Курс «Информационная безопасность и защита информации»

Задание 2.

Реализация криптографического алгоритма RSA

Задание

Создать приложение с графическим интерфейсом на языке C++/C#, реализующее алгоритм шифрования и расшифрования текста по алгоритму RSA.

Алгоритм

Алгоритм шифрования RSA является несимметричным алгоритмом, т.е. ключи, используемые при зашифровании и расшифровании различны.

Алгоритм формирования ключей:

1. Выбираются два случайных простых числа p и q, удовлетворяющих условию $|p| \approx |q|$. Для простоты считать данные числа 32-битными беззнаковыми (unsigned int). Во избежание выхода за пределы типа при умножении числа p и q генерировать в интервале от 0 до $2^{16} = 65536$. При генерировании чисел использовать вероятностные тесты на простоту, например, тест Ферма (см. лекции или литературу).
2. Вычисляется модуль системы RSA: $n = p \cdot q$
3. Вычисляется значение функции Эйлера от модуля системы: $\varphi(n) = (p-1)\cdot(q-1)$
4. Выбирается случайное целое число $e < \varphi(n)$, удовлетворяющее условию $\gcd(e, \varphi(n)) = 1$. Для генерации данного числа необходимо использовать алгоритм Евклида (см. лекции или литературу), который вычисляет наибольший общий делитель двух чисел. Если $\gcd(e, \varphi(n)) > 1$, то необходимо выбрать другое число e. Процедуру повторять до тех пор, пока не выполнится условие $\gcd(e, \varphi(n)) = 1$.
5. Вычисляется целое число d такое, что $ed \equiv 1 (\mathrm{mod}\, \varphi(n))$ (мультипликативно обратное числу e по модулю $\varphi(n)$. Для этого используется расширенный алгоритм Евклида (см. лекции или литературу).
6. Пара (n, e) используется в качестве параметров открытого ключа. Числа p, q и $\varphi(n)$ должны быть тщательно уничтожены. Число d используется в качестве закрытого ключа.

Алгоритм шифрования.

Исходный текст, содержащий символы, входящие в таблицу кодировки ASCII (массив unsigned char), разбивается на отдельные символы. По каждому символу вычисляется его код (например, приведением типа).

Шифрование символа осуществляется по формуле: $C = M^e (\mathrm{mod}\, n)$.

Расшифрование: $M = C^d (\mathrm{mod}\, n)$.

Возведение в степень по модулю осуществлять при помощи рекурсивного алгоритма (см. лекции или литературу).

Замечания по реализации

Программа должна содержать 4 текстовых окна:

- Окно для открытого текста. В данное окно вводится исходный текст в строковом формате, подлежащий шифрованию.
- Окно для зашифрованного текста. Для простоты шифрограмма выводится в данное окно в виде десятичных чисел, разделенных пробелом.
- Окно для открытого ключа. В данное окно выводится открытый ключ e в виде десятичного числа.
- Окно для закрытого ключа. В данное окно выводится закрытый ключ d в виде десятичного числа.