附：复旦大学博士资格考试安排表内考试科目考察要点及参考学习资料
本方案适用 2025 级及以前入学的博士研究生

考试科目 1：计算机编程基础（不分学科方向）

（一）考查知识内容或学术能力要点

主要考查内存数据组织，包括数组（连续存储方式下的一维、二维、三维数组地址计算）、顺序表（查找算法、插入算法和删除算法；性能评估）、链表（带表头结点单链表查找算法、插入算法和删除算法；循环链表查找算法、插入算法和删除算法；双向循环链表查找算法、插入算法和删除算法）、栈（顺序栈、多栈共享一段连续存储空间；链式栈；进栈算法、出栈算法、取栈顶算法和栈空栈满判定）和队列（循环队列进队算法、出队算法、取队头算法和队空队满判定）、递归（递归算法设计与实现；渐进时间复杂性评估）、非递归（递归算法到非递归算法的变换；渐进时间复杂性评估）、树（二叉树性质、二叉树遍历算法、二叉树计数求解；堆、调整算法、插入算法和删除算法）、图（图邻接矩阵、邻接表存储；图深度优先搜索遍历算法、广度优先搜索遍历算法；最小生成树构建、基于克鲁斯卡尔算法的构建实现、基于普利姆算法的构建实现；迪克斯特拉单源非负最短路径求解算法；拓扑排序算法；关键路径求解）、搜索结构（无序表和有序表顺序搜索算法；折半搜索递归和非递归算法；搜索性能评估；二叉搜索树构建算法、插入算法和删除算法；AVL 树四种平衡化旋转方式、AVL 树构建）、内排序（直接插入排序算法；冒泡排序算法；直接选择排序算法；快速排序算法；归并排序算法；基数排序算法；各类内排序方法性能比较与分析）等结构的有关性质及相关算法。在理论方面，要求熟练掌握各种结构的有关性质和算法，充分理解，灵活运用，同时掌握算法时空性能分析的基本技巧。在实践方面，能够利用 C/C++语言正确并熟练实现各种数据结构和有关算法，合理应用于各种问题的解决。

对应核心课程：

CS10004 《程序设计》周水庚 （本科课程）
CS20009 《数据结构》张玥杰 （本科课程）

（二）参考学习资料

殷人昆主编，《数据结构（用面向对象方法和 C++描述）》（第 2 版），清华大学出版社，2012 年。

计算机科学与技术一级学科

考试科目 2：智能化算法与系统

（一）考查知识内容或学术能力要点

考查内容包括 A、B 两个部分，每个部分提供三个内容选项，考生需从 A、B 两个部分中各选一个选项。

A：算法基础与应用（50 分）

A1 选项：算法理论与应用（对应《算法续论》）
A2 选项：神经网络与深度学习（对应《神经网络与深度学习》）
A3 选项：大数据挖掘（对应《大数据挖掘》）

B：计算机系统与分析（50 分）

B1 选项：高级网络（对应《高级网络》）
B2 选项：分布式数据库（对应《分布式数据库》）
B3 选项：程序分析技术（对应《程序分析》）

对应核心课程：

CS50034《算法续论》赵运磊
CS60010《神经网络与深度学习》邱锡鹏
CS70010《大数据挖掘》熊赟
CS50007《高级网络》吕智慧、赵进
CS60006《分布式数据库》卢暾
CS60027《程序分析》李弋

（二）各选项考查要点及参考资料

A：算法基础与应用（50 分）

- **A1：**《算法理论与应用》考查要点：

  1. 排序算法：快速排序，插入排序、二分排序
  2. 模拟算法：穷举、模拟场景
  3. 分治算法：最大子串和、第 k 小，归并排序
  4. 动态规划：贪心算法、动态规划
  5. 数/图：最小生成树算法

主要参考学习资料：

书名:《Introduction to Algorithms》Third Edition 作者：Thomas H. Cormen，

Charles E. Leiserson，Ronald L. Rivest，Clifford Stein. 出版社：Cambridge, Massachusetts London, England，Massachusetts Institute of Technology ISBN : 978-0-262-03384-8

其他参考学习资料：

书名：算法设计与分析 作者：王红梅 出版社：清华大学出版社，2006

- **A2**：《神经网络与深度学习》考查要点：

1.了解机器学习的基本概念和基础知识

（1）《神经网络与深度学习》2.1-2.2 节

（2）《神经网络与深度学习》3.1-3.3 节

2.熟悉神经网络的主要模型（前馈网络、卷积网络、循环网络等）

（1）《神经网络与深度学习》4.1-4.3 节

（2）《神经网络与深度学习》5.1-5.2 节

（3）《神经网络与深度学习》6.1-6.2、6.5-6.6 节

3.了解神经网络的优化和正则化方法

《神经网络与深度学习》7.1-7.2、7.7 节

参考学习资料：

邱锡鹏，神经网络与深度学习，9787111649687，机械工业出版社，2020.4

- **A3**：《大数据挖掘》考查知识内容或学术能力要点：

1. 熟悉数据挖掘的任务及其应用，了解大数据挖掘的特点及其挑战（第 1 章）：

（1）列举五大类数据挖掘任务及其定义；

（2）分别给出各类数据挖掘任务的应用案例。

2.掌握经典关联分析算法（Apriori、FPGrowth）、聚类算法（KMeans、DBSCAN）、分类算法（决策树、朴素贝叶斯）的原理、指标及可改进优化的基本思想和方向（3.3 节、4.2 节、5.3 节）：

（1）列举关联分析、聚类、分类这三大类数据挖掘任务的代表性算法的名称；

（2）给出 Apriori 性质及其优势和局限；

（3）给出 KMeans 算法的优势和局限性；

（4）给出分类算法的准确性评价指标。

3.了解异质数据网络基本概念、能应用异质网络进行数据建模（9.1 节、9.2 节）：

（1）给出异质网络、异质网络挖掘的定义并举例；

（2）对论文标题、论文作者等数据集转化为异质网络数据的表示；

（3）举例在上述数据集上可以做的数据挖掘应用场景。

参考学习资料：

熊赟,朱扬勇,陈志渊.《大数据挖掘》.上海科学技术出版社.

B：计算机系统与分析（50 分）

■ **B1**：《高级网络》考查要点：

1.计算机网络的定义、基本原理和体系结构：了解互联网的定义与组成、计算机网络的分类性能指标、网络体系结构的概念，熟悉主要的模型与层次划分（对应主要参考资料第 1 章）

2.网络核心协议 TCP/IP 的工作机制、拥塞控制：熟悉 IP 协议的基本原理、路由选择协议 RIP 和 OSPF 的工作机制；熟悉 TCP 的基本原理、流量控制的工作机制，掌握拥塞控制的算法，包括慢启动、拥塞避免、快速重传、快速恢复（对应主要参考资料章节 4.2、4.5、5.3、5.7、5.8）

3.网络多媒体传输及典型协议（RTP、SIP）：了解互联网多媒体的需求与分类，熟悉 RTP、SIP 协议的基本工作原理（对应主要参考资料章节 8.1、8.3）

4.互联网的服务质量（QoS）：了解服务质量的概念，掌握调度机制 FIFO、FQ、WFQ 的工作机制和特点（对应主要参考资料章节 8.4）

主要参考学习资料：

计算机网络（第 7 版） 作者:谢希仁 编著 出版社:电子工业出版社出版，2017 年 01 月

其他参考学习资料：

高级计算机网络（第 2 版） 作者：徐恪、徐明伟、李琦， 清华大学出版社，2021 年 03 月

■ **B2**：分布式数据库考查要点：

1.分布式数据库管理系统架构与设计（对应教材的第 3 章）

考察分布式数据库管理系统体系架构，分布式数据库设计方法，分布式数据库水平分片和垂直分片技术，以及分片分配方法等。具体包括：

（1）分布式管理系统的描述模型

（2）分布式数据库设计策略

（3）分片类型和分片原则

（4）水平分片的主要方法与过程

（5）垂直分片的主要方法与过程

2.分布式数据库查询与优化（对应教材的第6~8章）

考察分布式数据库查询处理方法，特别是带分片的分布式连接和半连接操作处理，以及经典的分布式查询优化算法与代价分析等。具体包括：

（1）查询优化过程和相关算法

（2）分布式代价模型与代价函数

（3）连接、半连接等常见查询操作结果大小的估算

（4）分布式查询中连接操作优化方法

（5）分片分配问题及其解决方法

3.分布式事务处理与故障恢复（对应教材的第10~13章）

考察分布式事务的性质与类型，可序列化理论，经典的分布式并发控制算法；分布式数据库故障与可靠性协议，分布式数据复制与一致性维护，以及分布式系统常见理论（CAP理论、BASE理论等）等。具体包括：

（1）事务的ACID性质及事务的形式化定义

（2）序列化的形式化定义与可序列化调度

（3）常见悲观和乐观并发控制算法（含基于锁/时间戳的算法等）

（4）可靠性保障协议（含原子提交、非阻塞终止与独立恢复等协议）

（5）复本数据库的一致性、更新管理与复制协议

参考学习资料：

分布式数据库系统原理（第3版） [Principles of Distributed Database Systems(Third Edition)]. [德] 顾兹叙（M.Tamer Ozsu），[德] Patrick Valduriez 编，周傲柱，范举，吴昊 等译. 清华大学出版社，ISBN：9787302346005. 2014-05-01.

■ B3：程序分析技术考查要点：

1.程序语言的类型和特点：命令语言、函数语言和逻辑语言

2.静态类型、动态类型、子类型和类型推断

3.程序语法和语义：抽象语法树 (AST, Abstract Syntax Tree)、中间表达式 (IR, Intermediate Representation)、程序状态和执行轨迹 (Trace)

4.部分函数、可计算性、图灵机和 Lambda 演算、格 (Lattice) 理论、最小不动点 (Least Fixed Point) 以及 Rice 定理

5.过程内分析：控制流 (Control Flow)、数据流 (Data Flow)、定义-调用链 (Define-Use Chain)、静态单赋值 (Static Single Assignment)、流敏感(Flow Sensitive)和流不敏感 (Flow Insensitive)

6.过程间分析：模块化分析、调用图、上下文敏感 (Context Sensitive) 分析和函数摘要

7.抽象解释 (Abstract Interpretation)：抽象域 (Abstract Domain)、实际域 (Concrete Domain)、Galois Connection 和运算的抽象解释

8.指针分析：内存模型、别名、字段敏感 (Field Sensitive)和指向分析方法

9.可靠性 (Sound)、完备性 (Complete)、上近似 (Over-approximation)和下近似 (Under-approximation)

主要参考学习资料：

1. 弗莱明·尼尔森, 汉内·里斯·尼尔森, 克里斯·汉金. 程序分析原理. ISBN: 9787111706885. 机械工业出版社, 2022-08-01.

2. Alfred V. Aho, Monica S. Lam, Ravi Sethi, and Jeffrey D. UIIman. Compilers: Principles, Techniques, and Tools. ISBN: 9787111326748. 机械工业出版社, 2022-11-01.

其他参考资料：

1. John C. Mitchell. Concepts in Programming Languages. Cambridge University Press, 2004.

2. Flemming Nielson, Hanne Riis Nielson. Semantics with Applications: An Appetizer. Springer, 2007.

网络空间安全一级学科

考试科目 2：网络空间安全理论与技术

（一）考查知识内容或学术能力要点

考查内容包括 A、B 两个部分，每个部分提供三个内容选项，考生需从 A、B 两个部分中各选一个选项。

A：计算与网络技术基础（50 分）

A1 选项：计算理论（对应 《计算理论选讲》阚海斌）
A2 选项：网络技术（对应 《高级网络》吕智慧、赵进）
A3 选项：神经网络与深度学习（对应 《神经网络与深度学习》邱锡鹏）

B：网络与系统安全（50 分）

B1 选项：密码基础（对应 《密码学》赵运磊）
B2 选项：网络安全（对应 《计算机网络安全技术》吴承荣）
B3 选项：系统安全（对应 《系统安全》杨珉、杨哲慜）

对应核心课程：

CSEC60014《计算理论选讲》阚海斌
CS50007《高级网络》吕智慧、赵进
CS60010《神经网络与深度学习》邱锡鹏
CS50035《密码学》赵运磊
CSEC60005《计算机网络安全技术》吴承荣
CSEC60010《多媒体安全》钱振兴
CSEC50011《系统安全》杨珉、杨哲慜

（二）各选项考查要点及参考资料

A：计算与网络技术基础（50 分）

- **A1**：《计算理论》考查要点：

下述教材的第二、三、四章，具体包括：P、NP、NPC、强 NPC 的定义；6 个基本 NPC 问题的证明；能证明一些问题是 NPC 的，掌握一些归约技巧；证明一些强 NPC 问题。

参考学习资料：

英文版

Michael R. Garey, David S. Johnson,《Computers and Intractability, a guide to the theory of NP-completeness》, ISBN: 0-7167-1044-7, 1979

中文版

张立昂、沈泓,《计算机和难解性》(原著：Computers and Intractability， 作者：Michael R. Garey, David S. Johnson)，科学出版社，1987 年。

■ **A2**：《网络技术》考查要点：

1.计算机网络的定义、基本原理和体系结构：了解互联网的定义与组成、计算机网络的分类性能指标、网络体系结构的概念，熟悉主要的模型与层次划分（对应主要参考资料第 1 章）

2.网络核心协议 TCP/IP 的工作机制、拥塞控制：熟悉 IP 协议的基本原理、路由选择协议 RIP 和 OSPF 的工作机制；熟悉 TCP 的基本原理、流量控制的工作机制，掌握拥塞控制的算法，包括慢启动、拥塞避免、快速重传、快速恢复（对应主要参考资料章节 4.2、4.5、5.3、5.7、5.8）

3.网络多媒体传输及典型协议（RTP、SIP）：了解互联网多媒体的需求与分类，熟悉 RTP、SIP 协议的基本工作原理（对应主要参考资料章节 8.1、8.3）

4.互联网的服务质量（QoS）：了解服务质量的概念，掌握调度机制 FIFO、FQ、WFQ 的工作机制和特点（对应主要参考资料章节 8.4）

主要参考学习资料：

计算机网络（第 7 版） 作者:谢希仁 编著 出版社:电子工业出版社出版，2017 年 01 月

其他参考学习资料：

高级计算机网络（第 2 版） 作者：徐恪、徐明伟、李琦， 清华大学出版社，2021 年 03 月

■ **A3**：《神经网络与深度学习》考查要点：

1.了解机器学习的基本概念和基础知识

（1）《神经网络与深度学习》2.1-2.2 节

（2）《神经网络与深度学习》3.1-3.3 节

2.熟悉神经网络的主要模型（前馈网络、卷积网络、循环网络等）

（1）《神经网络与深度学习》4.1-4.3 节

（2）《神经网络与深度学习》5.1-5.2 节

（3）《神经网络与深度学习》6.1-6.2、6.5-6.6 节

3.了解神经网络的优化和正则化方法

《神经网络与深度学习》7.1-7.2、7.7 节

参考学习资料：

邱锡鹏，神经网络与深度学习，9787111649687，机械工业出版社，2020.4

B：网络与系统安全（50 分）

- **B1：**《密码基础》考查要点：

1.对称加密选择明文攻击安全（CPA）和选择密文攻击安全（CCA）安全定义；

2.伪随机数生成器（PRG）和伪随机函授（PRF）定义；

3.哈希函数抗碰撞安全定义、生日攻击；

4.离散对数假设、计算 Diffie-Hellman（CDH）假设、判定 Diffie-Hellman（DDH）假设定义；

5.El Gamal 公钥加密构造，及 CPA 安全证明；

6.Schnorr 数字签名构造，及安全证明。

主要参考学习资料：

书名：Introduction to modern cryptography 作者：Jonathan Katz， Yehuda Lindell 出版社：CRC Press，2021

其他参考学习资料：

书名：现代密码学 作者：杨波 出版社：清华大学出版社，2007

- **B2：**《网络与内容安全》考查要点：

1.主流的网络攻击方法

（1）网络嗅探：各类网络介质的嗅探方法与原理。

（2）网络扫描：端口扫描和漏洞扫描的作用、原理与主流工具。

（3）拒绝服务攻击：DOS 和 DDOS 的概念；SYN Flood、 smurf、Ping of Death、Echo－Chargen 等攻击的原理。

（4）DNS、地址假冒和劫持类攻击：DNS Spoofing、DNS Cache Poisoning、MAC spoofing、IP spoofing、Traffic Redirection、Session Hijack 等攻击的原理。

（5）主流 WEB 攻击：SQL 注入(SQL injection)、跨站脚本(Cross-Site Scripting)攻击原理。

（6）恶意代码（Malware）：病毒（Viruses）、木马（Trojan Horses）、蠕虫（Worms）的原理；rootkit 的含义与特点。

（7）针对全分布网络(Fully-Distributed Networks)的攻击：日蚀攻击(Eclipse)、女巫攻击（Sybil）的原理。

2.主流的网络防御方法

（1）网络加密：端到端（End-to-End Encryption）加密和链路加密（Link Encryption）的区别；IPSEC 协议（协议组成，传输模式和隧道模式含义；AH 和 ESP 区别与组合应用方法）；其他安全协议（SSH、SSL、HTTPS）；VPN 原理。

（2）防火墙：防火墙类型（包过滤，状态检测，应用代理等），防火墙部署模式（DMZ 含义），规则设定逻辑。

（3）入侵检测技术：Network-based IDS 和 Host-based IDS，Signature-based IDS 和 Heuristic IDS 技术的区别，Intrusion Protection System (IPS)的概念。

（4）无线网络安全技术：WEP (Wired Equivalent Privacy)的缺陷，以及 WPA (WiFi Protected Access)的安全机制，Extensible Authentication Protocol (EAP)协议。

（5）云时代的网络安全新技术：SAML、Oauth 和 OpenID 的原理；NFV（Network Functions Virtualization），Zero Trust Networking 等概念。

3.多媒体内容安全

（1）多媒体信息安全：隐写术、数字水印、图像内容篡改检测、感知哈希等技术的基本原理。

（2）AIGC 安全：深度伪造（Deepfake）检测、AI 生成内容检测等方法。

4. 人工智能安全

（1）神经网络模型安全：FGSM、PGD、CW 等对抗样本方法，样本投毒、训练阶段后门攻击方法，模型窃取、成员推理、模型反演等攻击方法。

（2）大模型安全：提示词注入、越狱攻击的基本原理，提示词泄露与窃取的攻击与防御方法，成员推理与数据提取的基于概念与方法，智能体安全的主要技术范畴。

主要参考学习资料：

Security in Computing (5th Edition)，Pfleeger C P ， Pfleeger S L ，Margulies J，ISBN:978-0-13-408504-3 或中文版《信息安全原理与技术（第五版）》李毅超等译，ISBN 9787121296635。（其中的 3.2，4.3，5.3，6，8.4）

Cybok（The Cyber Security Body of Knowledge）中的 Network Security Knowledge Area：https://www.cybok.org/wp-content/uploads/Network_Security_v2.0.0.pdf

《多媒体安全基础导论》钱振兴等，ISBN 9787309163605。（其中的 2.2，2.3，3.6，5，6）

《人工智能安全简明教程》，钱振兴等，ISBN978-7-309-18224-8。（其中的 3,4,5,7,8)

- B3：《系统安全》考查要点：

1.了解系统安全的基本原理，熟知经典安全攻击方法和防御技术。

2.基本掌握系统安全领域主要技术及其原理，包括逆向工程技术、程序分析技术、漏洞挖掘、利用和缓解技术、恶意软件检测、分析和溯源技术、隐私和数据安全技术、人工智能安全技能等

主要参考学习资料：

深入理解计算机系统，Computer Systems: A Programmer's Perspective (3rd Edition)，作者：Randal E. Bryant / David R. O'Hallaron

其他参考学习资料：

计算机安全：原理与实践，Computer Security: Principles and Practice，作者：William Stallings / Lawrie Brown