CSCI 4331/6331

Quiz 9

Name:

In this quiz you will work through encryptions using El-Gamal, (plain) RSA encryption, and (plain) RSA signatures 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 $m = 4 = 2^2$ and the randomness $y = 3 \in \mathbb{Z}$

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

2. **RSA Encryption**
   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. **RSA Signature**
Let G be the group $\mathbb{Z}_{15}^*$ and we choose $e = 3$ (as in Problem 2)

(a) Show an execution of Sign on $m = 4$

(b) Show an execution of Verify on the generated signature