THE UNIVERSITY OF SYDNEY
Semester 1, 2004

MATH 3024 Elementary Cryptography and Protocols

Lecturer: Dr. David R. Kohel (kohel@maths.usyd.edu.au)
Office hours: Tuesday 3:00–4:00 PM in Carslaw 638, or by appointment.

Introduction

Cryptography is the branch of mathematics which provides the techniques for enabling confidential information to be transmitted over public networks. This unit is an introduction to cryptography, with an emphasis on the cryptographic primitives that are in most common use today. The first portion of the unit reviews classical cryptosystems, the attacks which render them insecure, and how composition of these elementary cryptosystems can yield a more resistant system. The unit then covers modern symmetric cryptosystems, from the block ciphers such as DES and AES to stream ciphers. Finally asymmetric, or public key, cryptosystems such as RSA and ElGamal are treated. These cryptographic primitives will be used to construct protocols for realising digital signatures, data integrity, identification, authentication and key distribution. An important feature of the course will be weekly exercises in practical cryptography using the computer algebra system `magma`.

Information page

The top–level information page is located at:

`http://www.maths.usyd.edu.au:8000/u/UG/SM/MATH3024/`

Links to tutorial sheets and solutions and lecture materials will be made available through this page.

Lectures

Current lecture venues are Tue 2:00–3:00 PM in 373 Carslaw & Wed 2:00–3:00 PM in 173 Carslaw.

Tutorials

Tutorials start in week 2 at Wednesday 3:00–4:00 PM and 4:00–5:00 PM in 705/6 Carslaw. Participation is required and accounts for 10% of the total marks for the unit. The tutorials meet in the computer labs and will emphasise exercises using the computer algebra system `magma`.

Assignments

There will be two assignments during the semester, each worth 10% of the total mark for the course. The assignments emphasise practice of cryptography and cryptanalysis using `magma`.

Assessment

Final marks for the unit will be calculated as follows:

10%: Tutorial participation.
20%: Assignment marks.
70%: Final exam at the end of semester.

Unit of Study Reader

There will be a reader which will be made available from Kopy Stop on Mountain street, mainly comprised of selections from the reference materials below. Additional materials such as lecture outlines, tutorial exercises, and tutorial solutions will be available from the unit of study information page.

Reference Materials

There is no official textbook. Copies of the following reference materials will be on closed reserve at Fisher library.

Denning, Dorothy. *Cryptography and data security*, Reading, Massachussets: Addison-Wesley, 1982.
Konheim, Alan G. *Cryptography, a primer*, New York: Wiley, 1981.
Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A. *Handbook of applied cryptography*, Boca Raton: CRC Press, 1997.
Schneier, Bruce. *Applied Cryptography : Protocols, Algorithms, and Source Code in C*, 2nd ed., John Wiley & Sons, 1995.
Sinkov, Abraham. *Elementary cryptanalysis : a mathematical approach*, Washington : Mathematical Association of America, 1966.
Stinson, Douglas. *Cryptography: theory and practice*, CRC Press, 1995.

Additional Reading

Those interested in pursuing additional reading on the subject of cryptography may find the following books of interest.

Kahn, David. *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1996.
Singh, Simon. *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, 2000.

Unit of Study Outline

Classical Cryptography, Cryptanalysis, and Foundations

1. Cryptographic concepts and terminology.
2. Substitution and transposition ciphers.
3. Enigma and rotor machines.
4. Elementary cryptanalysis of classical cryptosystems.
5. Information theory foundations: entropy, one-time pad.

Modern Cryptographic Algorithms and Constructions

1. Block ciphers: Feistel networks, DES, AES, modes of operation for block ciphers.
2. Stream ciphers: linear feedback register sequences, linear complexity, shrinking generator cryptosystem.
3. Public key cryptography and elementary number theory: modular arithmetic, discrete logarithms, RSA, ElGamal.
4. One-way ciphers: hash functions, message authentication, hashing based on block ciphers.

Cryptographic Protocols and Practice

1. Threshold secret sharing schemes.
2. Digital signatures and message authentication.
3. Blind signatures and digital money.
4. Relative strengths of modern cryptosystems.