**密码学原理**

**实验二：对称加密与认证**

学号： 姓名：

**实验目的**：本实验旨在掌握运用密码学工具实现CPA安全加密与CCA安全加密，并采用CCA能力攻击CPA安全加密方案。

1. **使用密码学工具实现CPA安全加密算法**
2. 使用密码学工具实现CPA安全加密方案

要求：选择CPA安全的加密方案对一个图片内容进行加密和解密，密文文件可用图片浏览器打开。

1. **采用CCA攻击分析CPA安全加密方案**
2. 利用CCA能力敌手攻击CPA安全的加密方案

要求：对上一步中CPA安全加密方案加密的图片文件进行CCA攻击：篡改密文图片，然后用解密预言机对篡改图片解密。

1. **使用密码学工具实现CCA安全的加密算法**
2. 使用密码学工具实现CCA安全加密方案

要求：选择CCA安全的加密方案对一个图片内容进行加密和解密，密文文件可用图片浏览器打开。

1. CCA敌手能否攻击成功CCA安全的加密方案

要求：尝试用第2步CCA攻击来攻击CCA安全加密的图片。