Cryptography
Academic Year 2025-2026
Homework III
November 27th, 2025

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-2526.tex`, which can be found retrieved from `http://virtuale.unibo.it` itself.
- The deadline for uploading the solutions is Sunday, December 7th, at midnight CET.

Exercise 1.
What happens if the Padded RSA scheme is modified in such a way that the amount of randomness incepted in messages is of size $\Theta(\lg n)$, namely logarithmic in the security parameter? Either show an attack against the scheme, or prove that its security is equivalent to the one of the variation of Padded RSA we claimed secure during the course.

Exercise 2.
Build an MSR theory corresponding to the Handshake Protocol, and show, through it, that the Handshake Protocol is insecure, mimicking the attack we found using ProVerif. In doing so:

- You should explicitly give the multset rewrite sequence, perhaps eliding some of the rewriting steps.
- You somehow have to take care of the fact that at least two sessions of the protocols have to be aunched for the attack to take place.

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

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

Here, m, p are messages, i, j, k, h are private keys, and $\{r\}_k$ denotes the ciphertext obtained by (symmetrically) 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 use it to determine whether any 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/`.