Cryptography – Winter 2007

AMAT/PMAT 4282

A course in Cryptography is scheduled to be offered as a special topics course in the Department of Mathematics and Statistics during the Winter 2007 semester. Interested students may find the following information helpful in deciding whether to take the course, as well as ensuring that they will have completed the necessary pre-requisites (particularly PMAT 3370 (Introductory Number Theory), which will be offered in the Fall 2006 term ... it should be noted that CS 2740 is acceptable as a pre-requisite for PMAT 3370).

For more information about the course, etc, contact Dr. David Pike (*dapike@math.mun.ca*).

Short Description

Summary of Topics. Topics include private-key cryptosystems (such as classical ciphers, the Hill cipher, and DES), computational complexity and relevant number theoretic problems (such as primality testing, factoring, and the discrete logarithm problem), public-key cryptosystems (such as RSA, Rabin, and ElGamal), digital signatures, and authentication protocols.

Format: Three hours of lecture per week.

Pre-requisites: PMAT 3370 (Introductory Number Theory) and a computing course (such as AMAT 2120 or CS 2710 or CS 2602).

Suggested Text: "Cryptography – Theory and Practice" by Douglas R. Stinson.

Course Outline

The following is a rough sketch of the topics that are likely to be included in the course. Note that emphasis will be placed upon the mathematics that is involved in the encryption and decryption protocols of ciphers, as well as in their security (or lack thereof). In that sense, the focus is on 'why' things work, not just 'how' they work.

1. Introduction to Data Security

   Included in this topic will be the question of how secure a cryptosystem is. For instance, what types of attack might it be susceptible to, such types including known plaintext attacks, chosen plaintext attacks, and known ciphertext attack. Also there's the distinction between absolute security and computational security.

2. Classical Ciphers

   (a) shift cipher
   (b) substitution cipher
   (c) Vigenère cipher
   (d) Hill cipher

In addition to studying the encryption/decryption protocols of each cipher, we will analyse the security of each cipher and show how each is insecure.

3. Feistel Ciphers

   The first example we consider is the New Data Seal, covering it's design as well as how it can be broken. Attention then shifts to the Data Encryption Standard (DES) which is a commercially-used cryptosystem.

4. Some comments on Private-Key Cryptosystems

   Up to this point all ciphers mentioned have been private-key systems. The nature of private-key cryptosystems is such that there are issues of key management and distribution. There are also the issues of how to achieve authentication (which introduces the concept of a digital signature), as well as how to agree upon a key in the first place (this would be a good spot to discuss the Diffie-Hellman key exchange protocol, but doing so first requires a discussion of the discrete logarithm problem).

5. Public-Key Cryptography

   The first cipher to be discussed is RSA. To fully appreciate and understand the mechanics and theoretical reliability of the RSA cryptosystem requires that we also study the topics of primality testing and factoring, which is where we get into some advanced number theory (particularly when discussing primality testing, where we look at quadratic residues, Legendre symbols, and Jacobi symbols). With respect to factoring, several methods are discussed:

   (a) the naïve method
   (b) Pollard rho
   (c) Pollard $p-1$
   (d) Random squares
   (e) Quadratic Sieve

   RSA can be used to implement digital signatures and authentication protocols, which we then discuss.

   The Rabin cryptosystem is introduced as a cipher whose security is provably equal to the difficulty of factoring.

   The ElGamal cryptosystem is an example of a cipher based upon the discrete logarithm problem. Methods for solving the discrete logarithm problem are therefore discussed.

6. Additional Topics

   Time permitting, additional topics may be considered, such as:

   - elliptic curves, the elliptic curve discrete logarithm problem, elliptic curve cryptography
   - the Rijndael Advanced Encryption Standard

Evaluation

Assessment will be based on assignments, midterm test(s), and a comprehensive final exam. A likely grading scheme will be 30% for assignments, 30% for tests, and 40% for the final exam.