Mathematics Department Colloquium

Organizer: Maciej Zworski

Thursdays, 4:10–5:00pm, Evans 60

March 16 **Alice Silverberg**, UC Irvine

Some Applications of Number Theory and Algebraic Geometry to Cryptography

We will discuss cryptography based on the discrete logarithm problem in multiplicative groups of finite fields, including an introduction to the Diffie-Hellman, ElGamal, and XTR cryptosystems. We will show that studying the underlying mathematics of these systems leads to interesting questions about algebraic tori, which in turn lead to new cryptosystems (such as the CEILIDH cryptosystem).