Solutions

Marking: **M1** a correct method, **A1** the correct answer, **B1** an independent mark.

Each answer shows the steps, then the **result**.

2.1

the SQL becomes `WHERE user = 'admin' --' AND pw = ...`

`--` starts a comment, so the password check is removed and the attacker logs in as admin

use a parameterised query: `WHERE user = ? AND pw_hash = ?`

2.2

```
CREATE VIEW office_view AS SELECT name, cid FROM ...;

GRANT SELECT ON office_view TO office;
```

2.3

$26^8 \approx 2.09 \times 10^{11}$ passwords

SHA-256: about **21 s**

bcrypt: 2.09×10^7 s, about **240 days**

2.4

pseudonymised: names are replaced by codes, but a key can link them back, so it is still personal data

anonymised: no one can identify the people any more

3.1

(a) every (age, postcode) pair is different, so $k = \mathbf{1}$

(b) join it with another list holding names, ages and postcodes, such as a club list; each match gives a name with a diagnosis

(c) age as 20–29 or 40–49; postcode as `3150**` or `3152**`: two groups of 3, so $k = 3$

(d) the diagnosis of everyone in that group, without knowing which row is theirs (homogeneity); this is why l-diversity is also needed

3.2

(a) 3 copies, on 2 kinds of media, 1 off site; here there are 2 copies in one room, so a fire or ransomware can destroy both

(b) up to 24 hours of changes; archiving the write-ahead log every few minutes allows recovery to within minutes

(c) a backup that cannot be restored is worthless, and faults are often found only when a restore is tried

3.3

(a) only marks and attendance, with a pseudonym, and maybe year group; name, address, phone numbers and full date of birth are not needed for learning analysis (data minimisation)

(b) there are only 10^6 possible ids, so anyone can hash them all and reverse the hash in seconds; use a keyed hash (HMAC) with a secret key that only the school holds, or random codes

(c) a fixed period, e.g. until the end of the school year; the company deletes all copies, including backups, and confirms in writing; no use for any other purpose

(d) yes, if the conditions hold: minimum columns, keyed pseudonyms, encryption in transit and at rest, a signed agreement with retention and audit rights, and parents told; otherwise no

exercises.lol exercises.com.cn