

THE TOPIC OF A COMPETITION PROMOTING STUDENT ENGAGEMENT IN SCIENTIFIC ACTIVITIES

Topic: Factorization of large semiprimes

Goal: Investigation of algorithms for RSA numbers factorization

Short description:

The main objective of this work is to study and apply algorithms for factorization of large numbers. During the work, the student will learn to use parallel calculations, and will also be able to try to modify existing algorithms.

The student will investigate factorization of RSA numbers. RSA numbers are a set of large semiprimes (numbers with exactly two prime factors) that were part of the RSA Factoring Challenge. The aim of the challenge was to find the prime factors of each number.

The student will be required to factorize numbers: RSA-100 and RSA-110.

Supervisor: prof. dr. Dmitrij Šešok