

Math 342 - Term 2, Spring 2013

Algebra and Coding Theory

Time and Place: TuTh 9:30-11, LSK 460.

Instructor: Kalle Karu.

Office: 213 Math Bldg.

Phone: 822-4787.

E-mail: karu@math.ubc.ca.

Office hours: Mon 2-3, Th 11-12.

Textbook: *A First Course in Coding Theory* by R. Hill.

Web site: www.math.ubc.ca/~karu/m342 Homeworks and solutions will be posted here.

Course description. This course has two main topics – coding theory and cryptography. For coding theory we cover Chapters 1-8 and 12 in the textbook. For cryptography we will use the original article “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems” by R.L. Rivest, A. Shamir, and L. Adleman. Both parts of the course emphasize connections with algebra, in particular, linear algebra, elementary number theory and combinatorics.

Homework. We will have a homework every week. Homeworks are posted on the course web site on Thursdays and they are due the following Thursday in class. Late homework will be accepted only in exceptional circumstances.

Exams. We will have two midterm exams, on Tuesdays Feb. 5 and Mar. 19, during regular class hours. The final will be a $2\frac{1}{2}$ -hour exam scheduled by the university. No makeup exams will be given.

Final Grade. Your final grade will be based on your performance on homework (15%), midterms (35%) and final exam (50%).