CSIC 4331/6331 November 18, 2019

Quiz 7

Name:

In this quiz you will work through encryptions using El-Gamal, (plain) RSA, and Paillier encryption by hand. For each of these, show the outputs of KeyGen, Enc, and Dec. Compute by hand and show your work (like we did in class).

1. **El Gamal**
   Let G be the group of quadratic residues mod 11 (Recall that quadratic residues are values $x \in G$ s.t. $\exists y \in g$ for which $x = y^2$).

   (a) Show an execution of Gen when we choose $g = 4^2 = 5 \bmod 11$ and $sk = 4 \in \mathbb{Z}_5$

   (b) Show an execution of Enc when $m = 4$ and the randomness $y = 3 \in \mathbb{Z}$

   (c) Show an execution of Dec on the obtained ciphertext.

2. **RSA**
   Let G be the group $\mathbb{Z}_{15}^*$

   (a) Show an execution of Gen when we choose $e = 3$

   (b) Show an execution of Enc when $m = 7$

   (c) Show an execution of Dec on the obtained ciphertext.

3. **Paillier**
Let $N = 15$, $N^2 = 225$. We will work in the group $\mathbb{Z}^*_{N^2}$.

(a) Show the output of Gen

(b) Show an execution of Enc when $m = 2$ and the randomness $r = 1 \in \mathbb{Z}^*_{15}$

(c) Show an execution of Dec on the obtained ciphertext. Note that $[31^8 \bmod 225] = 16$.