The Factorisation by Bases Algorithms, A Case Study

Bracely Magombedze
Harare Institute of Technology

Abstract:

One of the most difficult challenges in number theory and cryptography is the problem of factoring large integers since factoring large numbers more than 200 digits remain difficult. This difficulty has been useful in proving the strength of the RSA encryption scheme, which uses two large numbers of similar size. In this work, we introduce factorisation by bases algorithms (FBA) and implement them on the RSA-numbers defined by the RSA challenge. We analyse the time spent on factoring to check the speed and efficiency of each algorithm.