The SUMO Speaker Series for Undergraduates

Thursday, Novenber 20th
4:15-5:05, room 380C
(Food Provided)
Square Roots Modulo n and Secure Coin Flipping

PhD student Jeremy Booher

Abstract:

Given an integer that is known to be a square modulo n, how would one compute its square root? I will discuss such an algorithm and how to use it to simulate a coin flip without the possibility of cheating. The algorithm uses randomness to find a number which is not a square: time permitting I will discuss how trying to avoid randomness leads to hard problems in number theory

.sumo.stanford.edu/speakers