Algebra 1 (2012)-Aalborg University
Lecture 6, September 25th

6th Lecture: Tuesday September 25th.
I will not be present during this lecture.

- Work in groups. Exercises A, B.

  Exercise A: Answer briefly to the following questions about RSA:
  - 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?

  Exercise B: Compute in Maple an example of RSA:

  - Determine N, p and q at your choice.
  - Choose the encryption exponent e and compute the decryption exponent d. (Hint: exercise 1.13).
  - Determine a message X and encrypt it using e.
  - Decrypt the encrypted message using d.

  You can find some help for Maple in the slides for lecture 6 and in Mapleprimes.

  Each group can write their solution for exercises A and B and leave it in my mailbox (just one set of exercises per group). You can print exercise B and/or email me your Maple Worksheet.

- Lecture: This part will consist of self-study in the group rooms. The topic is "RSA explained" (section 1.9, pages 24–29). Your are welcome to orientate the teacher, by e-mail, about the successes and difficulties during the lecture.

Best regards,

Diego