MATEMATISKA INSTITUTIONEN
STOCKHOLMS UNIVERSITET
Avd. Matematik

SJÄLVSTÄNDIGT ARBETE I MATEMATIK

Onsdagen den 5 oktober kl. 10.00–11.00 presenterar Mihai-Dinu Lazarescu sitt arbete "Elliptic Curves Gone Cryptic" (30 högskolepoäng, grundnivå).

Handledare: Rikard Bögvad

Plats: Sal 21, hus 5, Kräftriket

Abstract: Ever since the dawn of civilization human beings have exchanged information and occasionally secret information. Irrespective of the method of encryption these questions can be addressed mathematically.
The public key cryptosystems are built on group theory or lattice theory. I shall consider the group theoretical variant. The security of these systems relies on two hard mathematical problems: the discret logarithm problem and the prime factorization problem. I shall consider only the former. The standard group in use is a finite field yet lately a more exotic group has come to the fore, viz. the additive group of an elliptic curve, over a finite field.

Alla intresserade är välkomna!