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 some other CAS) for some of the problems. You can have a sheet with Magma commands on it (one side only) 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 all possible cyclic codes of a given length
- Properties of the polynomial ring $K[x]$ e.g. division algorithm. Doing basic operations in $K[x]$ with Magma
- Symmetric key cryptosystems, one-time pad
- Elementary number theory (section 11.1): Divisibility, gcd, lcm, modular arithmetic, Fermat's little thm, Euler's generalization, order of an element etc.
- Go over exercises in 11.1. Go over hmw problems in general.
- Public-key cryptosystems. One-way functions.
- RSA cryptosystem
- Computational Complexity, Big-O notation.
- There will be some proofs and a number of True/False questions.