Department of Mathematics and Computer Science

Thursday, April 27, 2023, 3:00 pm

COLLOQUIUM TALK

Speaker: Tyler Billingsley (Rose-Hulman)

Old Main 2210

Communication and Cryptography: the Mathematics of Error-Correcting Codes

Abstract:

Coding theory is the mathematical theory of codes, the objects which facilitate digital communication. The theory was pioneered by Richard Hamming, a mathematician at Bell Labs who discovered the first error-correcting code in 1950 – that is, a code that can not only detect a transmission error caused by a noisy channel, but also correct it. One of the many applications of coding theory is to cryptography, where mathematicians such as McEliece and Niederreiter used difficult problems in coding theory to facilitate secure communication. In this talk, we will discuss the basics of coding theory, the difficult problem that makes coding theory relevant to researchers in post-quantum cryptography, and some of the speaker's work involving the cryptosystem BIKE that is being considered for post-quantum standardization by NIST. Attendees will be assumed to have some familiarity with basic linear algebra.