Рассмотрим алгоритм RSA с практической точки зрения.

Для начала необходимо сгенерировать открытый и секретные ключи:

 Возьмем два больших простых числа p and q.

 Определим n, как результат умножения p on q (n= p\*q).

 Выберем случайное число, которое назовем d. Это число должно быть взаимно простым (не иметь ни одного общего делителя, кроме 1) с результатом умножения (p-1)\*(q-1).

 Определим такое число е, для которого является истинным следующее соотношение (e\*d) mod ((p-1)\*(q-1))=1.

 Hазовем открытым ключем числа e и n, а секретным - d и n.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Для того, чтобы зашифровать данные по открытому ключу {e,n}, необходимо следующее:

 разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде числа M(i)=0,1,2..., n-1 ( т.е. только до n-1).

 зашифровать текст, рассматриваемый как последовательность чисел M(i) по формуле C(i)=(M(I)^e)mod n.

Чтобы расшифровать эти данные, используя секретный ключ {d,n}, необходимо выполнить следующие вычисления: M(i) = (C(i)^d) mod n. В результате будет получено множество чисел M(i), которые представляют собой исходный текст.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Следующий пример наглядно демонстрирует алгоритм шифрования RSA:

Зашифруем и расшифруем сообщение "САВ" по алгоритму RSA. Для простоты возьмем небольшие числа - это сократит наши расчеты.

 Выберем p=3 and q=11.

 Определим n= 3\*11=33.

 Hайдем (p-1)\*(q-1)=20. Следовательно, d будет равно, например, 3: (d=3).

 Выберем число е по следующей формуле: (e\*3) mod 20=1. Значит е будет равно, например, 7: (e=7).

 Представим шифруемое сообщение как последовательность чисел в диапозоне от 0 до 32 (незабывайте, что кончается на n-1). Буква А =1, В=2, С=3.

Теперь зашифруем сообщение, используя открытый ключ {7,33}

C1 = (3^7) mod 33 = 2187 mod 33 = 9;

C2 = (1^7) mod 33 = 1 mod 33 = 1;

C3 = (2^7) mod 33 = 128 mod 33 = 29;

Теперь расшифруем данные, используя закрытый ключ {3,33}.

M1=(9^3) mod 33 =729 mod 33 = 3(С);

M2=(1^3) mod 33 =1 mod 33 = 1(А);

M3=(29^3) mod 33 = 24389 mod 33 = 2(В);

Данные расшифрованы!

Алгоритм Диффи-Хеллмена

Предположим, что обоим абонентам известны некоторые два числа g и p, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют большие случайные числа: первый абонент — число a, второй абонент — число b. Затем первый абонент вычисляет значение A = gamod p и пересылает его второму, а второй вычисляет B = gbmod p и передаёт первому. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их (то есть у него нет возможности вмешаться в процесс передачи). На втором этапе первый абонент на основе имеющегося у него a и полученного по сети B вычисляет значение Bamod p = gabmod p, а второй абонент на основе имеющегося у него b и полученного по сети A вычисляет значение Abmod p = gabmod p. Как нетрудно видеть, у обоих абонентов получилось одно и то же число: K = gabmod p. Его они и могут использовать в качестве секретного ключа, поскольку здесь злоумышленник встретится с практически неразрешимой (за разумное время) проблемой вычисления gabmod p по перехваченным gamod p и gbmod p, если числа p,a,b выбраны достаточно большими.