中五资讯及通讯科技练习卷（第四份）｜子网划分、TCP/IP、正规化、复杂度、压缩、资讯保安

练习卷 · 高中资讯及通讯科技

中五资讯及通讯科技练习卷第四份，涵盖 IPv4 子网划分与可用主机数、TCP/IP 四层模型与 TCP / UDP 比较、MTU 与 MSS、数据库 1NF 至 3NF 正规化与 SQL 查询、线性与二分搜寻及排序算法复杂度、档案大小、RLE 压缩率、对称与非对称加密、网络钓鱼与个人资料隐私条例，全部附完整步骤及答案。

1. IPv4 子网划分与可用主机数（18 分）

可用主机数目 = $2^n - 2$（n 为主机位元，扣除网络位址与广播位址）。

#	Question	Answer and marking notes
1	(a) 网络 192.168.10.0/26：求每个子网的位址数目、可用主机数目，以及由 192.168.10.0/24 可划出多少个 /26 子网。	主机位元 = 32 − 26 = 6，位址数目 = 2^6 = 64；可用主机 = 64 − 2 = 62。由 /24 划出 2^(26−24) = 4 个 /26 子网。
2	(b) 网络 10.0.0.0/22：求子网遮罩、位址数目及可用主机数目。	遮罩 = 255.255.252.0（22 个 1 后接 10 个 0）。主机位元 = 10，位址数目 = 2^{10} = 1024，可用主机 = 1024 − 2 = 1022。
3	(c) 主机位址 172.16.5.130/27：求网络位址、广播位址及可用主机范围。	区块大小 = 2^(32−27) = 32。130 ÷ 32 = 4 余 2，故网络位址 = 172.16.5.128，广播位址 = 172.16.5.159，可用范围 172.16.5.129 至 172.16.5.158。
4	(d) 由 192.168.1.0/24 划分，需要至少 5 个子网、每个子网至少 25 部主机，求最合适的前置长度并说明理由。	25 部主机需 5 个主机位元（2^5 − 2 = 30 ⩾ 25）；用 /28 只有 2^4 − 2 = 14 部，不足。故前置长度 = 32 − 5 = /27（255.255.255.224），可划出 2^3 = 8 个子网，满足至少 5 个的要求。

2. TCP/IP 分层与协定（16 分）

答案须写出层名及协定名称。

#	Question	Answer and marking notes
5	(a) 列出 TCP/IP 模型四层，每层举一个协定。	应用层（HTTP、DNS、SMTP）、传输层（TCP、UDP）、互联网层（IP、ICMP）、网络存取层（Ethernet、IEEE 802.11）。
6	(b) 比较 TCP 与 UDP 的四项差异（连接方式、可靠性、开销、典型用途）。	TCP 为连接导向、可靠（确认、重传、按序交付）、标头较大开销高，用于网页与档案传输；UDP 无连接、不保证送达、标头小开销低、延迟低，用于语音、直播及 DNS 查询。
7	(c) 某段网络 MTU 为 1500 bytes，IP 标头 20 bytes、TCP 标头 20 bytes，求 MSS 及有效负载占整个讯框的百分比。	MSS = 1500 − 20 − 20 = 1460 bytes；占比 = 1460 ÷ 1500 × 100% = 97.33%。
8	(d) 简述 TCP 三次握手的三个步骤及其作用。	客户端送 SYN（含初始序号）→ 服务器回 SYN–ACK（确认并送自己的序号）→ 客户端回 ACK。作用是双方确认收发能力、同步初始序号，建立可靠连线后才传资料。

3. 数据库正规化与 SQL 查询（18 分）

SQL 答案须用标准语法；正规化须指出相依关系。

#	Question	Answer and marking notes
9	(a) 分别说明第一（1NF）、第二（2NF）、第三（3NF）正规化的要求。	1NF：每格只存单一原子值，无重复群组；2NF：符合 1NF，且非主键字段完全依赖整个主键（消除部分相依）；3NF：符合 2NF，且非主键字段之间无相依（消除递移相依）。
10	(b) 表 Enrol(student_id, student_name, class_code, class_teacher)：指出两项相依问题，并拆成 3NF 的表结构。	student_name 只依赖 student_id（部分相依，若主键为 student_id 加 class_code）；class_teacher 只依赖 class_code（递移相依）。拆为 Student(student_id, student_name, class_code)、Class(class_code, class_teacher)、Enrol(student_id, class_code)。
11	(c) 写出 SQL：列出平均分高于 70 分的班别及其平均分。	SELECT class_code, AVG(score) AS avg_score FROM Enrol GROUP BY class_code HAVING AVG(score) > 70;（查核样本资料下只有 A1，平均 80.33 分。）
12	(d) 写出 SQL：列出每位学生姓名及其班别老师姓名（两表连接）。	SELECT s.name, c.teacher FROM Student s JOIN Class c ON s.class_code = c.class_code;（查核样本资料回 5 行。）

4. 算法复杂度与排序比较（16 分）

须写出所用的计算式。

#	Question	Answer and marking notes
13	(a) 在一万零二十四个元素的已排序阵列中，线性搜寻与二分搜寻的最坏情况比较次数各为多少？（元素数目取 1,048,576）	线性搜寻最坏 = n = 1048576 次；二分搜寻最坏 = $\lceil \log_2 n \rceil = \lceil \log_2 \ 1048576 \rceil = 20$ 次。
14	(b) 对 1024 个元素，泡沫排序最坏比较次数为 $n(n-1)/2$，合并排序约为 $n \log_2 \ n$，分别计算并比较。	泡沫排序 = $1024 \times 1023 \div 2 = 523776$ 次；合并排序 $\approx 1024 \times 10 = 10240$ 次。两者相差约 51 倍，元素越多差距越大。
15	(c) 阵列 [42, 17, 68, 9, 55, 23, 71, 34]，以最后元素为基准做一次 Lomuto 分割，写出分割后的阵列及基准所在索引。	基准 = 34。由左至右把小于或等于 34 的元素换到前面，最后把基准交换到分界位置：结果 = [17, 9, 23, 34, 55, 68, 71, 42]，基准在索引 3，左边全部 $\leqslant$ 34、右边全部 > 34。
16	(d) 把 $O(n^2)$、$O(n \log n)$、$O(\log n)$、$O(1)$ 由增长最慢排到最快，并各举一例。	$O(1)$（阵列按下标取值）< $O(\log n)$（二分搜寻）< $O(n \log n)$（合并排序）< $O(n^2)$（泡沫排序）。n 越大，高阶项主导实际执行时间。

5. 数码档案大小与压缩（16 分）

1 MiB = 1,048,576 bytes；1 MB = 1,000,000 bytes。

#	Question	Answer and marking notes
17	(a) 一幅 1920 × 1080、24 位元色深的未压缩位图，求档案大小（MiB 及 MB）。	每像素 24 bits = 3 bytes；总量 = $1920 \times 1080 \times 3 = 6220800$ bytes = 5.93 MiB $\approx$ 6.22 MB。

#	Question	Answer and marking notes
18	(b) 一段 44.1 kHz、16 位元、立体声、长 3 分钟的未压缩 WAV，求档案大小。	每秒 = 44100 × 2 bytes × 2 声道 = 176400 bytes；3 分钟 = 180 秒；总量 = 31752000 bytes = 30.28 MiB ≈ 31.75 MB。
19	(c) 一行索引色像素为 WWWWBBBBWWWWWBBB（每像素 1 byte），用（颜色, 次数）每组 2 bytes 的行程编码（RLE），求压缩后大小及压缩比。	行程 = (W,4)(B,4)(W,6)(B,3)，共 4 组 × 2 bytes = 8 bytes；原本 17 bytes，压缩比 = 17 ÷ 8 = 2.125。颜色越集中，RLE 越有效。
20	(d) 比较有损与无损压缩，各举一例并说明适用情况。	无损压缩解压后与原档完全相同（PNG、ZIP、FLAC），适合文字、程式码、医疗影像；有损压缩舍弃部分资料换取更高压缩率（JPEG、MP3、H.264），适合相片、音乐、影片，但要避免反复压缩累积失真。

6. 资讯保安与相关法规（16 分）

答案须指出技术名称及作用。

#	Question	Answer and marking notes
21	(a) 比较对称与非对称加密，各举一种算法及一项用途。	对称加密用同一条金钥加解密（AES），速度快，适合大量资料如磁盘与 HTTPS 会话资料；非对称加密用公钥加密、私钥解密（RSA），适合金钥交换与数码签署，但运算较慢。
22	(b) 说明数码签署如何同时提供完整性与不可否认性。	寄件人先对讯息计杂凑（SHA-256），再用自己的私钥签署该杂凑值；收件人用寄件人公钥验签并重算杂凑，两者相同即证明内容未被篡改（完整性），而只有私钥持有人能产生该签署（不可否认性）。
23	(c) 列举三种常见网络攻击手法，并各写一项对应防御措施。	钓鱼电邮（防御：核对寄件网域、启用多重认证）；暴力破解密码（防御：长密码加账户锁定与 MFA）；中间人攻击（防御：强制 HTTPS 并验证凭证）。
24	(d) 就香港《个人资料（隐私）条例》（第 486 章）六项保障资料原则，说明与机构收集及使用顾客资料最相关的两项，并各举一例。	第 1 原则（收集目的及方式）：须为合法目的、与目的直接有关、足够但不超乎适度，并告知用途；例：试堂登记只收集姓名与电话。第 3 原则（使用）：除获资料当事人同意或法律准许，资料只可用于收集时所述目的；例：未经同意不得把名单转交第三方推销。