Cryptography
Academic Year 2024-2025
Homework III
December 3th, 2024

Please notice that:

- Exercises are meant to be solved *individually*.
- Solutions should be typeset in LaTeX, and uploaded, in pdf format, to `http://virtuale.unibo.it`. Students are encouraged to use the template `Homework-template-2324.tex`, which can be found retrieved from `http://virtuale.unibo.it` itself.
- The deadline for uploading the solutions is Tuesday, December 10th, at midnight CET.

**Exercise 1.**
Which one of the following numerical sets are *cyclic* groups when endowed with usual addition?

$$\mathbb{Z} \qquad \mathbb{Q} \qquad \mathbb{R}$$

Prove your answer. (Here, $\mathbb{Z}$ is the set of integer number, $\mathbb{Q}$ is the set of rational numbers, and $\mathbb{R}$ is the set of real numbers). Moreover, prove that every cyclic group is abelian. .

**Exercise 2.**
We saw that, in the context of multiset rewriting, there is a way to model the intruder in presence of a primitive for *encryption*. Show how the underlying signature and rules can be adapted so as to reflect the use of a (secure) *message authentication code*.

**Exercise 3.**
Consider the following protocol (we use the same notation we employed in the slides):

$$\begin{aligned}
A \to C: &\quad \{m\}_k \\
B \to C: &\quad \{p\}_h \\
C \to D: &\quad f(m,p) \\
D \to A: &\quad \{d(m)\}_j \\
D \to B: &\quad g(p)
\end{aligned}$$

Here, $m, p$ are messages, $j, k, h$ are private keys, and $\{r\}_k$ denotes the ciphertext obtained by encrypting $r$ with $k$. Moreover, $f, g$ are functions whose result does not reveal any information about any of their argument(s), while $d$ allows anyone seeing a message $d(x)$ to also know $x$. Formalize the protocol above by way of ProVerif, and show that no adversary interacting with the protocol is capable of determining either the value of $m$ or the value of $p$, of course assuming that the employed encryption primitive is secure. To do so, you are free to use any version of ProVerif, and in particular the one available online at `http://proverif20.paris.inria.fr/`.