Cryptography
Academic Year 2025-2026
Homework II
October 31th, 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 Sunday, November 9th, at midnight CET.

Exercise 1.
As we know well, each round of a block cipher designed as a SPN (Substitution Permutation Network) consists of three phases: the *key mixing* phase, the *substitution* (S-box) phase, and the *permutation* phase. Provide convincing arguments that all three of these phases are *necessary* for the SPN to achieve cryptographic security. More precisely, prove that the three block ciphers one obtains, from the 64-bit SPN we saw as an example, by simply omitting at each round one of the three aforementioned phases (keeping the other two) can be easily distinguished from a random function.

Exercise 2.
Suppose that (Gen, H) is a collision-resistant hash function. Prove that (Gen, K) where $K^s(x) = H^s(H^s(x))$ is also collision-resistant. What happens if, instead, $K^s(x) = H^s(J^s(x))$ where *both* (Gen, H) and (Gen, J) are collision resistant?

Exercise 3.
Give an example of a cyclic and *non*-abelian group of order 7, or show that such a algebraic structure cannot exist.