

CALIFORNIA STATE UNIVERSITY, LONG BEACH

THE MATHEMATICS COLLOQUIUM

presents

Alice Silverberg

University of California, Irvine

speaking on

Some applications of number theory and algebraic geometry to cryptography

Friday, April 29, 2005

12:00PM-1:00PM

LA5-267

Abstract: Public key cryptography is based on ideas from number theory. We will discuss Diffie-Hellman key exchange and ElGamal signature and encryption schemes, and some recent improvements on them. We show how number theory and algebraic geometry can be used to give new cryptosystems and a deeper understanding of them.