Cryptography
Academic Year 2025-2026
Homework I
October 10th, 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 retrieved from `http://virtuale.unibo.it` itself.
- The deadline for uploading the solutions is Monday, October 17th, at midnight CET.

In all the exercises below, if $y \in \{0,1\}^m$ and $n \leq m$, then $y|_n$ is the binary string obtained by considering the first n bits of y.

Exercise 1.
The *scytale* (see, `https://en.wikipedia.org/wiki/Scytale`) is a classical cipher from ancient Greece. Define it as a triple of algorithms $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ as we did in Section 2, and prove that Π is not perfectly secure.

Exercise 2.
Consider a pseudorandom generator G with expansion factor ℓ, and let ℓ' be any polynomial such that $\ell(n) > \ell'(n) > n$. Consider the function H defined as $H(x) = G(x)|_{\ell'(|x|)}$. Prove that H is still a pseudorandom generator.

Exercise 3.
Consider the following functions, and identify which ones of them are pseudorandom generators, proving your claims:

$$G_1(x) = x \cdot 010 \qquad G_2(x) = F(x, 0^{|x|}) \qquad G_3(x) = \begin{cases} x \cdot x & \text{if } |x| \leq 2 \\ F(x, 1^{|x|}) \cdot F(x, 0^{|x|}) & \text{otherwise} \end{cases}$$

Here, $\cdot$ is string concatenation, and F is a pseudorandom function. Moreover, prove that none of the following binary functions is a pseudorandom function:

$$F_1(k, x) = x \oplus k \qquad F_2(k, m) = G(k)|_{|k|} \oplus m$$

where G is a pseudorandom generator.