Алгоритм RSA

Алгоритм получил свое название по первым буквам фамилий разработчиков (Rivest, Shamir, Adleman) – математиков Массачусетского технологического института. Алгоритм имеет две пары характеризующих его чисел: открытый ключ и закрытый ключ. Зашифровать сообщение и отправить его получателю может любой обладатель открытого ключа. А расшифровать сможет лишь обладатель закрытого ключа. Теоретически зная открытый ключ можно получить и закрытый, но практически на решение этой задачи необходимо настолько много времени, что расшифровка просто потеряет смысл.

Дело здесь в составе открытого и закрытого ключа. У них есть общая часть - большое число n – являющееся произведением двух простых чисел. Знание этих двух простых чисел дает возможность получить и открытый ключ и закрытый, проблема однако в том, что операция факторизации – определение из каких чисел получено данное произведение требует неимоверно большого времени счета, настолько большого, что задача не решаема даже на современных суперкомпьютерах, при условии, конечно, что исходные простые числа достаточно велики. То есть получить два больших простых числа относительно несложно, получить их произведение не составляет никакого труда, а обратная задача – задача факторизации практически не решаема. А теперь рассмотрим вычислительную схему.

Вычисление ключей

Найдем, каким-либо способом, два больших, простых числа p, q. Определим их произведение: n=p*q. Это базовое число и для открытого и для закрытого ключа, оно еще называется модулем. Далее вычислим значение функции Эйлера по следующей формуле:

$$\varphi(n) = (p-1) * (q-1)$$

Следующим шагом вычисляем число e называемое открытой экспонентой и представляющего собой второе число открытого ключа. Оно выбирается в интервале

$$1 < e < \varphi(n)$$

и оно взаимно простое с вычисленным значением функции Эйлера, то есть, эти два числа (e и значение функции Эйлера) не имеют общих делителей. Затем вычисляем закрытую экспоненту d. Оно вычисляется как обратное к e по модулю φ(n) Это записывается следующим сравнением:

$$d \bullet e \equiv 1 \,(\mathrm{mod}\, \varphi(n))$$

После выполненных расчетов в нашем распоряжении две пары чисел {n, e} – открытый ключ и {d, n} закрытый ключ. Схема шифровки с использованием открытого ключа следующая: Пусть открытый текст это число m. Тогда его шифровка выполняется по формуле:

$$c = m^e \ \mathrm{mod}(n)$$

А расшифровка по формуле

$$m = c^d \mod(n)$$

Если исходное сообщение слишком велико, то шифровка может оказаться слишком сложной арифметически. В этом случае исходное сообщение разбивается на группы чисел приемлемой длины. Но в любом случае представленный алгоритм требует больших вычислительных ресурсов, поэтому реально он используется для передачи небольших сообщений, например цифровой подписи, то если проблемы вычислительных ресурсов нет, то он будет надежным шифром для любого сообщения. Алгоритм RSA потеряет свой смысл только тогда, когда будет найден способ быстрой факторизации, с вычислительной сложностью сопоставимой со сложностью произведения двух чисел, но пока даже неясно, когда эта задача будет решена и возможно ли её решить в принципе.