

## Math 465.3 (02): Cryptography, T2, 2011-12

**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.

**Prerequisites:** Math 364 (which is offered in term 1), or special permission by the instructor. Some basic knowledge of number theory (in particular, modular arithmetic) is required, but the basics can be acquired quickly before or at the beginning of the course through independent reading (e.g., from the book of Vanden Eynden cited below). For a possible prerequisite waiver, please talk to me in early September.

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: 20 %  
Midterm Exam: 30 %  
Final Exam: 50 %.

**Lectures:** TTh 8:30 am – 9:50 am, location t.b.a.

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

**Email:** fvk@math.usask.ca

**Office hours:** t.b.a.

**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