UNIVERSITY OF
CALGARY

FACULTY OF SCIENCE
Department of Mathematics and Statistics

PURE MATHEMATICS 629
"ELLIPTIC CURVES AND CRYPTOGRAPHY"

Calendar Description: H(3-0)

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 efficient implementation of point addition. Applications to cryptography will be discussed, including elliptic curve-based Diffie-Hellman key exchange, El Gamal encryption, and digital signatures, as well as the associated computational problems on which their security is based..

Prerequisite: Pure Mathematics 315 or consent of the Division.

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