VCU Discrete Mathematics Seminar

Code-based cryptography and graphical representations

Prof Gretchen Matthews (Virginia Tech)

Wednesday, Nov. 9
1:00-1:50 EST

Live in 4145 Harris Hall
& Zoom @ `https://vcu.zoom.us/j/92975799914`
`password=graphs2357`

How do we store private information? How do we communicate information securely? Answers to these questions are changing as computational capabilities change. Addressing them is vital not only to our national security but also our everyday existence, impacting commerce, healthcare, and the ways we interact with one another. Quantum computing poses a threat to current encryption schemes, such as RSA and elliptic curve cryptography, which underpin nearly all digital transactions. Public key encryption as we know it succumbs to Shor's Algorithm, making a replacement necessary. The National Institute of Standards and Technology (NIST) is in the process of standardizing cryptosystems which are post-quantum secure, meaning are resilient in the face of quantum algorithms. In this talk, we share modernizations of McEliece's 1978 code-based cryptosystem which are based on graphs.

For the DM seminar schedule, see:

`https://vcumath.github.io/Seminar/dms.html`