Network Security Technology

Tutorial 6, Week 6 (March 30) Due Date: April 6

薛春宇 518021910698

---

1. El Gamal 加密方案 (100 points)

对照 PKE 的 CCA 模型，说明 El Gamal 加密方案不是 CCA 安全的。

Answer：

记 *El Gamal* 加密方案为 Π，攻击者 *A*，我们证明 Π 在 *A* 下不满足 *CCA* 安全。攻击者 *A* 的算法如下：

在 *CCA* 的挑战阶段，攻击者 *A* 选择长度相同的明文：$m_0^* = x$，$m_1^* = y$，并将明文对 (m_0^*, m_1^*) 发送给被攻击者，被攻击者选择一个特殊的比特 $b \in \{0,1\}$，以此为依据选择使用哪一个明文，并计算 $c^* \leftarrow Enc(pk, m_b^*)$，将挑战密文 $c^* = (c_1, c_2)$ 提供给攻击者 A。

攻击者 *A* 随机选择一个唯一的 $z \in Z_q$，将挑战密文 c^* 的 c_2 乘以 *z*，得到一个**新的密文** $c_{new} = (c_1, c_2 \cdot z)$，并用该密文询问解码机 *decryption oracle*，将得到的结果除以 *z*，则要么是 m_0^* 要么是 m_1^*，对应了在挑战阶段被攻击者选择加密的明文。

在上述算法下，攻击者 *A* 会以不可忽略的优势赢得基于 *EI Gamal* 加密方案下的 *CCA* 挑战，即 Π 在 *A* 下不满足 *CCA* 安全。