题目：密码算法教学实验系统设计与实现

一、题目内容：

本课题来源于“密码学导论”课程教学需求，主要通过学习现有各类密码学函数库，针对密码学导论课程教学过程的需要，设计并实现一个适合初学者学习的教学平台。

二、任务要求：

1. 了解密码学对称加密、哈希算法、消息认证码算法等对称密码体制先关的知识；

2、 了解密码学非对称加密、数字签名等非对称密码体制相关的知识；

3、 了解数字证书和公钥基础设施等知识；

4、熟悉Python或者C语言，以及基于该编程语言实现的密码学库，如pypbc库、openssl库、RELIC库、Miracl库等。

5、完成毕业设计（论文）外文翻译，锻炼跨文化交流的语言和书面表达能力，能就工程专业问题，在跨文化背景下进行基本沟通和交流；

6、 完成毕业设计论文并提交软件及相关文档；

三、毕业设计进度安排示例：

A.复习密码学基础算法的理论知识（第1周-第3周）

B.学习并掌握前述密码学库的应用（第4周-第8周）

C.利用前述密码库，进行编程开发，设计并实现密码学实验教学系统（第9周-第14周）

D.完成毕业论文，提交软件及相关文档。（第14周-第15周）

E.完成本科生毕业设计（论文）外文翻译；（第1周-第15周）

F.完成本科生毕业设计（论文）答辩；（第1周-第15周）

四、参考文献示例：

[1] <https://openi.org.cn/index.php?m=content&c=index&a=show&catid=87&id=62>

[2] https://www.researchgate.net/publication/348392410\_mimaxuehunheshikechengjianshetansuo