Criptografia i Seguretat [104355]

Activity Cryptographical Mathematical Background

In these set of exercises you are required to implement the specified code described in the questions.

1. Make a program that for a given number n tells wether it is prime or not looking for factors in $[1 : n]$.
2. Make a program that for a given number n tells wether it is prime or not looking for factors in $[1 : n/2]$.
3. Make a program that for a given number n tells wether it is prime or not using Fermat's theorem.
4. Run your programs for one minute looking for primes.
5. Draw a graph (x-axis number, y-axis time) using both programs to calculate the time spent for every number.
6. Calculate $\phi(46)$
7. Calculate $inv(7, 46)$ using Euler's theorem.
8. Calculate $inv(9, 27)$ using Euler's theorem.
9. Calculate $inv(7, 25)$ using the Extended Euclides algorithm.
10. Calculate $19^{75} \mod 63$ using the Fast exponentiation algorithm.