

Network Security Technology

Spring, 2021

Tutorial 6, Week 6 (March 30)

LIU Zhen

Due Date: April 6

作业题目:

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。