The SUMO Speaker Series for Undergraduates

Thursday, November 15th

4:15-5:05, room 380C

(Food Provided)

Can you hear the deciban? Decoding the Traffic from the Enigma Machine: Combining Group Theory, Statistics and Information Theory.

Professor Susan Holmes

ABSTRACT:

I will explain how the Enigma machine worked and how the Polish mathematicians Jerzy Rozycki, Henryk Zygalski and Marian Rejewski used Group Theory to discover the wirings and break the original code. Alan Turing complemented this with Information Theory and Statistics. I will give a description of how Turing built on the discoveries made by the Poles on the cycle structure of groups and the mechanization of code breaking to decode the Naval Enigma's Traffic. His information approximation methods and statistical work with IJ Good would have started the era of modern Bayesian statistics if only it had been made public. His work on codebreaking machines started the world of modern computer science. I will explain some of the techniques used by the codebreakers of Bletchley Park that enabled the `Ultra' mission to succeed.

sumo.stanford.edu/speakers