CO 485/685: The Mathematics of Public-Key Cryptography

Instructor: David Jao

Course Outline. An in-depth study of public-key cryptography and number-theoretic problems related to the efficient and secure use of public-key cryptographic schemes. Topics to be covered may include:

- *Algorithmic number theory*: primality testing, integer factorization problem, discrete logarithm problem, elliptic curve discrete logarithm problem.
- *Public-key encryption*: RSA, ElGamal.
- *Signature schemes*: RSA, Schnorr, ECDSA.
- *Key establishment*: Diffie-Hellman and variants.
- *Provable security*: Security definitions, security models, security proofs.
- *Elliptic curve cryptography*: Bilinear pairings, isogeny-based cryptography.

References. The course textbook is:

- Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman, *An Introduction to Mathematical Cryptography*, second edition, Springer-Verlag, 2014.

The book is available online.

Prerequisites. This course assumes knowledge of abstract algebra and elementary number theory. Students without such background should read Sections 1.3–1.5, 2.8, and 2.10 of the course textbook.