Лабораторная работа №1

Общие требования: все программы должны корректно обрабатывать операции с числами порядка 10^9.

Написать криптографическую библиотеку с тремя функциями.

1) Функция быстрого возведения числа в степень по модулю. Данная функция должна позволять находить значение y в уравнении $y = a^x \bmod p$.
2) Функция, реализующая тест простоты Ферма. Функция должна определять, является ли число простым с высокой вероятностью.
3) Функция, реализующая обобщённый алгоритм Евклида. Данная функция должна позволять находить наибольший общий делитель НОД (a, b) и обе неизвестных x, y из уравнения $ax + by = \text{НОД}\ (a, b)$.

   Предусмотреть возможности:

   - ввода a, b с клавиатуры;
   - генерации a, b внутри функции;
   - генерации a, b внутри функции таким образом, чтобы a, b являлись простыми числами (с вызовом функции проверки на простоту тестом Ферма).