《RSA加密实验》说明

# 实验指导书勘误

由于实验网站上没有修改权限，暂时无法对实验指导书中存在的问题进行修改，现将部分问题在这里说明：

## 实验环境

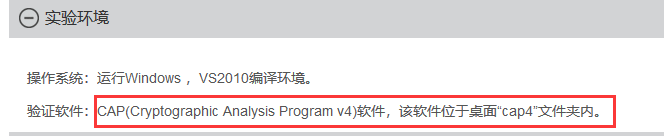


图 1 错误一

如图1是实验环境说明，实验中实际上不限制操作系统和编译环境，大家可以使用自己顺手的开发环境；

验证软件实际上并不在“cap4”文件夹，验证软件是远程桌面的“RSA加解密实验”文件夹中的一个压缩包：bmrsall.zip，解压后可以**按照README文件进行操作**，对照源代码进行理解学习并在实验报告中写出。

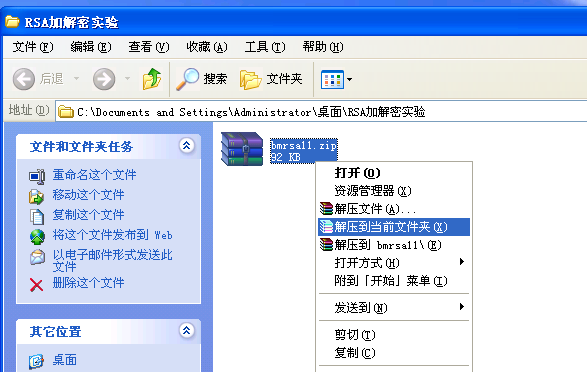
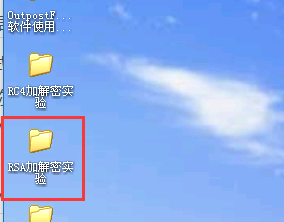


图 2 RSA加解密实验

## 实验任务二



图 3 错误二

如图2是实验任务二，实际任务是实现RSA加密算法（IDEA是另一种算法）。

实验指导书中的源代码对于不同开发环境可能需要进行适当修改，为了方便大家下载源码，在代码托管平台“码云”上传了代码片段（已在Codeblocks 17.10上运行通过）：<https://gitee.com/hitfyd/codes/i36h42myzecjol9sqb0dk35>。

# 远程桌面

远程桌面需要同意实验声明才能使用：



图 4 声明

本次实验中主要使用远程桌面上的“RSA加解密实验”文件夹。

# 其他问题

## 页面404

如果发现实验页面显示404，可以更换Chrome、Firefox浏览器重试，已经发现360极速、qq、edge、IE等浏览器可能显示页面404。

## 远程桌面连接问题

部分账户的远程桌面可能无法连接正常使用，可以联系助教解决。

## 实验操作分（！！！不计入分数！！！）

**由于第二、三组同学无法统计操作分，这一部分分数不再统计。**

实验具有操作分，即需要点击实验指导书中的若干个“已学”按钮。（第二、三组做实验的同学可能发现“已学”按钮已经操作过了是因为实验系统无法对清楚第一组的操作状态！！！！）

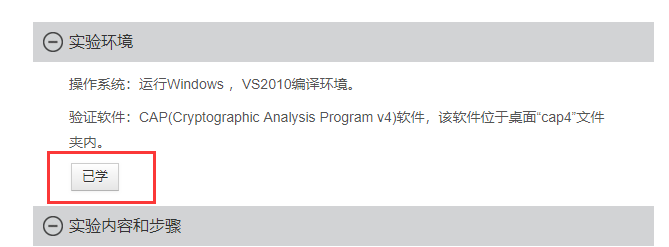


图 5 未操作



图 6 已操作

## 实验报告

每次实验的实验报告以10分制进行打分，期末再按照一定比例折合进总分。

实验报告应使用网站提供的模版，报告可以重复提交；如果逾期未提交可联系助教说明。

第二、三组的同学可能发现实验报告显示已提交，是第一组同学提交的实验报告，需要大家重新上传即可。

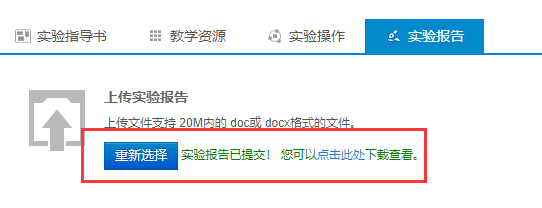


图 7 实验报告

同时发现大家提交的实验报告中部分格式较为混乱，希望大家重视文档格式，**格式、排版、标题等清晰明白的可酌情高分**。

## 改进意见

欢迎大家对实验提出改进意见，每一组提交实验报告后会统计整理大家的意见，对部分在权限内的可行意见加紧修改，对部分暂时无法改进的可行意见反映给任课老师。