

The SUMO Speaker Series for Undergraduates

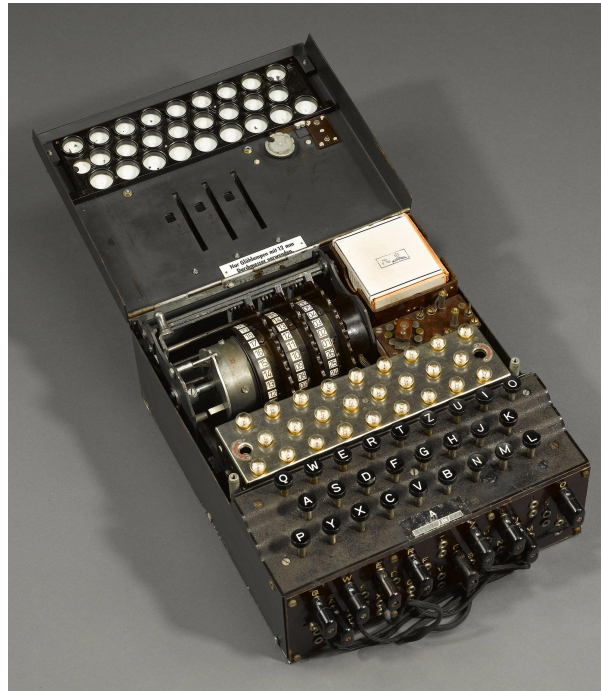
(Food Provided)

Wednesday, January 25th

4:15-5:05, room 380C

Cracking the Enigma

Rebecca Bellovin



ABSTRACT:

Enigma was a family of related machines used to encrypt German military traffic during the 1930's and World War II. Although the Germans considered it unbreakable, Polish and British mathematicians found ways to read messages encrypted with Enigma. I will talk about the mathematics behind the initial Polish break, and if time permits, I will sketch some of the later work at Bletchley Park.

sumo.stanford.edu/speakers