Mathematics, Statistics, and Computer Science **@ UIC**

Graduate Student Colloquium

An Introduction to the Theory of Cryptography

Adam Lelkes (UIC)

Abstract: This talk will be a brief introduction to the beautiful theoretical results in cryptography. Time permitting, we will answer questions such as: 1. Can you have perfect encryption? (Spoiler: yes, but it is impractical.) 2. Is there a notion of security that is practical but still hard enough to break? If so, can we achieve it? 3. Can we algorithmically generate pseudo-random bits? How random is random enough? 4. Is it possible to convince someone you proved the Riemann hypothesis without revealing any information at all about the proof itself? 5. You are talking to your friend on the phone and you want to decide an important question by flipping a coin. How can you make sure that your friend didn't lie about the result of the coin toss?

Monday, August 31 at 4:00 PM in SEO 636