Dan Shumow from Senior SDE at Microsoft Research

Friday, April 18, 2014 - 2:30pm
Loew Hall 101

From Algebraic Geometry to Politics: How Cryptography Connects Abstract Mathematics and Everyday Life

Cryptography is the mathematical science of keeping secrets and maintaining trust. Once an arcane study of primarily military significance, over the past several decades the advent of the internet has invigorated this science. There are now results in cryptography that draw from some of the most abstract branches of mathematics, such as Number Theory and Algebraic Geometry. While at the same time the applications of cryptography have proliferated widely. From the cellphones, to communications, to our personal data held in "the cloud" and the entertainment media we consume it is difficult to find a place where cryptography is not a part of modern life. Furthermore, government surveillance and electronic warfare have pulled it into the world of politics. This talk will focus on how the abstract mathematics used in cryptography have become of integral importance to the practical concerns of everyday life. To provide illustration I will draw on several examples of cryptography our daily lives and the news and discuss the underlying Mathematics.

Related Links:
Pacific Institute for the Mathematical Sciences