Number Theory and Cryptography (IT462) Program -5

Write a program that should demonstrate **Pollard Rho** factorization method.

Steps:

a. Consider run-time input positive integer "N" of any size, X and Y. Verify given input (numbers) is positive integers are not. If all of them are positive integers then find the factors for given "N" else terminate the program by displaying an error message.

b. Verify whether the derived factors are prime or not using any primality test.

c. Print all intermediate results as well as final output on terminal. Further, store all intermediate results as well as final output into an output file.

Note: You may use Extended Euclidean Algorithm to compute GCD of given two numbers.

Sample Text Case:

Input : N= 203299, X=2, Y=2

Submit program as well as screenshots of the output to it35215b@gmail.com before the deadline. Email Subject should be NTC(IT462)-Lab-Program-5

File name of the program : RegisterNo_IT462_P5

(P5 indicates Program Number-5)

File name of the screenshot : RegisterNo_IT462_P5_S1

(S1 indicates screenshot for the first test case, similarly, for other test cases S2, S3, S4, S5)

Date of Laboratory : 30th August 2019

Dead Line of Submission : 30th August 2019 (on or before 5:30PM).

Note: Kindly clarify the doubt(s) (if any related to the said program) before commencement of the laboratory.