Security on the Internet, summer 2006

MICHAEL NÜSKEN

3. Exercise sheet

Hand in solutions on Tuesday, 9nd of Mai, at the b-it info desk. Deadline for any completely signed(!) electronic solution is the same Tuesday, 23:59.

Exercise 3.1 (Birthday attack). (4 points)

Compute the probability that among 23 randomly chosen people there are two that have the same birthday up to an error of at most $\pm\frac{1}{2}10^{-5}$. (Assume that there are 366 days in a year.) Provide a formula for it as well. [1] [3]

Exercise 3.2 (Mail from yourself). (8 points)

(i) Examine the mail `[SotI: <your name>] Lonely 2 ...` (ignore the other one) that you got from yourself. Can you tell the difference from a true mail from yourself? Describe what you did in order to find your answer. [2]

(ii) Send an email to me that, apart from the body contents, seems to come from me and not from you. Include a signature in the message body to enable me to award you the points. (Sending a mail to yourself with your favourite mailing connector can give you a signed body, ready for reuse.) [3]

(iii) Would we want to prohibit this? [1]

(iv) Can we prohibit this misuse? [2]

Exercise 3.3 (A commutative Group: don't PANIC). (0+6 points)

An important example of a group is the *multiplicative group* $\mathbb{Z}_m^\times$ *modulo* m for some integer $m \geq 2$. The class elements are represented by integers in the range $0..m-1$ (alternatively, also the range $-\left\lceil\frac{m-1}{2}\right\rceil .. \left\lfloor\frac{m-1}{2}\right\rfloor$ is fine). Only those integers that have no common divisor with m represent legal class elements. The operation $\texttt{mul}(a,b)$ performs the multiplication of the representing integers and reduces the product modulo m (that is, divide the product $\tilde{a}\cdot\tilde{b}$ of the integers $\tilde{a}$ and $\tilde{b}$ representing a and b, respectively, by the modulus m with remainder in $0..m-1$ and return the remainder). For example,

$$4 \cdot 5 = 6 \quad \text{in } \mathbb{Z}_7^\times .$$

Prove that this satisfies all five axioms and thus is a commutative group. [+6]

Reminder: A commutative group in the language of object oriented programming is a class G defining a set of legal elements and one binary operation `mul`. It fixes a set of legal objects, and must satisfy the following axioms:

Proper It must be properly defined, that is, the binary operation must take two class elements and output an element of the class. Sometimes it has to be proved that the output element does not depend on the internal representation of the input elements or things thelike.

Associative The operation must be associative, that is, $\texttt{mul}(a, \texttt{mul}(b, c)) = \texttt{mul}(\texttt{mul}(a, b), c)$ must hold for all class elements a, b, c.

Neutral There must be a neutral element 1, that is, $\texttt{mul}(1, a) = a = \texttt{mul}(a, 1)$ for all class elements a. It may be convenient to have a nullary operation `one` that outputs this element.

Inverses For any class element a there must exist an inverse element a^{-1} in(!) the class: $\texttt{mul}(a, a^{-1}) = 1 = \texttt{mul}(a^{-1}, a)$. One can prove that there is never more than one inverse element, and it may be convenient to have a unary operation `inv` that outputs the inverse element.

Commutative Some groups are even commutative, that is, we have $\texttt{mul}(a, b) = \texttt{mul}(b, a)$ for all class elements a, b.

A possible source of confusion is the name given to the operation: For some groups the operation is called multiplication (as hinted to here by the operation name and used in the example), for others it is called addition. (Mathematician mostly use addition for commutative groups and multiplication for general groups [PANI], but they also decide that upon the origin of the group sometimes.) Though the notation varies the background is the same.