CSC 85030 Combinatorial group theory and cryptography
Professor Delaram Kahrobaei
Wednesdays, 4:15 – 6:15 pm

Description: This is an interdisciplinary course focused on applications of non-commutative groups in cryptography.

Cryptography is usually considered an area of computer science; however, there are areas of cryptography (most notably, public-key cryptography), where several different areas of mathematics find their important applications. Until recently, mathematics used in cryptography was "commutative", which means cryptographic primitives were based on commutative rings or commutative (finite) groups. Also, most of the cryptographic constructs which are used in practice today rely on a small handful of computational assumptions related to factoring and discrete logs (e.g. RSA, Diffie-Hellman). A number of alternatives have surfaced, beginning with elliptic curve cryptosystems and more recently with lattice-based constructions.
The basic objective of the present course is to introduce and employ new computational assumptions, coming from combinatorial group theory, in public-key cryptography.

Along the way, we will give a solid background in combinatorial group theory, from classical methods of Nielsen, Whitehead, Tietze, etc, to modern directions, with a focus on algorithmic problems and their complexity.