АЛГОРИТМ ШИФРОВАНИЯ RSA

В зависимости от структуры используемых ключей методы шифрования подразделяются на:

* симметричное [шифрование](http://www.e-nigma.ru/): посторонним лицам может быть известен алгоритм шифрования, но неизвестна небольшая порция секретной информации — ключа, одинакового для отправителя и получателя сообщения; Примеры: DES, 3DES, AES, Blowfish, Twofish, ГОСТ 28147-89
* асимметричное шифрование: посторонним лицам может быть известен алгоритм шифрования, и, возможно открытый ключ, но неизвестен закрытый ключ, известный только получателю. Криптографические системы с открытым ключом в настоящее время широко применяются в различных сетевых протоколах, в частности, в протоколах TLS и его предшественнике SSL (лежащих в основе HTTPS), а так же SSH, PGP, S/MIME и т. д. Российский стандарт, использующий асимметричное шифрование - [ГОСТ Р 34.10-2001](http://www.e-nigma.ru/stat/gost/).

На данный момент асимметричное шифрование на основе открытого ключа RSA (расшифровывается, как Rivest, Shamir and Aldeman - создатели алгоритма) использует большинство продуктов на рынке информационной безопасности.

Его криптостойкость основывается на сложности разложения на множители больших чисел, а именно - на исключительной трудности задачи определить секретный ключ на основании открытого, так как для этого потребуется решить задачу о существовании делителей целого числа. Наиболее криптостойкие системы используют 1024-битовые и большие числа.

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:

(И) C1 = (10^7) mod 33 = 100000000 mod 33 = 1;

(Н) C2 = (15^7) mod 33 = 170859375 mod 33 = 27;

(Т) C3 = (20^7) mod 33 = 1280000000 mod 33 = 26;

(Е) C4 = (6^7) mod 33 = 279936 mod 33 = 30;

(Г) C5 = (4^7) mod 33 = 16384 mod 33 =16;

(Р) C6 = (18^7) mod 33 = 61220032 mod 33 = 6;

(А) C7 = (1^7) mod 33 = 1 mod 33 =1;

(Л) C8 = (13^7) mod 33 = 62748517 mod 33 = 7;

M1=(10^3) mod 33 =1000 mod 33 = 10(И);

M2=(27^3) mod 33 =19683 mod 33 = 15(Н);

M3=(26^3) mod 33 = 24389 mod 33 = 20(Т);

M4=(30^3) mod 33 =27000 mod 33 = 6(Е);

M5=(16^3) mod 33 =4096 mod 33 = 4(Г);

M6=(6^3) mod 33 = 216 mod 33 = 18(Р);

M7=(1^3) mod 33 =1 mod 33 = 1(А);

M8=(7^3) mod 33 =343 mod 33 = 13(Л);