Project Proposal

“Implementation and Comparison of various Primality Testing Algorithms in JAVA”

Goal: The goal of this project is to

a. Implement the below mentioned Primality Test Algorithms
   1. AKS Primality Test
   2. Miller Rabin Primality test
   3. Solovay-Strassen Test
   4. Fermat's test
   5. Lucas-Lehmer primality test for Mersenne numbers
   6. Gordon's Algorithm for primality testing
   7. Maurer's algorithm for generating provable primes.

b. Analyze each algorithm and do a comparative study of the above mentioned algorithms

References:
Handbook of Applied Cryptography: Chapter 4.