Foundation of Cryptography (0368-4162-01), Fall 2011 Iftach Haitner

Problem set 6, exercises 12-13

January 25, 2012 Due: February 16

- Send your solutions in a PDF format to foc.exc@gmail.com.
- Solution for each exercise should be emailed *separately*, title: Exe # (e.g., 3), Id (Israel id) (write the same details in the body of the attached file).
- Please *don't* write your name in the email/attached file.
- Write clearly and shortly using sub claims if needed. The emphasize in most questions is on the proofs (no much point is writing a "solution" w/o proving its correctness)
- For Latex users, a solution example can be found in the course web site.
- In case you work in (small) groups, please write the id list of your partners in the solution file. I stress that each student should write his solution by *himself* (joint effort is only allowed in the "thinking phase")
- The notation we use appear in the first lecture (www.cs.tau.ac.il/∼iftachh/Courses/FOC/Fall11/Slides/OWF.pdf), section "Notation"

Exe 12: Assuming that TDP exists.

1. (5 points) give an example of a semantically-secure public-key encryption scheme, that is *not* CPA secure
2. (5 points) give an example of a CPA-secure public-key encryption scheme, that is *not* CCA1-secure.

Exe 13, (10 points): Prove Theorem 25 in Lecture 8