Cryptology Exercise Week 9

Zijun Yu 202203581

Octobor 2023

CPA security of El Gamal

The algorithm B works by sending $(\alpha^b, \alpha^c \cdot m)$ to Adv and outputs the same result as A does.

In the case where B is called on $(\alpha^a, \alpha^b, \alpha^c)$ where $c = ab$, what Adv sees is identical to interacting with the "real" oracle. In the case where B is called on $(\alpha^a, \alpha^b, \alpha^c)$ where c is random, what Adv sees is that it is talking to the "ideal" oracle, since $\alpha^c \cdot m$ is indistinguishable from the encryption of a random message, which is what the "ideal" oracle does, i.e. $\alpha^{ab} \cdot r$. (Given c and r are uniformly random values from the group, $\alpha^c \cdot m$ and $\alpha^{ab} \cdot r$ are also two uniformly random values, hence they are indistinguishable.)

This construction thus turns an adversary that breaks El-Gamal into one that breaks DDH with the same advantage.