Computer Science Seminar

Perfect Secrecy vs. Computational Security in Private Key Encryption Schemes

Steven La Fleur
Emory University

Abstract: As evidenced by recent events, privacy and security of data is increasingly important. There is a lot of interest in the ability to securely encrypt and send messages between two parties in such a way that any potential eavesdropper will be unable to read the message. But what does "security" of an encryption scheme mean, and how do we measure how secure a given scheme is?

In this talk we will investigate formal definitions for security of an encryption schemes, and what it means to prove that an encryption scheme is secure using these definitions. We will consider the practical drawbacks of "perfect secrecy" and how the definitions and assumptions made for computational security fix these drawback while still maintaining secrecy from attackers of different strengths.

The talk is intended for undergraduate students who have taken a course in discrete mathematics for computer science and have a basic understanding of probability, theory of computation and rigorous proof.

Monday, May 22, 2017, 4:00 pm
Mathematics and Science Center: W301

Mathematics and Computer Science
Emory University