Fordybelsesprojekt i Algebra 2010-AAU
Miniproject in Algebra 2010-Aalborg University

Welcome to the mini project in Algebra. We will use the project description by Christian Thommesen in 2009.

Bibliography:

- [Lau] Niels Lauritzen, "Concrete abstract algebra", Cambridge University Press, 2003. ISBN: 978-0-521-53410-9.
- [Tho] Slides by Christian Thommesen (2009): http://people.math.aau.dk/~cthom/kurser/algebra-09/trmin09.pdf and http://people.math.aau.dk/~cthom/kurser/algebra-09/Tr22a.pdf
- Some slides that will appear at the course web page (Algebra 2010), stay updated!

Project topic: Public-key cryptography. We will consider three cryptosystems:

- Knapsack (Merkle-Hellman)
- ElGamal
- RSA

Contents: The first aim of the project is to describe the three cryptosystems above. In particular, for each crytopsystem, the project should contain an example and a brief answer to the following questions:

- How are the public and private keys generated?
- How does the sender encrypt a message?
- How does the receiver decrypt a message?
- How can the receiver be sure that he/she will recover the original message?
- Why cannot an encrypted message be decrypted without the private key?

To answer the previous questions we will use the mathematical theorems and methods studied in the subject Algebra (chapters 1 and 2 in [Lau]). The second aim of the project is to put all this into practice in a series of exercises from [Tho], the exercises in the Problemkatalog (12 problems + Pollard's algorithms).

Schedule: We are meeting from Monday 25/10 to Friday 29/10 at 8:15 in G5-112, where there will be a short lecture. Afterwards you will be working in groups and I will be around to help you. We can also have a lecture at any moment if you need it. The lecture on Monday will be longer, so I have time to introduce the cryptosystems and explain what is expected from you. There will also be time for you to ask any questions you may have.

Evaluation: Each group has to deliver a project by the end of this week, the project can be written in Danish or in English. Two copies of each project are to be handed on Friday 29/10 at 12:00, one to Lisbeth Grubbe Nielsen and one to me. We need to find a date for the exam, which will be oral, where the project contents will be discussed. The grading is: Bestået/Ikke bestået.

Best regards,

Diego Ruano