中六资讯及通讯科技练习卷（第二份）：数据结构与程式追踪、IPv4 子网划分与传输时间、关联数据库与 SQL、多媒体档案大小与压缩、RSA 与数码签署、系统开发与关键路径（100 分）

练习卷 · 资讯及通讯科技 · 中六

中六资讯及通讯科技练习卷（第二份）：6 题 24 部分共 100 分、时限 75 分钟，涵盖堆叠与伫列追踪、后置式求值、IPv4 子网划分与传输时间、关联数据库正规化与 SQL 查询、图像与音讯档案大小及压缩、RSA 加解密与数码签署、系统开发生命周期与关键路径分析，全部附完整答案。

第 1 题 – 数据结构与程式追踪（16 分）

某程式以 Python 清单实作堆叠（list，只用 append 与 pop），并以 collections.deque 实作伫列（enqueue 用 append、dequeue 用 popleft）。堆叠初始为空；伫列初始有 5 个元素 A、B、C、D、E（A 在队首）。

#	Question	Answer and marking notes
1	依序执行 push(3)、push(7)、push(5)、pop()、push(1)、pop()，写出最终堆叠由顶至底的内容。	push 3 → [3]；push 7 → [3, 7]；push 5 → [3, 7, 5]；pop() 移除 5；push 1 → [3, 7, 1]；pop() 移除 1。最终堆叠由顶至底为 7、3。
2	求值后置式（postfix）算式 6 2 3 * – 4 2 / +，并写出每一步的中间结果。	读入 6、2、3；遇到 * 得 2 × 3 = 6，堆叠为 [6, 6]；遇到 – 得 6 – 6 = 0；读入 4、2；遇到 / 得 4 ÷ 2 = 2；遇到 + 得 0 + 2 = 2。答案为 2。
3	伫列先 dequeue 两次，再 enqueue F、G、H。写出最终伫列长度、队首与队尾元素。	dequeue 两次移除 A、B，余 [C, D, E]；enqueue F、G、H 后为 [C, D, E, F, G, H]，长度 6，队首 C，队尾 H。
4	在单向链表的头部插入一个新节点需要改动多少个指针？在已排序的 1,024 个元素阵列中以二分搜寻找一个值，最多比较多少次？并比较两者的时间复杂度。	头部插入只需 2 个指针改动（新节点的 next 指向原头节点、head 指向新节点），时间复杂度 O(1)。二分搜寻每次把搜寻范围减半，最多 log2 1024 = 10 次比较，时间复杂度 O(log n)。

第 2 题 – IPv4 子网划分与传输时间（18 分）

某学校获分配网络 192.168.10.0/24，管理员要把它平均划分为 4 个子网，其中一个子网使用 192.168.10.64/26。另外，一个 12 MB 的档案要经 100 Mbps 的线路传送，协定开销占带宽 8%（1 MB = 10^6 字节）。

#	Question	Answer and marking notes
5	写出 /26 的点分十进制子网遮罩，并计算每个子网可用的主机数目。	主机位元 = 32 − 26 = 6；遮罩 = 255.255.255.192（11111111.11111111.11111111.11000000）；可用主机 = 2^6 − 2 = 62。
6	把 /24 分为 4 个子网需要借多少位元？写出 192.168.10.64/26 的网络地址、广播地址及可用主机范围。	需要借 2 位元（2^2 = 4 个子网）。网络地址 192.168.10.64；区块大小 64，广播地址 192.168.10.127；可用主机范围 192.168.10.65 至 192.168.10.126。
7	计算在上述线路上传送该 12 MB 档案所需的时间（秒，四位小数）。	档案 = 12 × 8 × 10^6 = 96,000,000 位元；有效带宽 = 100 × 0.92 = 92 Mbps；时间 = 96,000,000 ÷ 92,000,000 = 1.0435 秒。

#	Question	Answer and marking notes
8	直播影片串流应选用 TCP 还是 UDP？指出一个理由及一个相应的风险。	应选用 UDP：不等待重传，延迟较低，适合直播的即时性。风险是封包遗失时不会重传，画面可能出现破格或短暂停顿。

第 3 题 – 关联数据库与 SQL（16 分）

补习社的数据库有三个关联表：Student(SID, SName, Class) 共 6 个学生、Course(CID, CTitle, Teacher) 共 3 个课程、Enrol(SID, CID, Score) 共 9 笔选课记录。学生 S06 未选任何课程；班别分布为 4A 三人、4B 两人、5A 一人。

#	Question	Answer and marking notes
9	指出三个关联表的主键，以及 Enrol 表中的外键。	Student 的主键是 SID；Course 的主键是 CID；Enrol 的主键是复合键 (SID, CID)；Enrol 的外键是 SID（引用 Student）与 CID（引用 Course）。
10	写出 SQL 语句列出每班人数并按班别排序，并写出查询结果。	SELECT Class, COUNT(*) FROM Student GROUP BY Class ORDER BY Class; 结果为 4A 3、4B 2、5A 1 三行。
11	若把 Student 与 Enrol 合并成一个表 EnrolAll(SID, SName, CID, CTitle, Score)，说明它违反第二正规化（2NF）的原因，并写出分解后的表结构。	主键为 (SID, CID)，但 SName 只依赖 SID、CTitle 只依赖 CID，属部分相依，违反 2NF。分解为 Student(SID, SName)、Course(CID, CTitle) 及 Enrol(SID, CID, Score)。
12	一个 INNER JOIN 查询 Student 与 Enrol，会返回多少行？改用 LEFT JOIN（以 Student 为左表）又会返回多少行？并解释差异。	INNER JOIN 只配对有选课的记录，S06 被排除，返回 9 行；LEFT JOIN 保留左表全部 6 个学生，S06 的 CID 与 Score 显示 NULL，返回 10 行。

第 4 题 – 多媒体档案大小与压缩（16 分）

一张 1024 × 768 像素、色彩深度 24 位元的位图像；一段 44.1 kHz 取样率、16 位元、立体声、长 60 秒的未压缩音讯（1 MiB = 1,048,576 字节）。

#	Question	Answer and marking notes
13	计算该图像未压缩时的档案大小（字节及 MiB）。	每像素 24 ÷ 8 = 3 字节；总计 1024 × 768 × 3 = 2,359,296 字节；2,359,296 ÷ 1,048,576 = 2.25 MiB。
14	若用无损压缩把档案缩小至八分之一，写出压缩后的大小（字节及 KiB），并说明为何位图像难以达到这个压缩率。	2,359,296 ÷ 8 = 294,912 字节 = 288 KiB。位图像每个像素独立储存，相邻像素颜色差异大时重复模式少，无损压缩可压缩的冗余有限，一般只有二至三倍。
15	计算该段音讯未压缩时的大小（字节及 MiB，三位小数）。	每秒字节 = 44,100 × 2 × 2 = 176,400；60 秒 = 10,584,000 字节；10,584,000 ÷ 1,048,576 = 10.094 MiB。
16	比较有损与无损压缩，并指出数码相机照片与医疗扫描影像分别应采用哪一种。	有损压缩永久舍弃部分数据以换取高压缩率，不能还原原档；无损压缩可完全还原，但压缩率较低。数码相机照片可用有损压缩（如 JPEG）；医疗扫描须用无损压缩，以免影响诊断。

第 5 题 – RSA 与数码签署（18 分）

某系统用 RSA 加密，取质数 $p = 5$、$q = 11$，公开指数 $e = 3$。要传送的明文为 $m = 7$。系统同时用数码签署保护重要档案。

#	Question	Answer and marking notes
17	计算模数 n、欧拉函数 φ(n) 及私钥指数 d。	$n = p \times q = 5 \times 11 = 55$；$\varphi(n) = (p-1)(q-1) = 4 \times 10 = 40$；d 满足 $e \times d \equiv 1 \pmod{40}$，$3 \times 27 = 81 = 2 \times 40 + 1$，故 $d = 27$。
18	用公开钥匙把明文加密成密文，再用私钥解密验证结果。	密文 $c = 7^3 \bmod 55 = 343 \bmod 55 = 13$；解密 $13^{27} \bmod 55 = 7$，还原明文正确。
19	TLS 为何同时使用对称与非对称加密？说明两者在连线中的分工。	非对称加密解决密钥分发问题：客户端用服务器的公开钥匙加密一把随机的对称密钥（会话密钥）。对称加密运算快，之后大量资料都用会话密钥加密，兼顾安全与效能。
20	说明数码签署的签署与验证过程，并指出杂凑（hash）在其中的作用。	发送者先对讯息计算杂凑值，再用自己的私钥签署该杂凑值；接收者用发送者的公开钥匙验证签署，并自行重算杂凑值比对。杂凑把任意长度讯息压成固定长度摘要，可侦测内容被篡改且签署更快。

第 6 题 – 系统开发与关键路径（16 分）

一个报名系统的开发活动如下：A（3 天）与 B（4 天）可立即开始；C（5 天）须待 A 完成；D（2 天）须待 B 完成；E（4 天）须待 C 与 D 均完成；F（3 天）须待 E 完成。专案以小组形式进行，并需要使用者验收。

#	Question	Answer and marking notes
21	按正确次序排列系统开发生命周期（SDLC）的五个主要阶段，并指出哪个阶段成本最高。	需求分析 → 系统设计 → 实作（编码）→ 测试 → 推行与维护；一般以推行与维护阶段成本最高，因为占整个系统生命周期最长时间。
22	计算专案的关键路径、总工期，以及活动 D 的浮时（slack）。	A–C–E–F = 3 + 5 + 4 + 3 = 15 天；B–D–E–F = 4 + 2 + 4 + 3 = 13 天。关键路径为 A–C–E–F，总工期 15 天；D 最早第 4 天开始、E 最早第 8 天开始，D 需 2 天，故浮时 = 8 − (4 + 2) = 2 天。
23	若登入功能在个别模组测试时全部通过，但与数据库连接后失败，应进行哪一类测试？并指出单元测试与使用者验收测试分别由谁负责。	应进行整合测试，检查模组之间的界面与资料传递。单元测试由程式员负责；使用者验收测试由使用者（或客户）负责，确认系统符合业务需求。
24	写出一个“网上报名”用例图中的两个主要参与者（actor），并说明为何要在设计阶段画出资料流程图（DFD）。	主要参与者：学生（报名者）与管理员（审核课程与名额）。资料流程图显示资料在系统内的来源、处理过程、储存位置与输出，协助在编码前发现流程缺漏与资料重复。