Progress Report for Course Project in Advanced Probelm Solving

1) Title of the Project:

Comparison for Determinstic and Probabilistic algorithms for Primality Test

2) Team Memebers:

i. Vivek Patare (201821078)
ii. Tarun Vatwani (2018201075)

3) Deliverables:

i. Implementing following Probablistic and Determinstic algorithms:
   a) Probabilistic
      1) Lehmann's Test
      2) Solvay- Strassen's Test
      3) Miller-Rabin Test
   b) Determinstic
      1) Trial Division Method
      2) AKS Primality Test
ii. Comaprisons between all the algorithms on the basis of accuracy and time complexity
iii. Finding a tradeoff between accuracy vs time complexity (i.e determinstic vs probablistic methods)

4) Project Delivery Plan:

i. First Week: Understanding the mathematical proofs and working of all the above mentioned algorithms
ii. Second Week: Implementation of all the algorithms
iii. Third Week: Tetsing and result conclusion, report writing

5) Technologies to be used:

i. c++14 library (For code implementation)
ii. GNU MP Bignum Library (For handling big integers)
iii. Python Matplotlib library (Plotting Graphs)
iv. Python Notebook / ORG mode emacs (For reporting)

6) Online Resources:

i. Martin Dietzfelbinger. Primality testing in polynomial time: from randomized algorithms to" PRIMES is in P", volume 3000. Springer, 2004.
ii. Bobby Kleinberg: The miller-rabin randomized primality test
http://www.cs.cornell.edu/courses/cs4820/2010sp/handouts/MillerRabin.pdf
iii. William Rundell: Primality testing
http://calclab.math.tamu.edu/~rundell/m470/notes/primality.pdf
iv. Implementation of AKS algorithm
https://www.cs.cmu.edu/afs/cs/user/mjs/ftp/thesis-program/2005/rotella.pdf
v. GMP Library Manual
https://gmplib.org/gmp-man-6.0.0a.pdf

7) Repository Link:

https://github.com/vivek-2018201078/APS_PROJECT_2018

8) Testing Plan:

i. Based on implementation of algorithms, test cases (whose desired output is known) are generated
ii. Test cases can be based on size of input, testing on known prime numbers, composite numbers etc.
iii. Test results are to be recorded for different algrithm (based on implementation) and comparision between them
iv. Recording Accuracy and time for each test case designed to beter understand each algorithm
v. Plotting Graphs to get better insight about test case output

9) End User Documentation:

i. Detailed report will provide all necessary info about algorithm and its analyis on test cases
ii. For user level tesing, user can provide input data as numbers in file (Each number on new line) and can test if number is prime or not.
iii. Based on analysis done on different test cases heurstic can be developed to optimize which algorithm can be used for output based on parameters like accuracy and speed