

**Course Designator/ Course Number:** CprE 533, Math 533

**Course Title:** Cryptography

**Course Length:** 45 hours in 15 weeks, 3 50-minute meetings per week

**Course Description:**

This course will cover the basic concepts of secure communication. Secret-key and public-key cryptosystems. Zero-knowledge proofs, key distribution, hash (a.k.a. message digest) algorithms. The relevant number-theory will be covered in class.

**ISU Catalog Description:**

Math 533. Cryptography (same as CprE 533) (3-0) Cr. 3. S. prereq: Math 301 or CprE 310 or Com S 330. Basic concepts of secure communication, DES and IDEA, public-key cryptosystems, elliptic curves, hash algorithms, digital signatures, social and political implications.

**Course Learning Objectives:**

Upon completion of this course, a student will understand the mathematical foundations of common cryptosystems: why they work, how the security of the system is tied to the underlying structure, and how different systems are related. The student will be able to evaluate a cryptosystem from the standpoints of security and practicality. A student will understand how the component parts of a cryptosystem work together to create a secure environment.

**Major Topics:**

1. Overview
2. Symmetric Key Cryptosystems
  - a) DES
  - b) IDEA
  - c) Skipjack
3. Differential and Linear Cryptanalysis
4. Public Key Cryptosystems
  - a) Relevant Number Theory
  - b) RSA
  - c) El Gamal
  - d) Signature Schemes
5. One-way Hash Functions
6. Key Exchange Algorithms
7. Stream Ciphers and Random Number Generation

- a) Linear Feedback Shift Registers and Variations
  - b) Blum-Blum-Shub Generator
8. Field Theory and Elliptic Curves
- a) Fields and polynomials
  - b) Elliptic Curve Cryptosystems
  - c) More about Linear Feedback Shift Registers
9. Social Implications

**Method of Instruction:**

The course is taught in a traditional lecture format. The lectures are also video taped and shipped out to the off campus students. Bi-weekly homework assignments are used to give students practice in the kind of analysis demonstrated in class, and to pursue subtle questions not addressed in the lectures.

**Evaluation Methods:**

Homework	approximately bi-weekly	75%
Final exam		25%

**Student Enrollment:**

On campus:	40 per year
Off campus:	12 per year

Last Modified: 05/03/2000