Instructions for the WIM paper

The WIM paper is one of the central requirements for the course. It should be of length 5-10 pages, and should be typeset in Latex. The paper should concern a topic in cryptography or coding theory. It should definitely include some mathematical content beyond that given in the course.

Here are some suggestions for topics.

1. Primality testing

2. Factoring

3. Elliptic curves

4. Quadratic reciprocity

5. Structure theorem of finite Abelian groups

6. Structure theorem for finitely generated modules over a principal ideal domain

7. Structure of finite fields

8. Discussion of a family of error correcting codes

Of course, you can select another topic, provided it is in the general area of cryptography and coding theory.

To begin, decide on a topic, and develop an outline for the paper, including all the topics that you will cover. Send this outline to

M1102016carl@gmail.com

on Monday, November 14. I will then send you feedback within the next couple of days, concerning any suggested modifications. The paper will be due on December 12.