Department of Mathematics and Statistics

PMAT 669

Cryptography

Prerequisites: PMAT 329 or permission of instructor

Instructor: H. C. Williams, MS 360, Ph. 220-6322

Textbook: None. Material will come from notes, handouts and published papers. The items mentioned in the attached reading list are also useful sources of information.

Outline: It is important to make this course accessible to as many students as possible. This includes students in computer science and computer engineering. Thus, the course content will to some degree depend on the interests and background of the students enrolled. Nevertheless, broad areas will include:

1. Substitution ciphers and information theory
   - -basic concepts
   - -entropy
   - -cryptanalysis
   - -perfect security
   - -unicity distance

2. Block ciphers and DES
   - -block ciphers
   - -product ciphers
   - -Data Encryption Standard (DES)
   - -cryptanalysis of DES
   - -modes of operation
   - -triple DES

3. The Advanced Encryption Standard
   - -modular arithmetic
   - -group theory
   - -field theory
   - -the Advanced Encryption Standard (AES)
   - -other block ciphers

4. Number theory and algorithms
   - -linear Diophantine equations
   - -the power algorithm
   - -Euler's φ function
   - -primitive roots

5. Public-key cryptography and RSA
   - -one-way functions
   - -Diffie-Hellman key exchange
   - -one-way trapdoor functions
   - -public-key cryptography
   - -the RSA cryptosystem

6. More public-key cryptosystems
    -quadratic residues
    -the Rabin-Williams PKC
    -the El Gamal PKC

7. Probabilistic public-key cryptography
    -semantic security
    -the Goldwasser-Micali PKC
    -the Blum-Goldwasser PKC

8. Authentication and digital signatures
    -hash functions
    -message authentication codes
    -digital signatures
    -the El Gamal signature scheme
    -the Digital Signature Algorithm (DSA)
    -elliptic curves

9. Key management and authentication
    -basic concepts
    -public-key infrastructure (PKI)

10. Cryptography in practice
    -email security and PGP
    -web security

Evaluation:

Two assignments: 40%

One research project (detailed outline 15%, writeup 30%, presentation 10%, class participation 5%): 60%