**Задание.** Программа для шифрования небольших сообщений алгоритмом RSA. В программе использована криптографическая библиотека, в которой имеется реализация RSA.

**Общие сведения.** Алгоритм шифрования RSA является алгоритмом с открытым ключом. *Для генерации двух ключей* (личного  и открытого ) абоненту B необходимы следующие действия.

1. Выбрать два больших случайных простых числа  и .
2. Вычислить  
   , .
3. Выбрать случайным образом простое число , меньшее, чем , у которого нет общих делителей (кроме 1) с числом  (взаимно простые числа). Числа  и  составляют открытый ключ абонента B: .
4. С помощью обобщенного алгоритма Евклида вычислить число  ( – инверсия  по модулю ), такое что остаток от деления  на  был равен 1: . Числа  и  составляют личный ключ абонента B: .

Абонент A *шифрует сообщение*  по формуле



и пересылает шифротекст  участнику B по открытой линии.

Абонент B, получивший зашифрованное сообщение, *вычисляет открытый текст* по формуле

.

Для шифрования большого сообщения оно разбивается на блоки .