Oklahoma State University — Department of Mathematics

Distinguished Colloquium Speaker

Supported by the Vaughn Foundation Professorship in Number Theory

How Quantum Computers Will Kill Bitcoin and Break the Internet, and What We Can Do About It

Dr. Joseph H. Silverman
Professor of
Mathematics
Brown University

Friday,
November 5, 2021
3:30 PM
SSH Building
Room 035

What do internet commerce, online banking, and updates to your phone apps have in common? All of them depend on modern public key cryptography for security. You've probably heard of the RSA cryptosystem, which is used by many internet browsers. A digital signature scheme called ECDSA that is based on elliptic curves is used by many applications, including for example Bitcoin. All of these cryptographic systems are doomed if/when someone (NSA? Russia? China? the hacker who lives next door?) builds a full-scale operational quantum computer. It hasn't happened yet, as far as we know, but there are vast resources being thrown at the problem, and slow-but-steady progress is being made. So the search is on for cryptographic algorithms that are secure against quantum computers. In this talk I'll discuss a mix of math and history and prognostication centered around the themes of quantum computers and public key cryptography. No background in either of these subjects will be assumed.