

MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik

SJÄLVSTÄNDIGT ARBETE I MATEMATIK

Fredagen den 7 juni kl. 13.00–14.00 presenterar Joakim Marklund sitt arbete “The art of integer factorization” (15 högskolepoäng, Grundnivå).

Handledare: Johan Andersson

Plats: Sal 32, hus 5, Kräftriket

Sammanfattning:

Multiplying integers together is a task that can be quickly done by computers, but the process of doing the reverse is a completely different story as there is no simple way to easily decompose any given integer into its proper factors.

In this paper we will give an overview for the techniques used to efficiently factorize integers of different types. We review some of the most common algorithms within the area of integer factorization with details describing the underlying methods together with examples for the sake of illustration.

We also look at some applications to why this is an interesting area of study and why it is considered a big part of modern cryptography.

Alla intresserade är välkomna!