытый ключ* передается по открытому каналу, любой может получить его и использовать для подмены сообщения. Избежать этого можно, используя более сложные протоколы, например, следующий.

Пусть, как и раньше, *пользователь* А хочет передать пользователю Б сообщение, состоящее из нескольких блоков mi. Перед началом сеанса связи абоненты генерируют открытые и закрытые ключи, обозначаемые, как указано в следующей таблице:

|  |  |  |
| --- | --- | --- |
|  | **Открытый ключ** | **Закрытый ключ** |
| Пользователь А | NA, dA | eA |
| Пользователь Б | NБ, dБ | eБ |

В результате каждый *пользователь* имеет свои собственные открытый (состоящий из двух частей) и закрытый ключи. Затем пользователи обмениваются открытыми ключами. Это подготовительный этап протокола.

Основная часть протокола состоит из следующих шагов.

1. g_i=c_i^{d_Б} \: mod \: N_Бc_i=m_i^{e_A} \: mod \:N_AСначала пользователь А вычисляет числа, то есть шифрует сообщение своим закрытым ключом. В результате этих действий пользователь А подписывает сообщение.
2. Затем пользователь А вычисляет числа , то есть шифрует то, что получилось на шаге 1 открытым ключом пользователя Б. На этом этапе сообщение шифруется, чтобы никто посторонний не мог его прочитать.
3. Последовательность чисел gi передается к пользователю Б.
4. c_i=g_i^{e_Б} \: mod \: N_БПользователь Б получает gi и вначале вычисляет последовательно числа , используя свой закрытый ключ.

При этом сообщение расшифровывается.

1. m_i=c_i^{d_A} \: mod \: N_A
   Затем Б определяет числа , используя открытый ключ пользователя А.

За счет выполнения этого этапа производится проверка подписи пользователя А.

В результате абонент Б получает исходное сообщение и убеждается в том, что его отправил именно абонент А. Данная схема позволяет защититься от нескольких видов возможных нарушений, а именно:

* пользователь А не может отказаться от своего сообщения, если он признает, что секретный ключ известен только ему;
* нарушитель без знания секретного ключа не может ни сформировать, ни сделать осмысленное изменение сообщения, передаваемого по линии связи.

Данная схема позволяет избежать многих конфликтных ситуаций. Иногда нет необходимости зашифровывать передаваемое сообщение, но нужно его скрепить электронной подписью. В этом случае из приведенного выше протокола исключаются шаги 2 и 4, то есть текст шифруется закрытым ключом отправителя, и полученная последовательность присоединяется к документу. Получатель с помощью открытого ключа отправителя расшифровывает прикрепленную подпись, которая, по сути, является зашифрованным повторением основного сообщения. Если расшифрованная подпись совпадает с основным текстом, значит, подпись верна.

Существуют и другие варианты применения алгоритма RSA для формирования ЭЦП. Например, можно шифровать (то есть подписывать) открытым ключом не само сообщение, а хеш-код от него.

Возможность применения алгоритма RSA для получения электронной подписи связана с тем, что секретный и открытый ключи в этой системе равноправны. Каждый из ключей, d или e, могут использоваться как для шифрования, так и для расшифрования. Это свойство выполняется не во всех криптосистемах с открытым ключом.

Алгоритм RSA можно использовать также и для обмена ключами.

**Пример вычисления и проверки цифровой подписи**

Пусть абоненты, обменивающиеся через Интернет зашифрованными сообщениями, имеют следующие общие параметры: Р = 11, А = 7.

Один из пользователей этой системы связи хочет подписать свое сообщение m=5 цифровой подписью, сформированной по алгоритму Эль-Гамаля. Вначале он должен выбрать себе закрытый ключ, например, Х1=3 и сформировать открытый ключ Y1 = 73 mod 11 = 2. Открытый ключ может быть передан всем заинтересованным абонентам или помещен в базу данных открытых ключей системы связи.

Затем пользователь выбирает случайное секретное число k, взаимно простое с Р-1. Пусть k=9 ( 9 не имеет общих делителей с 10 ). Далее необходимо вычислить число

a=A^k \: mod \: P=7^9\: mod \: 11=8

После этого с помощью расширенного алгоритма Евклида находится значение b в уравнении:

m=(X_1 \times a + k \times b) \: mod \: (P-1),\\5=(3 \times 8 + 9 \times b) \: mod \: 10

Решением последнего уравнения будет значение b=9.

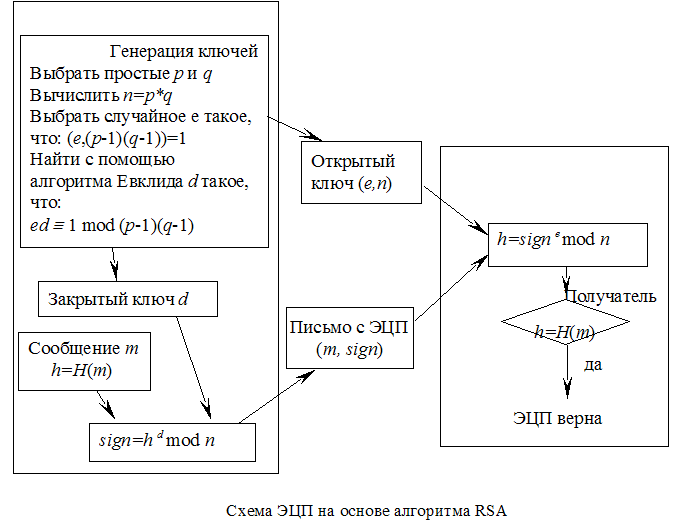
Таким образом, пара чисел (8, 9) будет цифровой подписью сообщения m=5.

Если любой другой пользователь сети желает проверить цифровую подпись в сообщении, он должен получить из базы данных открытый ключ первого пользователя (он равен 2 ), вычислить два числа с1 и с2 и сравнить их.

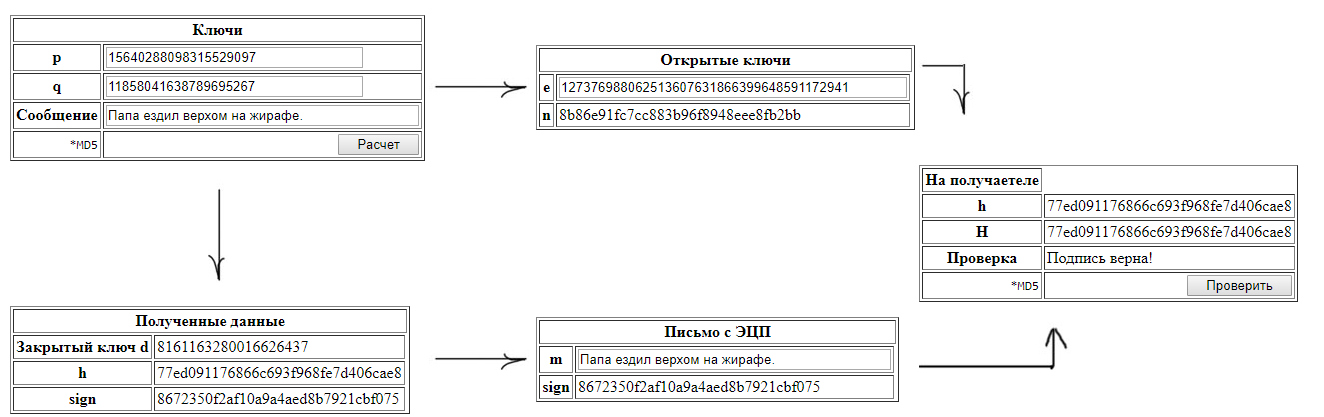
c_1-Y_1^a \times a^b \: mod \: P=2^8 \times 8^9 \: mod \: 11=10,\\c_2=A^m \: mod \: 11=10

Так как с1 = с2, то цифровая подпись первого пользователя в сообщения m=5 верная.

# Электронно-цифровая подпись: RSA



В отличие от алгоритма шифрования, отправителем здесь является владелец пары закрытый/открытый ключ. Процедура формирования электронной подписи sign под сообщением схожа с шифрованием документа, но в степень закрытого ключа d по вычету n возводится не само сообщение или его части, а дайджест сообщения h. Неотъемлемой частью алгоритмов ЭЦП является хэширование информации, на рисунке оно обозначено через H(), и это может быть любой из рассмотренных алгоритмов хэширования.

Сообщение m с подписью sign будет однозначно аутентифицировано. Авторство сообщения может быть установлено и доказано по паре ключей (d, e) с использованием сертификации по схеме, описанной в 3.2. Злоумышленник не сможет подменить сообщение m (точнее,ему будет очень трудно это сделать), поскольку ему необходимо вместо сообщения m подставить другое сообщение m’, удовлетворяющее его и имеющее такое же значение хэш-функции, что и у m, что является на сегодня вычислительно трудной задачей. По этой же причине злоумышленник не сможет применить перехваченную подпись sign для подписи другого документа, поскольку для другого документа будет получено иное значение хэш-функции h,а оно лежит в основе подписи. Таким образом, все необходимые свойства подписи описанным алгоритмом обеспечиваются, что же касается криптостойкости метода ЭЦП, то она определяется криптостойкостью используемого асимметричного криптографического метода и функции однонаправленного шифрования. Необходимо отметить также, что само сообщение m передается в открытом виде. Для того, чтобы обеспечить конфиденциальность передаваемой в нем информации, требуется использование дополнительного шифрования по симметричной или асимметричной схеме (при этом шифрование на ключе d конфиденциальности не обеспечит, поскольку сообщение может быть расшифровано открытым ключом e).