The University of Sydney
ICE-EM/AMSI Summer School

Summer **Cryptography** 2007

Lecturer: Dr. David R. Kohel (kohel@maths.usyd.edu.au)
Consultation hours are Thu 14:00–15:00 PM in 625 Carslaw.

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 SAGE.

Lectures are Tue 11:00–13:00, Wed 9:00–11:00, Thur 11:00–13:00 in 275 Carslaw.

Tutorials are Fri 15:00-16:00 in 729 Carslaw, and will emphasize practical exercises using the computer algebra system SAGE. In the second week, the tutorial will meet Thu 8:00-9:00!

Assessment: Marks for this course will be calculated as follows:

20%: Two assignments each worth 10%
80%: Exam

The exam will be at 14:00-16:00 on Friday 9 February.

Web page: The web page is located at:

`http://echidna.maths.usyd.edu.au/~kohel/tch/Crypto`

Lecture materials and information will be made available through this page.

Reference Materials

The course text and exercises will appear on the course web page; additional reference material will be on reserve in the mathematics library.

1. Buchmann, Johannes. *Introduction to Cryptography*, 2nd ed., Springer, 2004

2. Denning, Dorothy. *Cryptography and data security*, Addison-Wesley, 1982.

3. Konheim, Alan G. *Cryptography, a primer*, Wiley, 1981.

4. Menezes, Alfred J.; Van Oorschot, Paul C.; Vanstone, Scott A. *Handbook of applied cryptography*, CRC Press, 1997.

5. Ferguson, Niels and Schneier, Bruce. *Practical Cryptography*, Wiley, 2003.

6. Sinkov, Abraham. *Elementary cryptanalysis : a mathematical approach*, Mathematical Association of America, 1966.

Additional Reading

7. Kahn, David. *The Codebreakers; The Comprehensive History of Secret Communication from Ancient Times to the Internet*, Scribner, 1996.

8. Singh, Simon. *The Code Book : The Science of Secrecy from Ancient Egypt to Quantum Cryptography*, Anchor Books, 2000.