APPLIED MATHEMATICS COLLOQUIUM

Breaking ENIGMA: Applied Group Theory in Action

DAVID GOLDSCHMIDT
Center for Communications Research
Princeton, NJ

During World War II and in the years leading up to it, most German military wireless communications were encrypted by a cipher machine known as the ENIGMA. Thousands of these machines were deployed in all branches of the Nazi armed forces. In one of the most significant intelligence coups in history, the Allies were able to routinely read vast quantities of this traffic, even though the Germans believed the machine to be 100% secure. In this expository talk, I will describe the ENIGMA and give a hands-on demonstration with an actual machine. I will then discuss several of the mathematical ideas which were used to break it.

MONDAY, FEBRUARY 28, 2005
4:15 PM
Building 4, Room 231

Refreshments at 3:30 PM in Building 2, Room 349.

Applied Math Colloquium: http://www-math.mit.edu/amc/spring05
Math Department: http://www-math.mit.edu

Massachusetts Institute of Technology
Department of Mathematics
Cambridge, MA 02139