Code Wars:
The Joys and Perils of Mathematical Cryptography

Prof. Stefan Erickson
Colorado College

Pikes Peak Regional Undergraduate Mathematics Conference
March 1, 2024

Cryptography has long been a cat-and-mouse game between those who create new methods of encryption and those who find weaknesses in the methods. The earliest computers were used at Bletchley Park in order to break German ciphers during World War II. The stakes have never been higher, with cryptography forming the backbone of modern cybersecurity. There are constantly new applications, including digital signatures and cryptocurrencies.

We'll dive into this historical battle between cryptographers and cryptanalysts. We'll see how a 250-year old theorem in number theory is the basis for a public-key encryption system known as RSA. The rise of quantum computers will eventually make this cryptosystem obsolete, potentially putting much of internet security at risk. After decades of research, cryptographers have new tools ready that are currently believed to be resistant to quantum algorithms. However, the search goes on for new and more efficient methods of encryption. I encourage you to come along for the adventure!