Spiseseddel 5
Algebra 1, EVU 2011-Aalborg Universitet

9th lecture: Thursday 5th May, 9:00-12:00 at room G5-110.

- *Applications to cryptography: RSA and ElGamal* (section 1.5 in [KN] and Wikipedia)
- Bring a laptop with Maple (or any computer algebra system) to the lecture (it it is possible).
- Exercises:
  - Ex A: Consider the group $(\mathbb{Z}/34\mathbb{Z})^*$. Check that $[13] \in (\mathbb{Z}/34\mathbb{Z})^*$. Compute $[13]^{-1}$.
  - Ex B: Compute the Cayley table of $(\mathbb{Z}/8\mathbb{Z})^*$. Compare it with the one of $(\mathbb{Z}/4\mathbb{Z}, +)$
  - Ex C: Consider an example of RSA in Maple.
  - Ex D: Consider an example of ElGamal in Maple.

10th lecture: Friday 8th April, 18:00-21:00 at room G5-110.

- *Applications to coding theory* (section 2.11 in [KN]).
- Bring a laptop with Maple (or any computer algebra system) to the lecture (it it is possible).
- Exercises: TBA

I will post during the weekend in the web page the exercises that you can hand in.

Med venlig hilsen,

Diego