UNIVERSITY OF CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

Pure Mathematics 629 Elliptic Curves and Cryptography

(see Course Descriptions: www.ucalgary.ca/pubs/calendar/current/course-desc-main.html)

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 curve in different characteristics, other models	7
Elliptic curve cryptography: elliptic curve-based Diffie-Hellman, El Gamal, and Digitial Signature Algorithm	3
More on elliptic curves: endomorphism ring, singular curves, supersingular curves	4
Torsion groups: torsions points, Weil pairing, group structure	3
Elliptic curves over finite fields: Frobenius endomorphism, subfields curves, reduction, order, Hasse-Weil bound	6
Security of elliptic curves: Discrete log problem, Weil descent, Weil & Tate pairing, other weak curves	3
Efficient Implementation: Field representations, bases, group law, exponentiation	3
Optional topics	4
Total hours	**36**

****

2005:08:01
MJJ/RS