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
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。
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。
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。
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。

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
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。
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。
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）。
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。

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
9	指出三个关联表的主键，以及 Enrol 表中的外键。
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。
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。

#	Question
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。

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
13	计算该图像未压缩时的档案大小（字节及 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。
15	计算该段音讯未压缩时的大小（字节及 MiB，三位小数）。
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。

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
17	计算模数 n、欧拉函数 $\varphi(n)$ 及私钥指数 d。
18	用公开钥匙把明文加密成密文，再用私钥解密验证结果。
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。
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。

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
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。
22	计算专案的关键路径、总工期，以及活动 D 的浮时（slack）。
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。
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）。