Network Security Technology	Spring, 2021
Tutorial 5, Week 5 (March 23)	LIU Zhen
Due Date: March 30	

作业题目:

1. **随机素数生成算法** (50 points)

   (1) 实现 PPT《网络安全技术 5 公钥密码学-2 数学基础》第 39 页所述的生成随机素数的算法，并生成至少 2 个 32-bit 的素数，不需要第三方大整数运算库。(需要学习与实现 perfect power 的判定)

   (2) 学习开源库中已有的素数生成算法，撰写报告，阐明比我们讲的原理、比你的实现更优化的地方。

2. **RSA 算法** (50 points)

   检索和阅读文献，写一篇简单的 survey，包括历史上提出的一些要得到实际中可以安全使用的 RSA 加密的尝试，以及目前产业界在实际使用的基于 RSA 的公钥加密方案。给出其中各方案的具体算法、优缺点、解决了的问题、存在的问题等。