Algebra 1 (2012)-Aalborg University
Lecture 12, October 16th

12th Lecture: Tuesday October 16th. I will not be present during this lecture.

- Self-study of the cryptosystem Knapsack (Merkle-Hellman), see Knapsack in Wikipedia, based in the Knapsack problem. I have prepared some slides as well (see the web page). Knapsack is very fast and elegant, but it was broken in 1982. However, there are several improvements that have been (partly) broken as well (in the 80's and 90's). It is not considered secured nowadays but it would be very nice to get an improvement.

- Work in groups: Exercises A, B, C.

  - Exercise A: Answer briefly to the following questions about Knapsack:
    1. How are the public and private keys generated?
    2. How does the sender encrypt a message?
    3. How does the receiver decrypt a message?
    4. How can the receiver be sure that he/she will recover the original message?
    5. Why cannot an encrypted message be decrypted without the private key?
  - Exercise B: Consider the example in the slides. Encrypt $(0, 0, 0, 0, 1)$ and decrypt the encrypted message. Encrypt $(0, 1, 0, 0, 0)$ and decrypt the encrypted message.
  - Exercise C: Consider your own cryptosystem of Knapsack with 6 bits ($n = 6$), i.e. consider an easy knapsack problem, N and w. What are the private and public keys?. Encrypt a message and then decrypt it. You are welcome to use Maple (you can find some help for Maple in the last slide).

  Each group can write their solution for two exercises and leave it in my mailbox (just one set of exercises per group). You are welcome to orientate me, by e-mail, about the successes and difficulties during the lecture.

Best regards,

Diego