МАТЕМАТИКА В КРИПТОГРАФИИ. АЛГОРИТМ RSA

Белорусского государственного университета информатики и радиоэлектроники
Минск, Республика Беларусь

А. И. Хижняк

В. Э. Жавнерчик − к. ф.-м. н.,доцент

Криптография – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации

Выбранная для исследования криптосистема RSA является асимметричной, или с открытым ключом. Суть ассиметричной криптосистемы заключается в том, что в ней используется 2 ключа – открытый (Public Key) и закрытый (Private Key). Закрытый ключ используется для шифрования данных, а открытый – для расшифровки. Закрытый ключ должен храниться в секрете (у того, кто шифрует информацию), в то время как открытый ключ можно публиковать – с его помощью любой сможет убедиться в правильности подписанного документа.

Например, документы подписываются электронной цифровой подписью с использованием закрытого ключа, а проверяется подпись с помощью открытого ключа.

Криптографические функции с открытым ключом используют так называемые «односторонние функции». Это значит, что:

– зная значение *x, f(x)* можно вычислить относительно просто;

– зная значение *y = f(x),* вычислить *x* очень сложно, и простого (эффективного) пути вычисления нет/

Другими словами, для односторонних функций, зная значение функции, практически невозможно вычислить аргумент функции за обозримый интервал времени.

В основе асинхронной системы RSA лежит задача факторизации (разложения на простые множители) двух больших простых чисел. В случае, когда число является произведением двух больших простых чисел – задача факторизации очень сложна.

Рассмотрим алгоритм RSA подробнее.

Для начала, создаются открытый и закрытый ключи. Для этого:

1) выбираются 2 случайных простых числа p и q заданного размера (имеется ввиду размер переменной в памяти ЭВМ, необходимый для хранения этих чисел);
2) вычисляется произведение $n = pg$, которое называется модулем;
3) вычисляется значение функции Эйлера $\phi(n)$ от числа n, оно будет равно
$$\phi(n) = (p - 1)(g - 1);$$
4) выбирается целое число e, такое, что $1 < e < \phi(n)$, взаимно простое со значением функции $\phi(n)$, это число называется открытой экспонентой;
5) вычисляется число d, мультипликативно обратное числу e по модулю $\phi(n)$, то есть число, удовлетворяющее условию:
$$de \equiv 1 \bmod \phi(n),$$
это число d называется секретной экспонентой, оно может вычисляться при помощи расширенного алгоритма Евклида;
6) пара $\{e, n\}$ публикуется как открытый ключ, а пара $\{d, n\}$ играет роль закрытого ключа.

После получения ключей, шифруем любое сообщение m с помощью открытого ключа, и получаем шифр c

$c = m^e \bmod n.$

Полученный шифр можем расшифровать в исходное сообщение m с использованием закрытого ключа

$m = c^{Q} \bmod n.$

Для создания цифровой подписи s, используется закрытый ключ $\{d, n\}$

$s = m^{Q} \bmod n.$

Цифровая подпись передается адресату вместе с самим сообщением (не зашифрованным). После получения адресат вычисляет прообраз сообщения из подписи:
$$m' = s^e \bmod n.$$
После чего исходное и расшифрованное из подписи сообщение сравниваются. Если $m = m'$, то подпись считается подлинной, а сообщение – целое и не искаженное.

Итак, в рассмотренном алгоритме RSA используются следующие математические понятия: функция Эйлера, простые числа, сравнение чисел по модулю и алгоритм Евклида.

Список использованных источников

1. Menezes A., P. van Oorschot, Vanstone S. 8.2. RSA public-key encryption // Handbook of Applied Cryptography. – CRC-Press, 1996. – 816 p.
2.