MAT302H5S, LEC0101 – Introduction to Algebraic Cryptography

The course will take students on a journey through the methods of algebra and number theory in cryptography, from Euclid to Zero Knowledge Proofs. Topics include: block ciphers and the Advanced Encryption Standard (AES); algebraic and number-theoretic techniques and algorithms in cryptography, including methods for primality testing and factoring large numbers; encryption and digital signature systems based on RSA, factoring, elliptic curves and integer lattices; and zero-knowledge proofs.

45
1
45 hrs per tutorial & per semester
Jan – Apr 2020
Mon 10:00 - 11:00
Wed 10:00 – 12:00

Ph.D. in Mathematics or a related field, completed or nearly complete.
Advanced comprehension of the subject matter as evidenced by research activity and/or advanced teaching experience.
Strong organizational, interpersonal, and communication skills.
Demonstrated evidence of excellence in teaching preferred.
Preference will be given to candidates with demonstrable currency and mastery.

Application Process: If interested, please reply to: jobs mcs utm@utoronto.ca with the following information, in text, PostScript, or Portable Document Format:
- your current CV; and
- letter(s) of recommendation addressing your ability to teach

NOTES:
1. Department Standards and Policies are available in the Department office and in the CUPE Local 3902 office.
2. The positions posted above are tentative, pending final course determinations and enrolments.
3. Undergraduate or graduate students and postdoctoral fellows of the University of Toronto are covered by the CUPE 3902 Unit I collective agreement rather than the Unit 3 collective agreement, and should not apply for positions posted under the Unit 3 collective agreement.
4. Rate of pay for Sessional Lecturer I is $8,323.20 for half a course, and $16,646.40 for a full course (inclusive of vacation pay).

Preference in hiring is given to qualified individuals advanced to the rank of Sessional Lecturer II or Sessional Lecturer III in accordance with Article 14:12.
These jobs are posted in accordance with the CUPE 3902 Unit 3 Collective Agreement.