Hard Problems in Number Theory arising from Cryptography

Kristin Lauter
Microsoft

Many hard problems in number theory have arisen from applications in cryptography, inspiring new directions and techniques for mathematical research. The hardness of factoring integers has been intensely studied over the last 35 years thanks to the well-known public key cryptosystem RSA. However there are many other interesting problems which arise from cryptography and which relate to deep areas in number theory. For example the problem of generating elliptic curves for use in cryptography is related to explicit class field theory and Kronecker's Jungendtraum. Many other cryptographic constructions involve interesting number theory, such as elliptic divisibility sequences, the Tate-Shaferevich group, Stark's conjectures, the Hecke graphs, Weil pairings, etc. This talk will survey some of the interplay between cryptography and number theory.