Cryptography
Academic Year 2024-2025
Homework II
November 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, November 18th, at midnight CET.

Exercise 1.
Fix a pseudorandom generetor G with expansion factor ℓ, and consider the two algorithms defined as follows:

- Gen, on input 1^n, outputs a binary string k drawn uniformly at random from $\{0,1\}^n$.
- Mac, on input $k \in \{0,1\}^n$ and $m \in \{0,1\}^{\ell(n)}$, draws at random $r \in \{0,1\}^{\ell(n)}$ and outputs the pair $\langle r, G(k) \oplus m \oplus r \rangle$, where $\oplus$ stands for bitwise XOR.

First of all, give a definition of Vrfy such that the resulting MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ is at least correct. Is there any hope that Π is secure?

Exercise 2.
Let Gen be like in Exercise 1 above, and let F be a pseudorandom function. Consider the three functions H_1, H_2 and H_3 defined as follows (where $x, y \in \{0,1\}^n$ and $x \cdot y$ is the concatenation of x and y):

$$H_1^s(x \cdot y) = x \oplus y \oplus s \qquad H_2^s(x \cdot y) = F_s(x \oplus y) \qquad H_3^s(x \cdot y) = F_s(x) \oplus y$$

Which ones among (Gen, H_1), (Gen, H_2) and (Gen, H_3) are collision-resistant hash functions?

Exercise 3.
The notion of second pre-image resistance which we have informally considered, can be formalized through the following experiment, where $\Pi = (\mathsf{Gen}, H)$ is a hash function for messages of length $\ell(n)$:

$$\begin{aligned}
&\mathsf{HashSec}_{\mathcal{A},\Pi}(1^n): \\
&\quad s \leftarrow \mathsf{Gen}(1^n) \\
&\quad x \leftarrow \{0,1\}^{\ell(n)} \\
&\quad y \leftarrow \mathcal{A}(s, x) \\
&\quad \textbf{return} \ \ (x \neq y) \wedge H^s(x) = H^s(y)
\end{aligned}$$

As expected, such a Π is said to be second pre-image resistant if and only if for every PPT adversary $\mathcal{A}$ there is a negligible function ε such that

$$\Pr\left[\mathsf{HashSec}_{\mathcal{A},\Pi}(1^n) = 1\right] = \varepsilon(n)$$

Prove formally that collision resistance implies second-preimage resistance.