DEPARTMENT OF MATHEMATICS

Fall 2023 MATH Colloquium Series

Encryption via Permutations and Breaking the Enigma Machine

Dr. Tyler Evans

Professor, Cal Poly Humboldt

One way to encrypt a message is to choose some permutation, τ, of the letters in the alphabet and replace each letter x in the plain text message with τ(x). Any such encryption scheme turns out to be easy to break by analyzing the frequency distribution of each alphabet letter in the language. In the period between the two world wars, the German military began using the Enigma Machine to make such encryption schemes more difficult to break by constantly changing the permutation τ as the message was encrypted. In this talk, we will look at the structure of early Enigma machines and understand the means by which they encrypted messages. We will examine some of the ideas from group theory discovered by the Polish mathematician Marian Rejewski (1905 -1980) to assist in the eventual breaking of the Enigma Machine. The talk is open to all interested audience members. Abstract algebra students are particularly encouraged to attend.

September 28, 2023
Thursday

4:00 PM
BSS 166

FOR MORE INFO GO TO HTTPS://MATH.HUMBOLDT.EDU/GET-INVOLVED/MATHEMATICS-COLLOQUIUM

WE CORDIALLY INVITE YOU TO THE PRE-COLLOQUIUM TEA IN BSS 312
AT 3:30 PM