Cryptology Exercise Week 9

Zijun Yu 202203581

Octobor 2023

CPA security of El Gamal

The adversary Adv plays the CPA game, which means that it has the public keys G, α, and α^a. It then chooses a message m and sends to the oracle, and gets back (α^r, x). Let G, α, α^a, α^r, and $x \cdot m^{-1}$ be the inputs to B, namely G, α, α^a, α^b, and α^c. So $r = b$. Then notice that x is either $\alpha^{ab} \cdot m$ when we are in the real world, or $\alpha^{ab} \cdot s$, for some random s, when we are in the ideal world. We can rewrite $\alpha^{ab} \cdot s = \alpha^{ab} \cdot m \cdot \alpha^t = \alpha^{ab+t} \cdot m$. Because s is uniformly random, $ab + t$ is also uniformly random. This means that the oracle is always responding with $x = \alpha^c \cdot m$, where c is either ab or uniformly random, and Adv can distinguish between these two cases with advantage ϵ. We then simply let B output the same as Adv does and B will have ϵ advantage at distinguishing c is ab or uniformly random in α^c (since $x \cdot m^{-1}$ is exactly α^c).