CSIC 4331/6331 November 20, 2019

Homework Assigment 6

Due Dec. 2

Please answer each of the below questions. Remember, you may work together, but everyone MUST type up and understand their solutions. Solutions that appear copied will be considered a violation of the academic honesty code. Also, you must list all people you work with on this homework as well as any outside resources (e.g., web search, books, etc.) that you use.

For problems 1-3, compute by hand and show your work. Problems 4-6 are based on material we will cover in class on November 25th. Problem 7 is extra credit.

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 $[31^8 \bmod 225] = 16$.

4. Exercise 12.3 in the book
   In Section 12.4.1 we showed an attack on plain RSA signature scheme in which an attacker forges a signature on an arbitrary message using two signing queries. Show how an attacker can forge a signature on an arbitrary message using a *single* signing query.

5. Exercise 12.4 in the book
   Assume the RSA problem is hard. Show that the plain RSA signature scheme satisfies the following weak definition of security: an attacker is given public key (N, e) and a uniform message $m \in \mathbb{Z}_N^*$. The adversary succeeds if it can output a valid signature on m without making any signing queries.

6. Exercise 12.10 in the book
   Consider the Lamport signature scheme. Describe an adversary who obtains signatures on *two* messages of its choice and can then forge signatures on any message it likes.

7. **Extra Credit:** Exercise 13.2 in the book.
   Show that the isomorphism of Proposition 13.6 ($f : \mathbb{Z}_N \times Z_N^* \to \mathbb{Z}_{N^2}^*$ given by $f(a, b) = [(1 + N)^a \cdot b^N \bmod N^2]$) can be efficiently inverted when the factorization of N is known. Note that for $N = pq$, $\phi(N^2) = p \cdot (p - 1) \cdot q \cdot (q - 1)$.