大作业：期末研究报告

大作业占 40 分，形式是每人提交一份学习研究报告，内容是选取与该课程内容相关的某一主题，阅读相关文献，在报告中展示学习、**思考**、研究的结果。选取的主题并不需要十分复杂，表达清楚、排版优美、生动有趣……这些都是好文章的特点。

大作业有以下几个要求：

- 报告中请包含自己的思考
- 请避免报告中出现手写的部分
- 请以pdf形式提交

我们在此提供一些可供选择的主题（问题），并附上了一些资料，供大家参考，大家也可以自行选择感兴趣的问题：

1. 集合论与数学基础
    - Cantor-Bernstein 定理
        - 定理简介
    - ZFC 公理集合论；选择公理、良序公理与佐恩引理
        - 《数学基础》汪芳庭
2. 数论算法
    - 大数分解的快速算法（例如 Pollard's rho 算法）
        - Pollard-Rho算法
    - 素数的判定算法（例如 Miller-Rabin 算法）
        - Miller-Rabin 和 PollardRho讲解
        - Miller-Rabin
        - Miller-Rabin
3. 密码学
    - 基于RSA的电子签名
        - 数字签名介绍
        - 数字签名介绍
        - 数字签名和数字证书介绍
    - 哈希函数：Leftover Hash Lemma
        - Leftover Hash Lemma介绍
        - Leftover Hash Lemma, Revisited
        - Extractors and the Leftover Hash Lemma
    - 零知识证明
        - 零知识证明介绍
    - 多方安全计算
        - a pragmatic introduction to secure multi-party computation这里面囊括了很多的MPC协议，大家可以根据兴趣自行阅读
    - 格密码
        - 格密码简介
        - Lattice Based Cryptography for Beginners

- A Graduate Course in Applied Cryptography：这本书里面包含了基本上所有密码学的知识，有公钥密码（Public Key Cryptography），零知识证明（Zero Knowledge Proofs），大家可以根据需要直接看某一章的内容（具体也可参考Stanford CS 255里面有标明每个内容对应的章节）
- Stanford CS 355里面同样也有很多Lecture Notes值得参考

4. 确定有限状态自动机（Deterministic Finite Automata）
   - DFA简介
   - DFA简介
   - 正则语言与 Pumping Lemma
     - 正则语言介绍
     - Pumping Lemma介绍
   - Synchronizing word and Černý conjecture
     - Synchronizing word
     - Černý conjecture
5. 随机与伪随机
   - Markov Chain
     - Markov Chain介绍
     - Markov Chain Monte Carlo介绍
   - Pseudorandom Generator（伪随机数产生器）
     - 硬件PRNG介绍
     - Cryptographically secure PRNG介绍
     - Cryptographically secure PRNG的一种算法Dual_EC_DRBG
   - Yao's principle (also called Yao's minimax principle)
     - Yao's minmax principle cmu15859
     - Yao's principle介绍1
   - 线性规划中的对偶理论（Duality Theory）
     - 对偶理论的介绍
     - 强对偶理论的介绍
6. 量子计算
   - The Limits of Quantum Computers
   - 量子计算简介
   - UC Berkeley CS294-2 这门课有详细的lecture notes，对量子计算感兴趣的同学可以自行阅读
   - UC Berkeley CS191 这门课同样有详细的lecture notes，对量子计算感兴趣的同学可以自行阅读
   - Einstein–Podolsky–Rosen paradox (EPR paradox)
     - EPR简介
     - The Einstein-Podolsky-Rosen Argument in Quantum Theory
   - No-cloning Theorem
     - No-cloning Theorem简介
7. 计算机体系结构（Computer Architecture）
   - UC Berkeley cs61c 这门课里面讲解了计算机体系结构的伟大思想，有slide和video（B站），对arch感兴趣的同学可以自行了解
   - UC Berkeley cs152 这门课讲解了计算机体系结构，有slide，对arch感兴趣的同学可以自行了解

- 《Computer Architecture A Quantitative Approach》这本书里面详细讲解了计算机体系结构的各个部分，，对arch感兴趣的同学可以自行阅读
- 局部性原理和内存层次
  - Skewed associativity enhances performance predictability
  - Data caches for superscalar processors
  - Improving direct-mapped cache performance by the addition of a small fully-associative cache and prefetch buffers
  - High-bandwidth data memory systems for superscalar processors
  - Organization and performance of a two-level virtual-real cache hierarchy
  - A new era of fast dynamic RAMs
  - A case for direct-mapped caches,
  - Dead-Block Prediction and Dead-Block Correlating Prefetchers
- 并行与流水线
  - An analysis of pipeline clocking
  - The microarchitecture of superscalar processors
  - Implementing precise interrupts in pipelined processors
  - The MIPS R10000 superscalar microprocessor
  - Intel's P6 uses decoupled superscalar design
  - Digital 21264 sets new standard
  - The Alpha 21264 microprocessor
  - UltraSPARC-III: designing third-generation 64-bit performance
  - AMD 3DNow! technology: architecture and implementations
- 性能评估与指令集
  - (J. von Neumann) Preliminary discussion of the logical design of an electronic computing instrument, Report to the U.S. Army Ordinance Department, 1946.
  - SPEC95 retires SPEC92
  - (G. M. Amdahl) Validity of the single-processor approach to achieving large scale computing capabilities, April 1967.
  - Technology 1996: Solid state
  - The future of microprocessors
  - Compilers and computer architecture
  - Performance from Architecture: Comparing a RISC and CISC with similar hardware organization
  - PowerPC 601 and Alpha 21604: A tale of two RISCs, IEEE Computer, vol. 27, no. 6, pages 12-24, June 1994.

8. 操作系统
   - 复用（时分复用、资源复用）
     - The UNIX TimeSharing System https://dsf.berkeley.edu/cs262/unix.pdf
     - Multics：Wiki https://en.wikipedia.org/wiki/Multics；相关文章：https://www.multicians.org/papers.html
   - 文件系统
     - A Fast File System for UNIX
     - Measurements of a Distributed File System
     - Serverless Network File Systems
     - Disconnected Operation in the Coda File System
   - 虚拟内存
     - Machine-Independent Virtual Memory Management for Paged Uniprocessor and Multiprocessor Architectures
     - Application-Controlled Physical Memory using External Page-Cache Management

        - Virtual Memory Primitives for User Programs
        - Lightweight Recoverable Virtual Memory
        - Logged Virtual Memory
    - 分布式一致性协议
        - Paxos Made Simple https://lamport.azurewebsites.net/pubs/paxos-simple.pdf
        - Raft一致性算法 https://raft.github.io/
        - Chord协议：http://pdos.csail.mit.edu/papers/chord:sigcomm01/chord_sigcomm.pdf
9. 网络
    - OSI模型
    - page rank
    - 拥塞控制
    - TCP UDP