מכון איינשטיין למתמטיקה
האוניברסיטה העברית בירושלים
THE HEBREW UNIVERSITY OF JERUSALEM
Einstein Institute of Mathematics

הרצאת אשנב למתמטיקה חגיגית
על ידי זוכה פרס אוסטרובסקי 2017

Prof. Akshay Venkatesh
(Stanford)

Cryptography and the geometry of algebraic equations

Modern cryptography makes essential use of finite groups.

Despite the fact that mathematics is awash with interesting finite groups, it is surprisingly hard to find groups that are useful for cryptographic purposes. Most of the few available examples come from algebraic geometry - e.g. elliptic curves.

The analysis of these examples is tied in with some of the fundamental themes of 20th-century mathematics. I will explain this story, and speculate a bit on potential generalizations.

הרצאות אשנב מיועדות (בעיקר) לתלמידי תואר ראשון במתמטיקה בשנתם השניה והשלישית. מטרתם להציג נושאי מחקר מתמטי עכשויים בצורה נגישה.

פרס אוסרטובסקי יוענק למרצה, מהבולטים במתמטיקאים בעולם, יום אחר כך. ההרצאה תינתן באנגלית.

יום ד', 24.1.2018, בשעה 18:00
אולם 2 מתמטיקה
קרית אדמונד י. ספרא (גבעת רם)

לאחר ההרצאה יוגש כיבוד!

math.huji.ac.il