Лабораторная работа №4
Двухключевая система RSA

Задание:

Построить двухключевую систему с использованием алгоритма RSA и выполнить в ней операцию шифрования и дешифрования трех первых букв фамилии студента (при количестве букв меньше 3, недостающие буквы берутся из имени). Пара простых чисел P и Q выбирается из диапазона ближайших к количеству букв в фамилии и имени студента.

Например, Петров Владимир, P (5 или 7), Q (7 или 11). Методом испытаний подбирается также ближайшая пара чисел Е и Д.

В нашем случае это могут быть P=5; Q=7;

В случае неудачных сочетаний из названного диапазона берутся рядом другие ближайшие простые числа, например, P=5, Q=13

Описание метода. В системе RSA каждый пользователь имеет свой ключ шифрования. Ключи дешифрования известны всем, а шифрующий ключ держится в секрете. Криптографические системы типа RSA подходят для реализации цифровой подписи, применяемой в системах электронных платежей и при передаче сообщений с помощью устройств телесвязи.

К недостаткам системы RSA и аналогичных ей относят ее существенно более низкое быстродействие и потребность в более длинных ключах. Наиболее эффективные реализации RSA характеризуются скоростью шифрования порядка нескольких тысяч бит в секунду. Тогда как аналогичные реализации более простых систем шифруют несколько миллионов бит в секунду. В связи с этим наиболее целесообразным применением RSA считается организация обмена секретными ключами, необходимыми для обеспечения безопасности в сетях связи.

Основная проблема для системы RSA – генерация соответствующей пары ключей. Для генерации используется следующая процедура:

1. Выбрать 2 простых числа P и Q;

2. Найти произведение N=PQ и число L=(P-1)(Q-1);

3. Выбрать случайное число D такое, что оно должно быть взаимно простым с числом L. (Числа называются взаимно простыми, если они не имеют общего делителя);

4. Определяют другое число E такое, что (ED) mod L=1;

5. Как только все числа найдены, мы имеем: секретный ключ – E; открытый ключ – пара чисел D и N;

Тогда при шифровании сообщения его разбивают на блоки M. В результате шифрования для каждого блока M получим число

$C = (M^E) \bmod N$;

При дешифрации получаем:

$M^* = (C^D) \bmod N.$

Рассмотрим это на примере алфавита из букв {А,О,Я}={1,2,3} для передачи текста «ОЛЯ» (или 2,1,3). Цифровые обозначения букв или блоков обязательны, так как метод основывается на обработке натуральных чисел.

1. Выберем P=3 и Q=11;
2. Найдем N=PQ, N=33; L=(P-1)(Q-1); L=20
3. Выберем D взаимно простое с L: D=3;
4. Выберем E такое, что $(ED) \bmod L = 1$: E=7, действительно, $(7 \bullet 3) \bmod 20 = 1$;
5. Тогда открытый ключ $\begin{matrix} D = 3 \\ N = 33 \end{matrix}$ секретный $E = 7$

Производим шифрацию своим закрытым ключом 7:

$$C1 = (M1^B) \bmod N: \begin{matrix} C1 = (2^7) \bmod 33 = 29 \\ C2 = (1^7) \bmod 33 = 1 \\ C3 = (3^7) \bmod 33 = 9 \end{matrix}$$

Зашифрованный текст получается (29,1,9)

Расшифровка текста открытым ключом 3 и33:

$$M1^* = (C1^D) \bmod N: \begin{matrix} M1^x = 29^3 \bmod 33 = 2 \\ M2^x = 1^3 \bmod 33 = 1 \\ M3^x = 9^3 \bmod = 3 \end{matrix}$$

В результате мы получили исходный текст.

Остается только добавить, что для получения достаточно стойкой шифровки необходимо брать очень большие простые числа.

Выполнение соотношения $(ED) \bmod L = 1$ позволяет использовать этот факт для проверки подлинности подписи без знания секретного ключа E с помощью аппарата ХЭШ-функций.

В практической работе необходимо идентифицировать автора электронного документа и предприятие не по особенностям подписи и печати (например, по образцам подписей и печатей в банковской карточке клиента), а по наличию у него электронного ключа для подписывания документов. В этом случае конкретное число-подпись под данным документом в фиксированное время, может сделать только законный обладатель ключа (E).

Процедура электронной подписи включает в себя два этапа: первый – подписывание (вычисление параметров подписи, зависящих от текста конкретного документа, один из которых (E) хранится в секрете); второй – проверка получателем с помощью несекретных параметров (D,N) подлинности сообщения (подписи)

Сообщение шифруется по алгоритму RSA, где E подбирается и известно только отправителю, а D, N знает и получатель. Получатель должен иметь возможность с помощью открытого ключа проверить подлинность сообщения. Для этой цели в сообщение добавляется еще одно число, которое является результатом вычисления хэш-функции h (T), зависящей от текста T.