Assignment 04 – math for cryptography

Learning Objectives:

* To review modular arithmetic, and prime numbers
* Warm up to RSA by creating some functions used in the RSA algorithm

**Coding Workbench**

You can use any language you like. Python is recommended.

Test out these functions with a main (driver) program. Everyone can be in one file (example: prime.py) Please add comments/headers to explain what you are doing, and include your name, etc. We will be using these functions later.

1. Write a function getMod(b,e,m) that returns the modulus given 3 input parameters (the base, the exponent, and the modulus). Some test inputs:
   * 515 (mod 13)
   * 1518 (mod 17)
   * 45618 (mod 17)
   * 145102 (mod 101)
   * 143 (mod 12)
2. Write a function isPrime(x) that returns true if the number x is a prime number. Write a driver to test out a few numbers.
3. Write a function listPrimes(n) that returns an array of all the numbers between 3 and “n” that are prime numbers.
4. Write a function gcd(a,b) that returns the greatest common divisor between “a” and “b”.