Introduction to Modern Cryptography
Class Exercises #4

University of Amsterdam, Master of Logic, 2014
Lecturer: Christian Schaffner
TA: Malvin Gattinger

Thursday, 25 September 2014

Class Exercises (to be solved during exercise class)

1. Let G be a polynomial-time algorithm which computes a function $\{0,1\}^n \to \{0,1\}^{\ell(n)}$ for which $\ell(n) > n$. Let $\Pi_s = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ be defined as follows for the security parameter n and messages of length $\ell(n)$:

   $\mathsf{Gen}(1^n)$: $k \leftarrow \{0,1\}^n$.

   $\mathsf{Enc}_k(m)$: Return $c := G(k) \oplus m$.

   $\mathsf{Dec}_k(c)$: Return $m := G(k) \oplus c$.

   Show that G is a PRG if Π_s is eavesdropper secure (according to Definition 3.8 in [KL]).

2. Let $\Pi' = (\mathsf{Gen}', \mathsf{Mac}', \mathsf{Vrfy}')$ be a secure MAC for messages of fixed length n. Consider the following MAC $\Pi = (\mathsf{Gen}, \mathsf{Mac}, \mathsf{Vrfy})$ for messages of fixed length $2n - 2$:

   $\mathsf{Gen}(1^n)$: $k \leftarrow \mathsf{Gen}'(1^n)$.

   $\mathsf{Mac}_k(m)$: Given $m = (m_0, m_1)$ where $m_i \in \{0,1\}^{n-1}$, return

   $$t := (t_0, t_1) := (\mathsf{Mac}'_k(m_0, 0), \mathsf{Mac}'_k(m_1, 1))$$

   (a) Define a correct Vrfy function.

   (b) Show that Π is <u>not</u> secure.