The Mathematics of Cryptology: An Overview

Phong Nguyen

INRIA and ENS, France

http://www.di.ens.fr/ pnguyen/

Resumen

Cryptology uses more and more mathematics, and this trend is unlikely to stop. Back in 1978, the first public-key cryptosystem by Rivest, Shamir and Adleman (RSA), only used basic modular arithmetic. Nowadays, non-elementary mathematical objects such as pairings over elliptic curves have become mainstream in cryptology.

In this talk, we will survey the mathematics used in modern cryptology, and we will try to explain why cryptology seems to require more and more mathematics.

No prior knowledge of cryptology will be required. For a different take on the relationship between mathematics and cryptography, one might be interested in reading a non-technical publication by Neal Koblitz which appeared in the Notices of the AMS, in 2007: http://www.ams.org/notices/200708/tx070800972p.pdf