Cryptography, winter term 16/17: Assignment 6

Prof. Markus Bläser, Cornelius Brand, Marc Roth
http://www-cc.cs.uni-saarland.de/course/55/

Due January 4th, 2016

Exercise 6.1 (Be nice to yourselves, Knowledge) Refresh your knowledge about basic group theory by reading Chapter 8.1 in the book.

Exercise 6.2 (Be nice to your tutors and TAs, 1 Bonus Point) Write the name and matriculation number of every author as well as number, time slot and the name of the tutor of your tutorial group on the first page of your solution. Furthermore write in english and staple *all* sheets of your solution.

Exercise 6.3 (Canonical Verification, 5 Points) Let $\Pi = (\text{Gen}, \text{Mac}, \text{Vrfy})$ be a secure MAC that uses *canonical verification*. Prove that Π is a strong MAC.

Exercise 6.4 (MACs, 6 Points) Let F be a PRF. Show that each of the following MACs is insecure, even if used to authenticate fixed-length messages. (In each case Gen outputs a uniform $k \in \{0,1\}^n$ and $[i]_2$ denotes the $\frac{n}{2}$-bit binary encoding of i.)

(a) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^n$, compute

$$t := F_k(m_1) \oplus \cdots \oplus F_k(m_\ell)$$

(b) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, compute

$$t := F_k([1]_2 || m_1) \oplus \cdots \oplus F_k([\ell]_2 || m_\ell)$$

(c) To authenticate a message $m = m_1 \dots m_\ell$, where $m_i \in \{0,1\}^{\frac{n}{2}}$, choose uniform $r \leftarrow \{0,1\}^n$ and compute

$$t := (r, F_k(r) \oplus F_k([1]_2 || m_1) \oplus \cdots \oplus F_k([\ell]_2 || m_\ell))$$

Exercise 6.5 (Hash Functions, 5 Points) Let $\Pi = (\text{Gen}, H)$ be a collision resistant hash function and define the hash function $\hat{\Pi} := (\text{Gen}, \hat{H})$ such that

$$\hat{H}^s(x) := H^s(H^s(x)) \,.$$

Prove or disprove: $\hat{\Pi}$ is a collision resistant hash function.