This course will cover a broad aspect of modern cryptography from a mathematical perspective. This will include public key cryptosystems, digital signatures, identification and secret sharing schemes and to delve beyond the first level we will need both algebraic and analytical tools. The course is not a follow-on from Math470 with new material as M470 usually has quite comprehensive coverage of the topics listed but is often set at the “general science” level with mathematical explanations given for “why things might work”. M471 will differ significantly not on range, or even particular topics covered, but on the level of mathematical sophistication. We will prove the viability of the cryptographic protocols as much as possible within the level of undergraduate mathematics. For a senior-level mathematics major this will not be either an obstacle or beyond similar 400-level classes. In fact for such students m470 would be merely useful, certainly not a requirement. This class is an excellent opportunity for the mathematics student to see both really clever ideas and real world applications of their subject. Students who do not have this mathematical level, in particular with prior proof-based courses, will be at a severe disadvantage as the exams, assignments and homework will require such mathematical ability.

- **Public Key cryptography.** This will include the systems: RSA, ElGamal, knapsack and lattice methods, elliptic curve methods.
- **Security Protocols.** Digital Signatures; Identification and Secret sharing schemes; zero-knowledge proofs.
- **Information theory and error-correcting codes.**
  Entropy and perfect secrecy; general bounds on error-correcting codes; Hamming and Golay codes; The McEliece public key system.
- **Number theory tools:**
  - The Euclidean algorithm and its convergence rate.
  - Prime numbers: Euler’s representation, the Riemann-zeta function, the Prime Number Theorem and Chebyshev’s approximation.
  - Discrete Logarithms: the Pohlig-Hellman and Index Calculus algorithms.
  - Finite fields, quadratic residues and quadratic reciprocity.
  - Polynomial Congruences and their solution: the Tonelli-Shanks and Hensel lifting theorems.
  - Primality and Factorization: deterministic vs probabilistic tests; Fermat’s and Euler’s theorems; the primality tests of Solovey-Strassen, Miller-Rabin, Pocklington-Lehmer and AKS.
  - Factoring: the Quadratic Sieve and Elliptic Curve methods.
  - The Generalised Riemann Hypothesis and some of its consequences for determinism in cryptographic protocols.

**Syllabus content:** (in approximate order of appearance in the course)
- Primes: Asymptotic values and distribution; primality tests.
- Factoring: methods and their computational complexity; public key systems and identity systems based on this idea.
- Discrete logarithms: their computation; public key and identity systems based on this technique.
- Introduction to error-correcting codes and the utility for cryptographic protocols.
- Introduction to elliptic curves; their use in cryptographic protocols.
Grading

As this course contains more challenging material and thought-provoking problems the grading scale based on total percentage will be as follows:

\[ \geq 75 = A, \quad 60 - 74 = B, \quad 50 - 59 = C, \quad 46 - 49 = D, \quad \leq 45 = F. \]

There will be two in-class exams and a final exam at the appointed time for the course with a points scale in the ration \((1 : 1 : 1.5)\). There will also be homework and possibly student projects. The class size will determine the existence of the latter and also the weighting of the exams and the homework/projects. This course has been only offered every two years and enrollment has varied between 15 and almost 50. At the lower end of the range assignments and projects can be a significant part of the class but at the upper end of the enrollment limit there will be no practical opportunity for these and exams will represent almost all of the graded material.

Times and locations

- Class time: 1:30 – 2:45pm, HECC 110
- Office: Bloc 614C

Suggested Text