Computer Science & Engineering Department
I. I. T. Kharagpur

Computational Number Theory: CS60094

Assignment - 2 (Marks: 10)

Return on or before: *15th April, 2015*

Write a *Python* function `isPrimeMR(n, k)` to implement the *Miller-Rabin* test for prime. The first parameter n is an odd positive integer that is tested. The second parameter is the number of iterations for the test. This function calls `modExp(a, k, n)` that computes $a^k \bmod n$ by repeated squaring.

Write a `Python` program that takes a positive integer l, $2 \leq l \leq 128$ as input. It generates and prints a *random prime* p, $2^l \leq p < 2^{l+1}$.

In a loop an integer n, $2^l \leq n < 2^{l+1}$ is generated at random. The function `isPrimeMR(n, k)` is called to test whether n is prime. If n is a prime, the program terminates by printing n; otherwise the loop continues.

The name of the python program file should be: *roll number*.2.`py`. Kindly do not import name and use Python-2.
Send it to `goutamamartya@gmail.com`

Make sure that the assignment reaches me on or before the date. It will not be possible to accept any assignment after *15th April, 2015*.