**Лабораторная работа**

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 и q.
* Определим n, как результат умножения p на q (n= p\*q).
* Выберем случайное число, которое назовем d. Это число должно быть взамно 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.

Пример:

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 и q=11.
* Определим n= 3\*11=33.
* Найдём (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 диапазоне от 0 до 32 (не забывайте, 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);

***Задание – создать свои открытый и закрытый ключ. Написать программную реализацию.***