MARKING SCHEME (GUIDE)

1. (a) Transistor.

   (b) 1st-Vacuum Tubes; 3rd-ICs; 4th-VLSI.

2. (a) Wekesa: Control Unit (CU); Njoroge: Arithmetic Logic Unit (ALU).

   (b) False.

3. (a) Half-Duplex.

   (b) Half-duplex is one direction at a time; Full-duplex is both directions simultaneously.

4. (a) Software that manages computer hardware and software resources.

   (b) Command Line Interface (CLI).

5. (a) Identifier: total_score/math_mark; Operator: + / *.

   (b) Brackets () have the highest precedence.

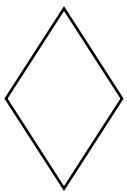
6. (a) Star Topology.

   (b) If the main cable fails, the whole network goes down.

7. (a) Lists, Tuples, Dictionaries, Sets.

   (b) Lists are mutable (can change); Tuples are immutable (cannot change).

8. (a) Diamond.



   (b) Oval/Capsule shape.

9. (a) MAN (Metropolitan Area Network).

   (b) Fiber Optic.

   (c) Attenuation, Noise, Distortion.

   (d) Routes data packets between different networks.

(e)

i. **Man-in-the-Middle (MitM) Attacks:** An attacker positions themselves between your device and the connection point, allowing them to intercept and even change the data you are sending or receiving.
ii. **Unencrypted Networks:** Many public hotspots do not use encryption (like WPA2/WPA3). This means any data sent over the air is "in the clear" and can be easily read by anyone with basic hacking tools.
iii. **Evil Twin Hotspots:** Hackers set up a fake Wi-Fi network with a name identical or similar to a legitimate one (e.g., "Town_Free_WiFi"). When you connect, they gain full access to your traffic.
iv. **Packet Sniffing:** Using software called "sniffers," cybercriminals can monitor all data packets moving through the network to pull out passwords, account numbers, and personal details.
v. **Malware Injection:** Attackers can use the network connection to slip malicious software onto your device, which could then lead to identity theft or the locking of your files (ransomware).
vi. **Session Hijacking:** A hacker can steal your "session cookie"—the small file that keeps you logged into a site—to take over your active accounts (like social media or email) without needing your password.
vii. **Snooping and Eavesdropping:** Even without high-tech tools, someone on the same network can see which websites you are visiting and how long you stay on them, compromising your digital privacy.
viii. **Shoulder Surfing:** Because public Wi-Fi is used in public spaces, there is a physical risk of someone simply watching you type in passwords or viewing sensitive documents over your shoulder.
ix. **Network Sluggishness:** Because these networks are shared by many users, they are often slow, prone to dropping connections, and can lead to data corruption if a file transfer is interrupted.
x. **Adware and Tracking:** Some providers of "free" Wi-Fi track your browsing habits or force pop-up advertisements onto your device to monetize the service.

10. (a) i. **SSD:** Solid State Drive
    ii. **HDD:** Hard Disk Drive

    (b) Primary is volatile/temporary; Secondary is non-volatile/permanent.
    (c) Faster speed, more robust/durable.
    (d) ALU.
    (e) RISC uses simple instructions; CISC uses complex ones.
    (f) PROM/EPROM/EEPROM.

11. (a) Problem Definition -> Design -> Coding -> Testing -> Implementation.

    (b)

```
START

  PRINT "Enter the age of the first student:"

  INPUT age1

  PRINT "Enter the age of the second student:"

  INPUT age2



  SET sum = age1 + age2

  SET average = sum / 2



  PRINT "The average age is: " + average

END
```

(c) Syntax Error/Type Error (cannot concatenate string and integer).

12. (a) Repeatedly swapping adjacent elements if they are in the wrong order.

(b) Sequential checks one by one; Binary divides the list in half (requires sorting).

(c) Dictionary.

(d) Finite, Definite, Effective.