CSE 207B
Applied Cryptography

October 26, 2023
Due: Thursday, November 9

Homework 5

Your homework should be submitted electronically via Gradescope before class on the due date. Please type up your solutions to the following problems using Latex and submit in pdf form as `hw5-solutions.pdf`, along with a text file `hw5-sol.py` containing the code you used to solve the first part. Please credit any collaborators you worked with and any sources you used.

---

0. (a) Describe the vulnerability you exploited.

   (b) Describe how you exploited the vulnerability.

   (c) How should an implementer protect against this vulnerability?

1. The Boneh & Shoup textbook calls the variant of ElGamal that was used in the decryption "multiplicative ElGamal". In these problems we will explore more about the structure of this problem. Let G be a cyclic group of prime order q generated by $g \in G$.

   - The key generation algorithm runs as follows: $a \leftarrow \mathbb{Z}_q$, $u \leftarrow g^\alpha$, $pk \leftarrow u$, $sk \leftarrow \alpha$
   - For a given public key $pk = u \in G$ and message $m \in G$,
   $$\text{Enc}_{pk}(m) = \beta \leftarrow \mathbb{Z}_q, v \leftarrow g^\beta, e \leftarrow u^\beta \cdot m, \text{ output } (v, e)$$
   - For a given secret key $sk = \alpha \in \mathbb{Z}_q$ and a ciphertext $(v, e) \in G^2$,
   $$\text{Dec}_{sk}(v, e) = e/v^\alpha$$

   (a) Show that this encryption scheme is semantically secure assuming the DDH assumption holds in G. In particular, you should show that the advantage of any adversary A in breaking the semantic security of E is bounded by 2ϵ, where ϵ is the advantage of an adversary B (which is an elementary wrapper around A) in the DDH attack game.

   (b) Show that this encryption scheme is not semantically secure if the DDH assumption does not hold in G.

   (c) Show that this encryption scheme has the following property: given a public key pk and two ciphertexts $c_1 \leftarrow \text{Enc}_{pk}(m_1)$ and $c_2 \leftarrow \text{Enc}_{pk}(m_2)$, it is possible to create a new ciphertext c that is an encryption of $m_1 \cdot m_2$. This property is called a multiplicative homomorphism.

2. Let p and q be large primes such that q divides $p - 1$. Let G be the order q subgroup of $\mathbb{Z}_p^*$ generated by $g \in G$ and assume that the DDH assumption holds in G. Suppose we instantiate the multiplicative ElGamal scheme described above with the group G. However, plaintext messages are chosen from the entire group $\mathbb{Z}_p^*$ so that the system is defined over $(\mathbb{Z}_p^*, G \times \mathbb{Z}_p^*)$. Show that the resulting system is not semantically secure.