Задача 3. Алгоритм RSA

Имя входных файлов: задается в параметрах командной строки
Имя выходного файла: стандартный вывод
Ограничения по времени: -
Ограничения по памяти: -

Реализовать следующие алгоритмы работы с длинными числами и алгоритмы, реализующие арифметику сравнений:

1. Add – сложение двух чисел по модулю N
2. Multiply – умножение двух чисел по модулю N
3. ModExp – возведение в степень по модулю N
4. Euclid – алгоритм Эвклида
5. ExtendedEuclid – расширенный алгоритм Эвклида
6. Primality – проверка числа на простоту
7. Primality2 – проверка числа на простоту
8. GetRandomPrim – получение случайного простого числа
9. Алгоритм RSA

Величину разрядности *n* выбрать в зависимости от номера варианта:

№№ вариантов	**Разрядность, бит**
1, 6, 11, 16	128
2, 7, 12, 17	256
3, 8, 13, 18	512
4, 9, 14, 19	1024
5, 10, 15, 20	2048

Формат входных данных

Для алгоритма Add:
`<project> mul <mod> <file1> <file2>`
Для алгоритма Multiply:
`<project> mul <mod> <file1> <file2>`
Для алгоритма ModExp:
`<project> mod <mod> <file1> <file2>`
Для алгоритма Euclid, ExtendedEuclid:
`<project> euc <file1> <file2>`
`<project> eucx <file1> <file2>`
Для алгоритма Primality, Primality2:
`<project> prim <file1>`
`<project> prim2 <file1>`
Для алгоритма GetRandomPrim:
`<project> rnd`
Для алгоритма RSA:
`<project> rsa <file1>`

Пусть
x – значение, записанное в `<file1>`;
y - значение, записанное в `<file2>`,
N – значение, переданное параметром `<mod>`.

Формат выходных данных

Для алгоритма Add: значение `x+y mod N`
Для алгоритма Multiply: значение `x*y mod N`
Для алгоритма ModExp: значение `x^y mod N`
Для алгоритма Euclid: `НОД(x, y)`
Для алгоритма ExtendedEuclid: пара чисел, возвращаемых алгоритмом Extended uclid
Для алгоритма Primality, Primality2: `1` – если число простое, `0` – если составное.
Для алгоритма GetRandomPrim: случайное число.
Для алгоритма RSA: необходимо продемонстрировать пошаговую работу алгоритма с выводом промежуточных результатов, а также осуществить проверку правильности шифрования, проведя дешифровку полученного закодированного числа.