Security

Assignment 9, Friday, November 18, 2016

Handing in your answers: For the full story, see

`http://www.sos.cs.ru.nl/applications/courses/security2016/exercises.html`

To summarize:

- Include your name and student number **in** the document (they will be printed!), as well as the name of your teaching assistant (Hans or Joost). When working together, include **both** your names and student numbers.
- Submit one single **pdf** file – when working together, only hand in **once**.
- Hand in via Blackboard, before the deadline.

Deadline: Monday, November 28, 09:00 sharp!

Goals: After completing these exercises successfully you should

- be familiar with the Euclidian and Extended Euclidian algorithm;
- know the relation between inverting and computing EGCD;
- be able to work with groups and subgroups and their properties.

Marks: You can score a total of 100 points.

1. **(35 points)** Last week, we computed the GCD for small numbers by factoring. Now, we have a much stronger method at our disposal: the Euclidian algorithm.

   (a) Use the Euclidian algorithm to find $\gcd(2145, 903)$. Show intermediate steps.

   (b) Are 2145 and 903 relative prime? Why (not)?

   (c) Use the Euclidian algorithm to compute the GCD of 1269 and 137.

   (d) Are 1269 and 137 relative prime? Why (not)?

   (e) Find n and m using the Extended Euclidian algorithm such that:

   $$n \cdot 1269 + m \cdot 137 = \gcd(137, 1269)$$

   (f) Using the equation from (e), what is the multiplicative inverse of 137 mod 1269?

2. **(25 points)** Recall the definition from the lecture; a tuple $(A, \star)$ is a group if its $\star$ operation has the following properties (recall that $\forall$ is 'for all', $\exists$ is 'there exists'):

closedness:	$\forall a, b \in A:$	$a \star b \in A$
associative:	$\forall a, b, c \in A:$	$(a \star b) \star c = a \star (b \star c)$
neutral element:	$\exists e \in A, \forall a \in A:$	$a \star e = e \star a = a$
inverse element:	$\forall a \in A, \exists a' \in A:$	$a \star a' = a' \star a = e$

   For each of the following tuples, say if they form a group. If they are a group, describe the neutral element and how inverting works. If not, state which properties are missing.

   NOTE: this exercise has been revised to use $\mathbb{Z}_{\geq 0}$ (instead of $\mathbb{N}$) to represent all positive integers *including* zero.

   (a) $(\mathbb{Z}_{21}, +)$

   (b) $(\mathbb{Z}_{\geq 0}, -)$

   (c) $(\mathbb{Q}, \times)$

   (d) $(\{-1, 1\}, \times)$

   (e) $(\mathbb{Z}_{\geq 0}, \ominus)$ with $a \ominus b = \begin{cases} 0 & \text{if } a < b \\ a - b & \text{if } a \geq b, \end{cases}$

3. **(40 points)** In this exercise we take a closer look at the structure of $(\mathbb{Z}_{15}^*, \times)$. Recall that $\mathbb{Z}_{15}^*$ is the set of integers that are relative prime to 15. *Note:* for this exercise, feel free to use a calculator, but do write down intermediate steps.

   (a) Which elements does $\mathbb{Z}_{15}^*$ contain?

   (b) What is the order of $\mathbb{Z}_{15}^*$?

   (c) Is $\mathbb{Z}_{15}^*$ a cyclic group?

   In the general case, finding all subgroups of a group is a difficult task. For small groups, however, you can construct them by hand.

   (d) For each element of $\mathbb{Z}_{15}^*$, give its inverse.

   (e) What possible orders can the subgroups of $\mathbb{Z}_{15}^*$ have?

   (f) What subgroups does $\mathbb{Z}_{15}^*$ have? *Hint:* make use of the fact that the neutral element is always in the subgroup, and that the inverse of each element in the subgroup must also be in the subgroup.

   (g) For each subgroup, say if it is cyclic or not.

   (h) For each cyclic subgroup you found in (g), list all its generators.