Cryptography
Academic Year 2024-2025
Homework I
October 8th, 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-2425.tex`, which can be retrieved from `http://virtuale.unibo.it` itself.
- The deadline for uploading the solutions is Monday, October 14th, at midnight CET.

Exercise 1.
Consider the the encription scheme Π^G as we introduced it in the course. In that encryption scheme, $\mathsf{Enc}(k, m)$ is defined as $G(k) \oplus m$, where G is a pseudorandom generator. Prove that any instance of Π^G obtained by fixing the value of the security parameter is *not* perfectly secure. In doing so, which ones of the three requirements about pseudorandom generators (i.e. being polytime, having a nontrivial expansion factor, being indistinguishable from a source of true randomness) are actually necessary?

Exercise 2.
Consider the following functions, and prove that none of them is a pseudorandom generator:

$$G_1(x) = x \cdot (\oplus_{i=1}^{|x|} x_i) \qquad G_2(x) = F(0^{|x|}, x) \qquad G_3(x) = F(x, x) \cdot x$$

where $\cdot$ is string concatenation, $\oplus$ is the exclusive or boolean operator, and F is a pseudorandom function. Similarly, prove that none of the following binary functions is a pseudorandom function:

$$F_1(k, x) = k \oplus x \qquad F_2(k, m) = G(m)|_{|k|} \qquad F_3(k, m) = G(k)|_{|m|}$$

where G is a pseudorandom generator and $s|_n$ denotes the prefix of the binary string s having length equal to $n \in \mathbb{N}$.

Exercise 3.
A length-preserving function H on binary strings is said to be an efficiently computable permutaion if it is bijective and both H and its inverse $H^{-}1$ can be computed in deterministic polynomial time. Given a private-key encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ and two efficiently computable permutations H, J, write $\Pi_{H,J}$ for the encryption scheme $(\mathsf{Gen}, \mathsf{Enc}_{H,J}, \mathsf{Dec}_{H,J})$ such that

$$\mathsf{Enc}_{H,J}(k, m) = J(\mathsf{Enc}(k, H(m))) \qquad \mathsf{Dec}_{H,J}(k, c) = H^{-1}(\mathsf{Dec}(k, J^{-1}(c)))$$

Prove that if Π is correct and secure against passive attacks, then $\Pi_{H,J}$ is also correct and secure against passive attacks. How about CPA-security?