Mathematics 3159B **Bradley Assaly-Nesrallah**
Introduction to Cryptography
Assignment 2, Problem 1 Due Date: October 6, 2020

Solution

We fix a large prime p and a primitive root g mod p. Assume Alice and Bob are communicating via the ElGamal PKC and that eve is an adversary. Let a be Alice's private key and k be Bob's private key, and m be Bob's message.

1.We state the ElGamal Problem, ie, the underlying computational problem of the ElGamal cryptosystem, as follows:
Eve is given $A \equiv g^a \pmod{p}$, $C_1 \equiv g^k \pmod{p}$, $C_2 \equiv m \cdot A^k \pmod{p}$ and must solve for the message m.
The ElGamal Problem is to solve for $(g^{ak})^{-1} \equiv ((g^a)^k)^{-1} \equiv A^{k^-}1 \pmod{p}$ when given g^a and g^k, which are used to compute $(g^{ak})^{-1} \cdot C_2 \equiv m \mod p$.

2.We want to show that if Eve has a Diffie-Hellman Oracle then she can solve the ElGamal problem.

Proof. Suppose that Eve has a Diffie-Hellman Oracle, namely that that given any A, B $\in \mathbb{F}_p$ such that $A \equiv g^i \pmod{p}$ and $B \equiv g^j \pmod{p}$ for some $i, j \in \mathbb{N}$ the Oracle will return the value g^{ij} in polynomial time.
Eve knows $A \equiv g^a \pmod{p}$, $C_1 \equiv g^k \pmod{p}$ and $C_2 \equiv m \cdot A^k \pmod{p}$.
Eve knows the values of g^a and g^k,
Thus Eve may now use the Diffie-Hellman Oracle to compute the value of $g^{ak} \pmod{p}$ in polynomial time.
We know that $g^{ak} \equiv (g^a)^k \equiv A^k \pmod{p}$,
Hence Eve may obtain the message m, by computing $(g^{ak})^{-1} \cdot C_2 \equiv m \mod p$, using the EEA to find the inverse and the fast powering algorithm to compute the exponents, which are both in polynomial time.
Thus Eve has solved the ElGamal Problem in polynomial time, so we are done. □