

INTS 465.3 (01): Cryptography, T1, 2009-10

COURSE OUTLINE

This course will consist of an introduction to the mathematical foundations of cryptography. We will study results from number theory and algebra and how they are used for the safe transmission of information. We will discuss various security protocols, the mathematical principles needed for them, and the mathematical principles used in possible attacks.

Brief outline of the topics covered:

Mathematical Background – Symmetric Cryptosystems – Asymmetric Cryptosystems – Primality Testing – Factoring Integers – RSA – Discrete Logarithm Cryptographic Schemes – Diffie-Hellman – ElGamal – Public Key Management – Security Questions and Attacks.

The students are expected to hand in assignments (about one every other week). There will also be a midterm exam.

The **final mark** will be calculated as follows:

Assignments: 25 %

Midterm Exam: 25 %

Final Exam: 50 %.

Lectures: TTh 8:30 am – 9:50 am, Physics 130

Tutorial: M 4:30 pm – 5:50 pm, Arts 217

Course Web Site: on PAWS. Home work, practise exams and other information and links will be posted there.

Email: fvk@math.usask.ca

Office hours: F 2–3 and by appointment.

Literature (more references will be given during the course):

Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996. ISBN: 0-8493-8523-7

J. A. Buchmann: *Introduction to Cryptography. Undergraduate Texts in Mathematics*, 2nd edition (paperback), Springer, 2004. ISBN: 0-387-20756-2

C. Vanden Eynden: *Elementary Number Theory*, McGraw-Hill, 2001. ISBN 0-07-232571-2

Neal Koblitz: *A course in number theory and cryptography*, Springer GTM **114**, 1994. ISBN 0387942939