中五资讯及通讯科技练习卷（第四份）：关联数据库与 SQL 查询、IPv4 子网划分、Python 程式追踪、排序与搜寻算法复杂度、图像与影片档案大小及压缩、资讯保安（100 分）

中五资讯及通讯科技 | 100 分 | 75 分鐘

第 1 题 — 关联数据库与 SQL（17 分）

下表为学校数据库的两个关联表。Scores(student_id, name, class, score)；Clubs(student_id, club, joined_year)。所有部分须以 SQL 作答。

写出显示 5A 班首三名学生姓名及分数的 SQL 语句（分数由高至低）。 *(4 分)*

答案：SELECT name, score FROM Scores WHERE class = '5A' ORDER BY score DESC LIMIT 3;

写出列出每位学生姓名及其平均分（只显示平均分不低于 60 的学生）的 SQL 语句。 *(4 分)*

答案：SELECT name, AVG(score) FROM Scores GROUP BY student_id, name HAVING AVG(score) >= 60;

Scores 表有 2,000 笔记录，每笔 320 bytes，资料页大小 4,096 bytes。求整表占用多少 bytes，以及至少需要多少个资料页（须显示算式）。 *(4 分)*

答案：总大小 = 2,000 × 320 = 640,000 bytes；页数 = 640,000 ÷ 4,096 = 156.25，故最少需 157 页。

Clubs 表原本把学生姓名、班别与所属学会全部存在同一表内，出现资料重复与更新异常。简述把该表拆成两张关联表的正规化做法及其一项好处。 *(5 分)*

答案：把学生个人资料（student_id、name、class）存于 Students 表，Clubs 表只保留 student_id、club、joined_year，以 student_id 作外键连结；好处是姓名或班别只需更新一次，避免资料重复及更新异常。

第 2 题 — IPv4 子网划分（17 分）

某学校获分配网络 192.168.10.0/24，需划分为 4 个大小相同的子网，供四个部门各自独立使用。

写出新子网前缀长度及子网遮罩（以点分十进制表示）。 *(4 分)*

答案：前缀 /26；子网遮罩 255.255.255.192。

求每个子网的地址总数及可用主机数目（须显示算式）。 *(4 分)*

答案：主机位 = 32 − 26 = 6，地址总数 = 2^6 = 64，可用主机 = 64 − 2 = 62 个。

写出第三个子网的网络地址、首个及最后一个可用主机地址，以及广播地址。 *(5 分)*

答案：网络地址 192.168.10.128；首个可用 192.168.10.129；最后可用 192.168.10.190；广播地址 192.168.10.191。

若日后其中一个部门只需 20 部主机，改为借用主机位再划分是否可行？指出一个考虑因素。 *(4 分)*

答案：可行：再借 1 位可得 /27，每子网 30 个可用主机，足够 20 部主机；但要考虑会浪费地址并增加路由与管理复杂度。

第 3 题 — Python 程式追踪（16 分）

细阅以下程式码，然后回答各部分的输出。 `nums = [2, 5, 8, 11, 13] acc = {} for n in nums: acc[n % 3] = acc.get(n % 3, 0) + n print(acc) print(sum(nums))`

写出 print(acc) 的输出。 *(4 分)*

答案：{2: 26, 1: 13}

写出 print(sum(nums)) 的输出。 *(4 分)*

答案：39

解释 acc.get(n % 3, 0) 中第二个参数 0 的作用。 *(4 分)*

答案：当字典中没有键 n % 3 时返回预设值 0，令首次出现的键可以由 0 开始累加，避免 KeyError。

若把 nums 改为 [1, 4, 7]，写出新的 print(acc) 输出。 *(4 分)*

答案：{1: 12}

第 4 题 — 排序与搜寻的比较次数（17 分）

一个已排序的整数阵列有 1,024 个元素。所有答案须显示算式。

用气泡排序处理 6 个元素，最坏情况需要多少次比较？写出公式。 *(5 分)*

答案：公式 $n(n-1) \div 2 = 6 \times 5 \div 2 = 15$ 次比较。

用二分搜寻在 1,024 个元素中找目标值，最坏情况最多比较多少次？并解释。 *(4 分)*

答案：最多 10 次，因为每次把搜寻范围减半，2^10 = 1,024。

若改用线性搜寻，最坏情况需要多少次比较？与二分搜寻相差多少倍？ *(4 分)*

答案：最坏 1,024 次比较；$1{,}024 \div 10 = 102.4$ 倍。

合并排序处理 1,024 个元素约需 $1{,}024 \times \log_2(1{,}024)$ 次比较。计算该次数，并指出其时间复杂度比气泡排序优胜之处。 *(4 分)*

答案：$1{,}024 \times 10 = 10{,}240$ 次比较；合并排序为 $O(n \log n)$，气泡排序为 $O(n^2)$，元素增多时合并排序增长慢得多。

第 5 题 — 图像、影片档案大小与压缩（16 分）

一张 24-bit RGB 图像的分辨率为 1920 × 1080。一段影片以每秒 30 格拍摄，每格 1.0 MB，片长 90 秒，经 100 Mbps 网络传送。

求该图像未压缩的档案大小（以 bytes 及 MiB 表示，MiB 取二位小数）。 *(4 分)*

答案：$1920 \times 1080 \times 24 \div 8 = 6{,}220{,}800$ bytes = 5.93 MiB。

若无损以外的压缩令档案只剩原来的 40%，求压缩后大小（bytes 及 MiB）。 *(4 分)*

答案：$6{,}220{,}800 \times 40\% = 2{,}488{,}320$ bytes = 2.37 MiB。

求该段影片的总大小（以 MB 表示）。 *(4 分)*

答案：$30 \times 1.0 \times 90 = 2{,}700$ MB。

以 100 Mbps 传送该影片，求所需时间（以秒及分秒表示）。 *(4 分)*

答案：$2{,}700 \times 8 = 21{,}600$ Mb；$21{,}600 \div 100 = 216$ 秒 = 3 分 36 秒。

第 6 题 — 密码空间与资讯保安（17 分）

某系统要求 8 位字元密码，字元只可选小写英文字母。假设攻击者每秒可尝试 1,000,000 次。

求只用 26 个小写字母时的可能密码总数。 *(4 分)*

答案：26^8 = 208,827,064,576 个。

若同时可用 10 个数字，写出新的密码总数（可保留指数式）。*(4 分)*

答案：36^8 = 2,821,109,907,456 个。

以每秒 1,000,000 次计算，穷举 26^8 个密码约需多少日（取二位小数）？ *(4 分)*

答案：208,827,064,576 ÷ 1,000,000 = 208,827.06 秒；÷ 86,400 ≈ 2.42 日。

系统储存密码时应使用杂凑而非对称加密，并在服务器端加盐。解释两个做法各自的保安作用。 *(5 分)*

答案：杂凑是不可逆单向函数，数据库外泄亦难还原原密码；加盐令相同密码产生不同杂凑值，可防止彩虹表及批量比对攻击。
