Лабораторная работа №2.

1. Пользователем вводится целое число m.
    1. Напишите программу, выводящую все простые числа, которые меньше m.
    2. Выведите на экран приведенную систему вычетов по модулю m.
    3. Напишите функцию, вычисляющую значение $\varphi(m)$, где $\varphi(m)$ −функция Эйлера.
    4. Напишите программу, представляющую число m в каноническом разложении по степеням простых чисел.
2. Разработайте программы шифрования и дешифрования данных с помощью алгоритмов Эль-Гамала и Рабина.
3. Реализуйте алгоритм быстрого возведения в степень в кольце вычетов.
4. Реализуйте алгоритм RSA.
5. Арифметика в $GF(256)$.
    1. Напишите функцию, представляющую элемент из $GF(256)$ в полиномиальной форме.
    2. Напишите функцию, умножения двух двоичных многочленов; умножения двух элементов из $GF(256)$.
    3. Напишите функцию, для поиска мультипликативного обратного для элемента из $GF(256)$.
6. Разработайте процедуры, осуществляющие сложение, умножение и деление в полях двоичных многочленов большой степени.
7. Разработайте приложение, обеспечивающее безопасность данных на основе алгоритма Rijndael. Реализовать возможность выбора длины блока шифротекста и длины ключа.