About Exam II

The second exam will cover everything we did after the first exam (including RSA cryptosystem and one-way functions).

You will need to use Magma (or Maple) for some of the problems. You can have a 3 by 5 index card with Magma commands on it during the exam. The sheet cannot contain anything else. Pay special attention to the following topics:

- Bounds on the Parameters Codes (sphere packing, singleton, G-V)
- Perfect codes, MDS codes.
- Hamming codes: Construction, parameters
- Extended codes, Self dual codes
- Cyclic codes: Structure and properties. Generator polynomials, generator and parity check matrices, dual of a cyclic code finding cyclotomic cosets mod n.
- Finding all possible cyclic codes of a given length
- Properties of the polynomial ring $K[x]$ and computations in it such as division algorithm, computing gcd's, factorizing $x^n + 1$. Should know how to do these operations in Magma.
- Symmetric key cryptosystems, one-time pad
- Elementary number theory: Divisibility, gcd, lcm, modular arithmetic, Fermat's little thm, Euler's generalization, Chinese Remainder Theorem, order of an element in $\mathbb{Z}_n^*$, cyclic groups etc.
- Go over examples and exercises in Number Theory and hmw problems in general.
- Public-key cryptosystems. One-way functions.
- RSA cryptosystem and its implementation.
- Computational Complexity, Big-O notation.
- There will be some proofs and a number of True/False questions.