(—–; 3-0-0) **Number Theory and Cryptography** MATH-418*

This course is offered every second year and was last offered in Winter 2004.

Textbook: *A Course in Number Theory and Cryptography*
by N. Koblitz (Springer-Verlag)

Prerequisite: MATH-212* *or* MATH-217*.

Instructor: E. Kani

Evaluation: Based on 5 Problem Sets and 1 Take-Home Examination.
The maximum of formula A and B:
A: 65% Problems + 35% Examination
B: 40% Problems + 60% Examination

Outline:

1. *Time Estimates for Doing Arithmetic*: Multiplication, division, Euclidean algorithm, modular arithmetic.
2. *Algebra*: Basic facts about cyclic groups, finite fields. Quadratic reciprocity.
3. *Cryptography*: Classical cryptosystems, public key cryptosystems (RSA), discrete log cryptosystems. Algorithms to compute discrete log. Zero-knowledge proofs.
4. *Elliptic Curves and Cryptography*: Basic facts of elliptic curves, elliptic curve cryptosystems, EC primality tests, factorization methods.