Oberseminar Theoretische Informatik
Wintersemester 2009/2010

Dr. Gábor Farkas

Primality and cryptography

Montag, 26.10.2009 14:00 (c.t.) Seminarraum 3319 (Ernst-Abbe-Platz 2, 3. Stock).

The evolution of computers in the last decades changed the cryptographic methods significantly and redefined the notion „computable“ in number theory. Since the speed of the basic arithmetical and algebraic operations has a direct effect even for the speed of the algebraic operations and complicated number theoretical computations, therefore their implementation play an important role in modern cryptography.

In line with the improvement of encryption/decryption schemes, primality testing and factorization methods are studied by „ccomputational number theory“.

In this talk we would like to investigate the question whether the tools and results of theoretical mathematics can promote the implementation of above mentioned algorithms. We concentrate our attention to the elliptic curves.

Homepage:
http://theinf1.informatik.uni-jena.de/teaching/ws0910/oberseminar-ws0910