

## 1.3 EXCHANGING DATA · 1.3.1

**Encryption & hashing — Mark scheme**

30 marks · spec 1.3.1(c)(d)

**AO key:** AO1 = knowledge & understanding · AO2 = application · AO3 = reasoned judgements. Accept any valid alternative; do not award the same point twice.

| Q    | ANSWER                                                                | AO  | MARKS |
|------|-----------------------------------------------------------------------|-----|-------|
| 1(a) | To keep data confidential / unreadable to anyone without the key. (1) | AO1 | 1     |
| 1(b) | Plaintext (before) (1); ciphertext (after) (1). (2)                   | AO1 | 2     |
| 1(c) | Two-way. (1)                                                          | AO1 | 1     |

| Q    | ANSWER                                                                                                                                                            | AO  | MARKS |
|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------|
| 2(a) | A single (shared) key (1) is used for both encryption and decryption (1). (2)                                                                                     | AO1 | 2     |
| 2(b) | The key must be shared with the recipient (1); if it is intercepted in transit the encryption is broken (key distribution problem) (1). (2)                       | AO2 | 2     |
| 2(c) | Asymmetric uses a public key to encrypt that can be shared openly (1); only the secret private key can decrypt, so no secret key needs to be transmitted (1). (2) | AO2 | 2     |

| Q    | ANSWER                                                                                                               | AO  | MARKS |
|------|----------------------------------------------------------------------------------------------------------------------|-----|-------|
| 3(a) | A fixed-length value produced from data by a hash function (1) that is one-way / cannot be reversed (1). (2)         | AO1 | 2     |
| 3(b) | If the database is stolen the real passwords are not revealed (1) because the hash cannot be reversed (1). (2)       | AO2 | 2     |
| 3(c) | Hash the password the user enters (1) and compare it with the stored hash; if they match, access is granted (1). (2) | AO2 | 2     |

| Q    | ANSWER                                                                                                                                                                                                                                                                                                                    | AO  | MARKS |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-------|
| 4(a) | 1 mark each, max 2: checking data integrity (file unchanged) · hash tables / fast lookup · digital signatures. (2)                                                                                                                                                                                                        | AO1 | 2     |
| 4(b) | 2 characteristics, 1 mark + 1 for the second / development, max 3, e.g.: <ul style="list-style-type: none"> <li>• quick to compute but practically impossible to reverse (1)</li> <li>• produces few collisions (different inputs rarely give the same hash) (1)</li> <li>• produces a fixed-length output (1)</li> </ul> | AO1 | 3     |

| Q                | LEVELS-OF-RESPONSE MARK SCHEME                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | AO    | MARKS      |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|---------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------|---|-----------------------|-------------------------------------|---|
| 5                | <p>Mark using the levels descriptors below. AO1 (knowledge of encryption/hashing), AO2 (application to the robot), AO3 (justified choice for each purpose).</p> <table><tr><th>LEVEL</th><th>DESCRIPTOR</th></tr><tr><td>Level 3<br/>(7–9)</td><td>Compares encryption and hashing accurately, clearly <b>applied</b> to both storing passwords and transmitting data, with a clear <b>justified</b> choice for each. Well structured.</td></tr><tr><td>Level 2<br/>(4–6)</td><td>Discusses both with <b>some</b> application; choices made with partial justification.</td></tr><tr><td>Level 1<br/>(1–3)</td><td>Basic points about encryption and/or hashing with little application or justification.</td></tr><tr><td>0</td><td>Nothing creditworthy.</td></tr></table> <p><b>Indicative content</b> (credit any valid point):</p> <ul style="list-style-type: none"><li>• Hashing is one-way — ideal for stored passwords: even if the robot's storage is accessed, passwords cannot be recovered.</li><li>• Encryption is two-way — ideal for transmitted data: the control centre needs to decrypt and read it, which hashing could not allow.</li><li>• Transmitted data could use asymmetric encryption (no shared secret over the air) or a symmetric key exchanged securely.</li><li>• Justified conclusion: hash the passwords, encrypt the transmitted data — they solve different problems.</li></ul> | LEVEL | DESCRIPTOR | Level 3<br>(7–9) | Compares encryption and hashing accurately, clearly <b>applied</b> to both storing passwords and transmitting data, with a clear <b>justified</b> choice for each. Well structured. | Level 2<br>(4–6) | Discusses both with <b>some</b> application; choices made with partial justification. | Level 1<br>(1–3) | Basic points about encryption and/or hashing with little application or justification. | 0 | Nothing creditworthy. | AO1<br>×3<br>AO2<br>×3<br>AO3<br>×3 | 9 |
| LEVEL            | DESCRIPTOR                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |       |            |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |
| Level 3<br>(7–9) | Compares encryption and hashing accurately, clearly <b>applied</b> to both storing passwords and transmitting data, with a clear <b>justified</b> choice for each. Well structured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |       |            |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |
| Level 2<br>(4–6) | Discusses both with <b>some</b> application; choices made with partial justification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |            |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |
| Level 1<br>(1–3) | Basic points about encryption and/or hashing with little application or justification.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |       |            |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |
| 0                | Nothing creditworthy.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |       |            |                  |                                                                                                                                                                                     |                  |                                                                                       |                  |                                                                                        |   |                       |                                     |   |

**Total for paper: 34 marks**