UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

PMAT 503.01 Elliptic Curves and Cryptography

Calendar Description: An introduction to elliptic curves over the rationals and finite fields. The focus is on both theoretical and computational aspects; subjects covered will include the study of endomorphism rings, Weil pairing, torsion points, group structure, and effective implementation of point addition. Applications to cryptography will be discussed, including elliptic curve-based Diffie-Helman key exchange, El Gamal encryption, and digital signatures, as well as the associated computational problems on which their security is based.

Prerequisites: PMAT 315 Abstract Algebra (or consent of instructor)

Recommended Preparation: PMAT 418 Introduction to Cryptography

Assessment:
40% assignments
60% research project (proposal, written report, presentation)

Notes: This course will share lectures with PMAT 629. Students will be assessed in a similar way, but with reduced expectations as compared to the graduate students. In particular, students will complete roughly 75% of the assignment questions, and the research projects will be less ambitious, with topics assigned by the instructor.

(see Course Descriptions under the year applicable: http://www.ucalgary.ca/pubs/calendar/)

Syllabus

Topics	**Number of hours**
Finite Fields: overview, extension fields, construction	3
Introduction to Elliptic Curves: Weierstrass equation, group law, projective space and points at infinity, elliptic curves in different characteristics, other models	7
Elliptic curve cryptography: elliptic curve based Diffie-Hellman, ElGamal, and digital signature algorithm	3
More on elliptic curves: endomorphism ring, singular curves, supersingular curves	4
Torsion groups:	3

torsion points, Weil pairing, group structure

Elliptic curves over finite fields: 6
Frobenius endomorphism, subfield curves, reduction, order, Hasse-Weil bound

Security of elliptic curve cryptosystems: 3
discrete logarithm problem, Weil descent, Weil and Tate pairing, other weak curves

Efficient implementation: 3
field representations, bases, group law, exponentiation

TOTAL HOURS **32**

* * * * * * *

Date: Dec. 6, 2013
Creator: M. Jacobson