

## **Cryptography**

**Mike Jacobson, University of Calgary**

**Overview:** Cryptography, the study of the means by which information can be transmitted and stored in a secure fashion, is of central concern to modern day information management. Once the restricted interest of the military and foreign affairs specialist, an understanding of the central themes and algorithms of cryptography is now of importance to citizen, consumer, business and government. This course is designed to give the student a broad understanding of the subject and an appreciation of the mathematical background essential to its understanding.

**Prerequisites:** This is an introductory course. No prior knowledge about cryptography is assumed; the only prerequisite is an undergraduate course in discrete mathematics and proof techniques. Basic knowledge in abstract algebra, number theory, and/or probability theory are an asset, but by no means required.

**Outline:** Topics will include

- substitution ciphers, information theory, perfect security, and the one-time pad;
- block ciphers, modes of operation, and the Advanced Encryption Standard;
- public-key cryptography (the RSA system, Diffie-Hellman key exchange, provably secure public-key cryptography);
- data integrity and authentication (hash functions and digital signatures).
- Other topics such as key management and examples of real-world cryptographic applications will be included if time permits.

Required mathematical concepts, including a variety of number-theoretic results and algorithms, will be introduced as required.

**Textbook and Evaluation:** There will be no official textbook; I will instead give out a list of sources and make use of handouts and web sites. Evaluation will be based on assignments and a research project.