Cryptography, winter term 16/17: Assignment 11

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

Due February 1st, 2017

Exercise 11.1 (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 11.2 (Key encapsulation, 2 + 3 Points) Let $\Pi = (\mathrm{Gen}, \mathrm{Encaps}, \mathrm{Decaps})$ be a CCA-secure KEM.

(a) Given a PRG G, construct a CPA-secure public-key encryption scheme and prove security.

(b) Given a PRF F, construct a CCA-secure public-key encryption scheme and prove security.

Exercise 11.3 (Key-exchange and CPA security, 6 Points) Let Π be a *two round* key-exchange protocol, that is, trans consists of two messages t_1 (which was sent from Alice A to Bob B) and t_2 (which was sent from B to A afterwards). Furthermore, we assume Π to be secure in the presence of an eavesdropper. We construct a public-key encryption scheme Π' from Π as follows:

- Gen simulates A until it outputs a message t_1. Let s be the state of A at this point in the simulation [1]. Then we output $\mathrm{pk} = t_1$ and $\mathrm{sk} = s$.
- Enc_{t_1}, on input m, first simulates B with t_1. At some point B will output a message t_2 (for A) and furthermore, it will eventually output a key k. Now Enc_{t_1} outputs $c := (t_2, m \oplus k)$.
- Dec_s, on input $c = (t_2, c')$, continues the simulation of A at point s by giving t_2 to A. Eventually, A will ouput a key k (which follows from the definition of a key-exchange protocol). Now Dec_s outputs $c' \oplus k = m \oplus k \oplus k = m$.

Prove that Π' is a CPA-secure public-key encryption scheme.
Hint: It may be advisable to do a proof by reduction.

Exercise 11.4 Prove formally that the El Gamal encryption scheme is not CCA-secure, that is, provide an adversary $\mathcal{A}$ for the CCA-experiment that wins it with probability non-negligibly greater than $\frac{1}{2}$.

[1] You can think of A being ”stopped” as soon as t_1 was sent. Then s is the encoded information that is needed to continue the simulation of A. For this exercise, you do not need any further details of s or its encoding.