中六资讯及通讯科技练习卷：网络与数据传输、加密与网络安全、数据库与 SQL、算法与程式编写、系统开发与测试、科技伦理与可持续运算

中六　资讯及通讯科技　|　时限：75 分钟　|　总分：100 分　|　共 24 题

第一部分 网络与数据传输

甲部：每题 4 分，共 16 分。

1. 一个 480 MB 的档案经一条标称 100 Mbps 的连线传送，实际有效带宽只有标称值的 80%。求传送所需的时间（秒）。

答案：有效带宽 = 100 × 0.8 = 80 Mbps，即 80 ÷ 8 = 10 MB s⁻¹；时间 = 480 ÷ 10 = 48 s（以 bit 计：480 × 8 × 10^6 ÷ 80 × 10^6 = 48 s）。

2. 一幅 3000 × 2000 像素、每像素 24 位色的未压缩位图，求档案大小（MB）。若以无损方式压缩后体积减少 70%，求压缩后大小（MB）。

答案：像素数 = 3000 × 2000 = 6 000 000；总位元 = 6 000 000 × 24 = 144 000 000 bit；÷ 8 = 18 000 000 byte = 18.0 MB；压缩后 = 18.0 × 0.3 = 5.4 MB。

3. 一个 IPv4 网络使用 /26 前缀。求该子网可用主机数目、子网遮罩（点分十进制）及广播位址（以 192.168.10.64/26 为例）。

答案：主机位元 = 32 − 26 = 6，位址数 = 2^6 = 64，可用主机 = 64 − 2 = 62；遮罩 = 255.255.255.192；网段 192.168.10.64 – 127，广播位址 = 192.168.10.127。

4. 一个 60 MB 的档案经 50 Mbps 连线传送，连线来回时间（RTT）为 40 ms，需要两次来回才完成握手。假设忽略其他延误，求总传输时间（秒）。

答案：传输时间 = 60 × 8 ÷ 50 = 9.6 s；握手延误 = 2 × 0.04 = 0.08 s；总时间 = 9.6 + 0.08 = 9.68 s。

第二部分 加密与网络安全

乙部：每题 4 分，共 16 分。

5. 比较对称与非对称加密在密钥分发上的差别：10 名用户两两通讯，各需多少条密钥？并各举一项效能上的优缺点。

答案：对称加密每人共用一条密钥：10 × (10 − 1) ÷ 2 = 45 条；非对称每人一对公私钥：2 × 10 = 20 条。对称运算快但密钥分发困难（n 人需 n(n−1)/2 条）；非对称密钥分发容易但运算慢，故实务上用非对称交换会话密钥，再以对称加密传资料。

6. RSA 取质数 p = 61、q = 53，公开指数 e = 17。求 n、φ(n) 及私钥 d，并以明文 m = 65 验证加解密。

答案：n = 61 × 53 = 3233；φ(n) = 60 × 52 = 3120；由 $e \cdot d \equiv 1 \pmod{3120}$ 得 d = 2753（17 × 2753 = 46801 = 15 × 3120 + 1）。加密：c = 65^17 mod 3233 = 2790；解密：2790^2753 mod 3233 = 65，还原成功。

7. 某系统密码由大写、小写字母及数字组成（共 62 个字元），长度固定 8 位。求可能组合总数；若攻击者每秒可试 10 亿个组合，求平均破解时间（以日为单位，取一位小数）。

答案：组合数 = 62^8 = 2.183e+14 ≈ 2.18 × 10^{14} ；全部试完需 218,340 s；平均（一半）= 1.3 日。故须加长度、加盐及限制尝试次数。

8. 某公司有 500 名员工，钓鱼测试中 3% 的人点击了假连结。计算点击人数，并说明防火墙与员工培训在防御上分别针对哪些风险。

答案：点击人数 = 500 × 3% = 15 人。防火墙过滤未经授权的埠与流量，阻挡外部扫描与部分恶意连线；但钓鱼邮件多用正常埠（80/443），故须靠培训、邮件过滤与多重认证，并以“四眼原则”处理汇款要求。

第三部分 数据库与 SQL

丙部：每题 4 分，共 16 分。

9. 解释主键、外键与正规化的作用，并说明为何未正规化的表会产生更新异常。

答案：主键唯一识别每笔记录且不可为空；外键参照另一表的主键以维持参照完整性；正规化（1NF→2NF→3NF）消除重复组与部分 / 传递相依。未正规化时同一事实重复储存，改一处漏改另一处即造成更新异常，删除一笔又可能连带丢失其他资料。

10. 资料表 Marks 有 5 笔分数：72、58、91、45、84。写出求平均分的 SQL，并算出结果。

答案：SELECT AVG(score) AS avg_score FROM Marks; 合计 = 350，平均 = 350 ÷ 5 = 70.0。若要四舍五入至整数可用 ROUND(AVG(score), 0)，并可用 WHERE 加条件筛选。

11. 现有 Student(student_id, name) 与 Enrol(student_id, class_code)。写出 SQL 列出每班学生人数，只显示多于 20 人的班别，并按人数由多至少排序。

答案：SELECT class_code, COUNT(*) AS n FROM Enrol GROUP BY class_code HAVING COUNT(*) > 20 ORDER BY n DESC; 要点：JOIN 只为取姓名，计人数用 Enrol 已足够；筛选聚合结果用 HAVING，不可用 WHERE；ORDER BY 放最后。

12. 一张有 1,000,000 笔记录的表，全表扫描每笔比较约 10 微秒；用 B-tree 索引只需 20 次节点读取，每次 5 毫秒。求两者平均查询时间及速度比。

答案：全表扫描平均扫 500,000 笔：500,000 × 10 μs = 5.0 s；索引：20 × 5 ms = 100 ms = 0.1 s；速度比 = 5.0 ÷ 0.1 = 50 倍。但索引会增加写入成本与储存空间，且对低选择性字段效益有限。

第四部分 算法与程式编写

丁部：每题 4 分，共 16 分。

13. 在 1,000,000 个已排序项目中，线性搜寻平均比较多少次？二分搜寻最多比较多少次？求两者之比。

答案：线性搜寻平均 500,000 次；二分搜寻最多 $\lceil \log_2 1{,}000{,}000 \rceil$ = 20 次；比 = 500,000 ÷ 20 = 25,000 倍。二分搜寻要求资料已排序，插入新资料需维持排序。

14. 气泡排序对 12 个项目作最坏情况（完全逆序）排序，共需多少次比较？若每次比较与交换合计 1 微秒，求所需时间。
答案：比较次数 = $n(n-1)/2 = 12 \times 11 \div 2 = 66$ 次；时间 $\approx 66\ \mu s = 0.066$ ms。时间复杂度 $O(n^2)$，资料量倍增时比较次数约增四倍，故大数据应用改用 $O(n \log n)$ 的排序。

15. 以递回定义计算 fib(10) 的朴素算法共会被呼叫多少次？并说明为何改用备忘录法可大幅减少。
答案：fib(10) 的呼叫次数（含本身）= 177 次，因为同一个 fib(k) 被重复计算多次，时间复杂度约 $O(1.6^n)$。备忘录法把已算结果存入阵列或字典，每个 k 只算一次，复杂度降为 O(n)，fib(10) 只需约 10 次计算加查表。

16. 比较 O(1)、O(log n)、O(n)、O(n log n)、O(n²) 在 n = 1024 时的运算次数，并指出哪一种最不适合处理大型输入。
答案：$O(1) = 1$；$O(\log n) = 10$；$O(n) = 1{,}024$；$O(n \log n) = 10{,}240$；$O(n^2) = 1{,}048{,}576$。$O(n^2)$ 最不适合：n 增至 10 倍时运算量增 100 倍，实际会超时；故选算法先看增长的阶，再看常数与内存。

第五部分 系统开发与测试

戊部：每题 4 分，共 16 分。

17. 列出系统开发生命周期（SDLC）的主要阶段，并说明“需求分析”做得不好会如何影响后期成本。
答案：阶段：可行性研究→需求分析→系统设计→编码实作→测试→推行转换→维护检讨。需求阶段的错误在设计、编码、测试各阶段被放大，越后期才发现，修改要重做设计与测试，成本最高；故须与用户确认需求并以原型验证。

18. 某判断逻辑有 3 个互相独立的条件。以白盒测试的“条件组合覆盖”计，最少需要多少个测试案例？并说明黑盒测试与白盒测试的分别。
答案：每个条件有真 / 假两种，组合数 = 2^3 = 8 个案例。白盒测试看程式内部结构与路径，由开发者设计；黑盒测试只看输入与输出是否符合规格，由测试者或用户按需求设计，两者互补。

19. 比较瀑布模型与敏捷开发，并说明在需求经常改变的项目中为何多用敏捷。
答案：瀑布模型按阶段顺序推进，每阶段完成才进下一阶段，文件齐全但难回头，适合需求稳定的项目；敏捷以短迭代交付可用版本，每个冲刺后检视与调整，客户持续参与，故需求常变时能及早修正方向，风险分散但要求团队自律与持续沟通。

20. 说明用户验收测试（UAT）的目的与做法，并解释版本控制（如 Git）在团队开发中的作用。
答案：UAT 由实际用户按业务情境执行，确认系统符合需求才可上线；做法包括以真实资料跑主要流程、记录缺陷并签署验收。版本控制保存每次修改与作者，可分支平行开发、合并变更、必要时回退，避免档案互相覆盖，并留下可追溯的修改纪录。

第六部分 科技伦理与可持续运算

己部：每题 5 分，共 20 分。

21. 比较自由及开放源码软件（FOSS）与专有软件的授权、成本与风险，并各举一个适用情境。
答案：FOSS（如 GPL、MIT）可自由使用、修改及再发布，无授权费，源码可审计，但需自负支援与维护；专有软件收取授权费、封闭源码，供应商负责支援与更新，但易受厂商锁定。学校教学平台可用 FOSS 降低成本，金融核心系统多选专有软件以取得合约保障。

22. 列举《个人资料（隐私）条例》六项保障资料原则中的四项，并说明学校应如何处理学生资料。

答案：六项原则：①收集目的及方式合法相关而不过度；②准确及保留不超过所需时间；③使用限于原定目的（除非同意）；④保安措施；⑤政策公开；⑥查阅与改正权利。学校应只收集教学所需资料、加密储存、限制存取、订明保留期，并向家长说明用途与查阅途径。

23. 说明以大数据或机器学习作决策时，偏见可能从何而来，并提出两项减低风险的措施。

答案：偏见源头：①训练资料本身有历史歧视或取样偏差；②特征选择把受保护属性（性别、族裔）间接编码；③标签由人决定而带主观；④模型在黑盒下难以解释，错误难察觉。措施：审核资料分布与代表性、以不同群组分别评估准确率与误判率、保留人工复核与申诉机制、公开模型卡与决策依据。

24. 某数据中心的 IT 设备耗电 400 kW，总耗电 500 kW。求 PUE；若全年不停运作（8 760 小时）、每度电排放 0.6 kg 二氧化碳，求年排放量（公吨）。并提出一项降低 PUE 的方法。

答案：PUE = 500 ÷ 400 = 1.25；年用电 = 500 × 8 760 = 4,380,000 kWh；排放 = 4,380,000 × 0.6 = 2,628,000 kg = 2,628 公吨。降 PUE：改用自然冷却（如冷通道封闭、提高送风温度）、余热回收或虚拟化提高使用率。

TutorZone 中六资讯及通讯科技练习卷｜题目与文章为原创，并非任何学校或出版社的教材。