Section 1:

Number theoretic methods in cryptography:

The objective of the course is to study computational number theoretic methods with an emphasis on applications in cryptography. Topics will include classical algorithms for factoring integers, like the number field sieve and Lenstra's elliptic curve factorization; and exciting recent developments including pseudo polynomial time algorithms for discrete logarithms in small characteristic finite fields, Diem's algorithm for the elliptic curve discrete logarithm problem and regularity assumptions in Grobner basis methods for finding zeroes of elliptic curve summation polynomials. Further applications in lattice based cryptography, coding theory and quantum computation will also be covered.

Section 2:

CS 101: Projects in Machine Learning
9 Units (0-9-0)
Prerequisite: CS 155 or equivalent
Instructors: Yisong Yue and Omer Tamuz

Description:

This is a project-based course for students looking to gain practical experience in machine learning. Students are expected to be proficient in basic machine learning. Students will work in groups. Each group will be provided a project topic to work on along with domain expert advisors. Alternatively, students can propose their own projects, subject to approval by course instructors.