G. Milton Wing Lecture Series

Fall 2014

Susan Landau

http://privacyink.org/

Landau is a number theorist, cryptographer, and cybersecurity expert who has held many positions in both academia (UMass, Wesleyan) and industry (Sun Microsystems, Google). She is currently a professor of cybersecurity policy in the Department of Social Science and Policy Studies at Worcester Polytechnic Institute.

What's Significant in the NSA Revelations *Public Lecture*

October 22, 5–6:15 p.m., Hubbell Auditorium

Did the documents released this summer cause irreparable harm, or were these facts that should be publicly examined? What are the facts, anyhow? This talk puts the NSA revelations in context, explaining what's new, why it matters, and what might happen next. This area is so densely overlaid by laws and secret rulings that even the lawmakers who created it can't always see inside. So part of the talk will simply clear the underbrush to get a feel for the general shape of the forest; then I will discuss what's new, what was already known (by anyone paying attention), what was surprising, and what is most disturbing.

Cryptography and Privacy—and the Role for Mathematicians—I and II

October 23, 2–3 p.m., Gavett Hall, Room 202

October 24, 1–2 p.m., Goergen Hall, Room 108

In 1977, the National Bureau of Standards announced a block-structured algorithm designed by IBM and using a 56-bit key would be the new Data Encryption Standard (DES). Its design, which had been vetted by the National Security Agency, was considered suspect; its key length, even more so. In the same year, Rivest, Shamir, and Adleman announced a public-key cryptosystem for transmitting information securely over an insecure channel. The RSA algorithm was dependent on factoring integers being computationally hard—but no one knew that was true (that is, there was no lower bound on how hard it is to factor). In the nearly 40 years since that time, we've developed some mathematical theories for cryptography and some understanding of what privacy might mean from a mathematical standpoint. In these two talks, I will illuminate the types of insights mathematicians have brought and can bring to important technical and policy issues in cryptography and privacy.

UNIVERSITY COMMUNICATIONS • 1310-50-914DC

Lecture Series Sponsored by the Department of Mathematics

UNIVERSITY of ROCHESTER