Introduction to Modern Cryptography
Class Exercises #6

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

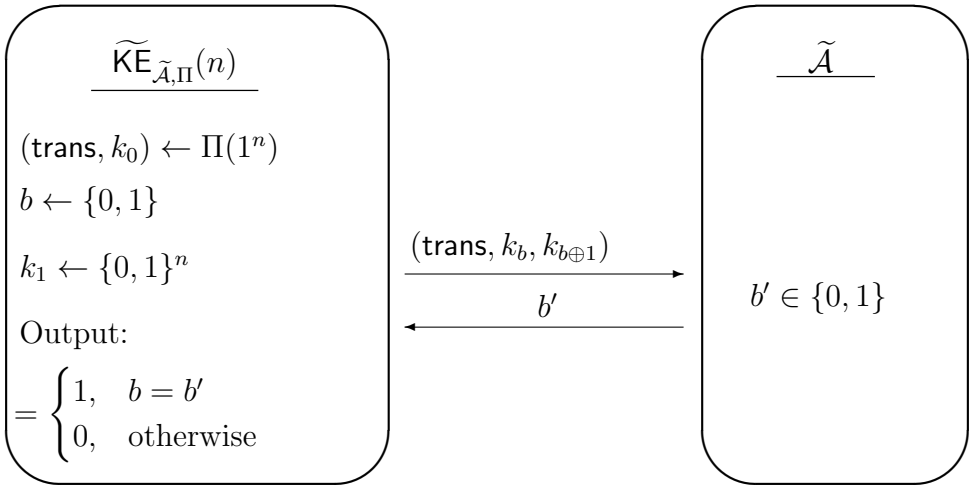
Thursday, 9 October 2014

Class Exercises (to be solved during exercise class)

1. **Definition:** A key exchange protocol Π is called *strongly secure* against passive attacks, if for all PPT adversaries $\widetilde{A}$, we have that

$$\mathsf{Ws}[\widetilde{\mathsf{KE}}_{\widetilde{A},\Pi}(n) = 1] \leq \frac{1}{2} + \mathsf{negl}(n).$$

This definition considers a modification $\widetilde{\mathsf{KE}}$ of the KE-game from the lecture. The adversary $\widetilde{\mathcal{A}}$ gets as challenge $(\mathsf{trans}, k_b, k_{b\oplus 1})$ instead of (trans, k_b), i.e. $\widetilde{\mathcal{A}}$ receives both the correctly generated *and* the randomly generated key as inputs and has to decide in which order he received them.



Show that these two security notions are equivalent:

   (a) Show that every *strongly secure* key exchange protocol is *secure*.

   (b) Show that every *secure* key exchange protocol is *strongly secure*.

2. **Calculations:**

   (a) Compute (by hand) the final two (decimal) digits of 3^{1000} (Exercise 7.5 in [KL]).
   Hint: The answer is $[3^{1000} \mod 100]$.

   (b) Compute $[101^{4'800'000'023} \mod 35]$ by hand (Exercise 7.6 in [KL]).

(c) Find a $x \in \mathbb{Z}_{9999}$ that fulfills the following system of congruences:

$$\begin{aligned} 13x &\equiv 4 \mod 99 \\ 15x &\equiv 56 \mod 101\,. \end{aligned}$$

Hint: First use the Extended Euclidean Algorithm to invert 13 mod 99 and 15 mod 101 in order to obtain a system of congruences where the coefficients of x are 1, then apply the Chinese Remainder theorem. You may want to use a calculator, there are *many* (simple) calculations in this exercise.

3. **Public-Key Infrastructures:** Assume revocation of certificates is handled in the following way: when a user Bob claims that the private key corresponding to his public key pk_B has been stolen, the user sends to the CA a statement of this fact signed with respect to pk_B. Upon receiving such a signed message, the CA revokes the appropriate certificate.
Explain why it is not necessary for the CA to check Bobs identity in this case. In particular, explain why it is of no concern that an adversary who has stolen Bobs private key can forge signatures with respect to pk_B (Exercise 12.13 in [KL]).