IGCSE Computer Science Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. What is a consequence of data loss?

A. Increased data accessibility

B. Potential disruption to operations

C. Improved security measures

D. Enhanced device performance

2. Which statement is true regarding biometric passwords?

A. They can be easily forgotten

B. They are unique and cannot be easily shared

C. They are less secure than text-based passwords

D. They can be changed frequently

3. What are the primary colors used in an LCD display?

A. Red, Yellow, Blue

B. Red, Green, Blue

C. Green, Blue, Yellow

D. Cyan, Magenta, Yellow

4. What is the function of a motion sensor in security devices?

A. To control the temperature settings

B. To detect the presence of movement

C. To measure the humidity levels

D. To adjust the light intensity

5. How does a 3D cutter achieve precise and clean cuts?

A. Using basic manual controls

B. By operating at low power

C. Through sophisticated computer control and software

D. Utilizing standard cutting techniques

6. Which unit follows megabyte in increasing memory sizes?

A. Terabyte

B. Gigabyte

C. Kilobyte

D. Petabyte

7. What characteristic defines a computer virus?

A. It is a program designed to protect your computer

B. It self-replicates and disrupts computer operations

C. It requires user permission to operate

D. It is created for educational purposes

8. What is plagiarism?

A. Using someone's work with permission

B. Claiming someone else's ideas as your own

C. Collaborating with others on projects

D. Referencing sources incorrectly

9. What does the sensor in an inkjet printer detect?

A. The model of printer being used

B. Whether paper is available for printing

C. The quality of the ink

D. The temperature of the printer

10. What is shareware?

A. Software available for free indefinitely

B. Software that offers a trial version before purchase

C. Software that cannot be purchased

D. Software provided without copyright

Answers

1. B
2. B
3. B
4. B
5. C
6. B
7. B
8. B
9. B
10. B

Explanations

1. What is a consequence of data loss?

A. Increased data accessibility

B. Potential disruption to operations

C. Improved security measures

D. Enhanced device performance

Data loss can significantly impact an organization or individual by causing interruptions to operations. When data is lost, it may result in the inability to access important information needed for daily business activities, decision-making, or customer service. This disruption can lead to delays, financial losses, and potential damage to reputation as stakeholders may become frustrated with the lack of access to necessary data. In contrast, increased data accessibility, improved security measures, and enhanced device performance do not stem from data loss. Rather, these are factors that might be considered as goals for an organization when managing data. Data loss leads to complications and challenges rather than improvements in these areas. Thus, the correct answer highlights a realistic and serious consequence of experiencing data loss.

2. Which statement is true regarding biometric passwords?

A. They can be easily forgotten

B. They are unique and cannot be easily shared

C. They are less secure than text-based passwords

D. They can be changed frequently

Biometric passwords refer to authentication methods that utilize unique physical characteristics of an individual, such as fingerprints, facial recognition, or iris scans. The statement regarding their uniqueness is accurate because biometric data is inherently specific to each individual, making it difficult to replicate or share. Unlike traditional passwords, which can be easily shared or guessed, biometric identifiers greatly enhance security by relying on traits that are unique to each user. In addition to their uniqueness, biometric passwords offer the advantage of being very difficult for others to acquire or reproduce without having direct access to the individual. This feature helps to ensure that access to secure systems is limited to authorized users, significantly reducing the chance of unauthorized access. Understanding the properties of biometric passwords allows for better security practices in digital environments, reinforcing the importance of unique identification in safeguarding personal and sensitive data.

3. What are the primary colors used in an LCD display?

A. Red, Yellow, Blue

B. Red, Green, Blue

C. Green, Blue, Yellow

D. Cyan, Magenta, Yellow

The primary colors used in an LCD display are red, green, and blue. These colors are the fundamental elements of the additive color model, which is based on the principle that when combined in various ways, they can create a broad spectrum of colors. In an LCD (Liquid Crystal Display), each pixel is made up of sub-pixels that emit red, green, and blue light. By varying the intensity of each of these three colors, the display can produce a wide range of colors by combining them in different proportions. For example, combining red and green light creates yellow, red and blue light create magenta, and green and blue light create cyan. ThisRGB color model is standard in various digital displays, including computer monitors, televisions, and smartphone screens. The choice of red, green, and blue is significant in electronic devices because these colors align well with human vision, providing an effective means to represent colors accurately.

4. What is the function of a motion sensor in security devices?

A. To control the temperature settings

B. To detect the presence of movement

C. To measure the humidity levels

D. To adjust the light intensity

The function of a motion sensor in security devices is primarily to detect the presence of movement. Motion sensors are designed to identify changes in physical space, typically by using various technologies such as infrared, microwave, or ultrasonic waves. When an object, such as a person or an animal, moves within the sensor's coverage area, the sensor triggers an alert or activates a camera, alarm, or other security protocol. This capability is crucial for security systems because it enables real-time responses to potential intrusions, thereby enhancing the overall safety of a premises. Additionally, motion sensors can help reduce false alarms since they specifically respond to movement rather than just detecting light changes or temperature variations.

5. How does a 3D cutter achieve precise and clean cuts?

A. Using basic manual controls

B. By operating at low power

C. Through sophisticated computer control and software

D. Utilizing standard cutting techniques

A 3D cutter achieves precise and clean cuts primarily through sophisticated computer control and software. This technology allows for intricate design inputs and optimizes the cutting path and speed, ensuring that the cutter can follow very detailed and complex specifications with high accuracy. Advanced software also enables features such as simulation and error detection, which help in refining the cutting process before it begins. This level of control ensures that the cutter can maintain tight tolerances and produce high-quality finishes, making it highly effective in various applications, from manufacturing to intricate artistic designs. In contrast, basic manual controls would lack the precision and repeatability necessary for high-quality cutting, while operating at low power could further compromise the effectiveness of the cut. Utilizing standard cutting techniques might not leverage the advantages of modern technology and could result in less precision compared to what computer-controlled methods can achieve.

6. Which unit follows megabyte in increasing memory sizes?

A. Terabyte

B. Gigabyte

C. Kilobyte

D. Petabyte

The unit that follows a megabyte in increasing memory sizes is the gigabyte. In the hierarchy of data storage units, the sequence progresses as follows: kilobyte, megabyte, gigabyte, terabyte, and then petabyte. Each of these units represents a significant increase in data size. A megabyte amounts to 1,024 kilobytes, and a gigabyte is 1,024 megabytes. Therefore, the gigabyte directly follows the megabyte in this standard measurement system. Understanding this hierarchy is essential for grasping how data storage capacities are incremented and how much information they can hold.

7. What characteristic defines a computer virus?

A. It is a program designed to protect your computer

B. It self-replicates and disrupts computer operations

C. It requires user permission to operate

D. It is created for educational purposes

A computer virus is characterized primarily by its ability to self-replicate and disrupt normal computer operations. This means that a virus can make copies of itself and spread to other files or programs on the computer and potentially across networks. The disruption can manifest in various ways, such as corrupting files, monitoring user activity without consent, or slowing down system performance. Self-replication is a fundamental trait separating viruses from other types of software; while many programs can perform tasks or have effects on a computer, a virus specifically aims to spread and cause interference. This behavior can lead to significant security risks and damage, making it crucial for users to have protective measures in place. Other characteristics listed, such as requiring user permission to operate or being created for educational purposes, do not define a virus. In many cases, viruses can execute without explicit user consent or knowledge, highlighting their malicious nature.

8. What is plagiarism?

A. Using someone's work with permission

B. Claiming someone else's ideas as your own

C. Collaborating with others on projects

D. Referencing sources incorrectly

Plagiarism is defined as the act of claiming someone else's ideas, work, or intellectual property as your own without proper acknowledgment. This can include copying text, ideas, images, or code from another source and presenting it as if it were created by you. The key aspect of plagiarism is the lack of attribution to the original creator, which is essential in respects to intellectual integrity and academic honesty. When someone fails to give credit where it is due, they misrepresent their own efforts and contributions, which undermines the value of their work. This is particularly crucial in educational and professional contexts, where clarity about the origin of ideas and concepts is necessary to promote trust and credibility. In contrast, using someone's work with permission, collaborating with others on projects, or incorrectly referencing sources, while potentially problematic in different contexts, do not fit the strict definition of plagiarism as they either involve honest acknowledgment of sources or collaborative effort where contributions are shared and recognized. The focus on ownership of ideas and the ethical implications make the definition of plagiarism specific to the misappropriation of intellectual property.

9. What does the sensor in an inkjet printer detect?

A. The model of printer being used

B. Whether paper is available for printing

C. The quality of the ink

D. The temperature of the printer

In an inkjet printer, the sensor plays a crucial role in the printing process by detecting whether paper is loaded and available for printing. This detection is important because it prevents the printer from attempting to print when there is no paper, which could lead to errors or damage. The sensor ensures that the printer operates smoothly by signaling the presence or absence of paper in the feed mechanism. This functionality is fundamental to the printer's operation, as it directly impacts the success of print jobs and the user experience. Other options involve aspects that are not typically monitored by the printer's sensor. For instance, while the model of the printer might be identified by internal software, it is not a function of the sensors. Similarly, while ink quality is vital for print outputs, ink levels are typically monitored through other means, such as electronic signals from the cartridges rather than direct sensing. Lastly, the temperature of the printer is not usually detected by a sensor specifically for paper handling but might be monitored through other components or safety mechanisms.

10. What is shareware?

A. Software available for free indefinitely

B. Software that offers a trial version before purchase

C. Software that cannot be purchased

D. Software provided without copyright

Shareware refers to a distribution method for software that allows users to try a limited version of a program before making a purchasing decision. Typically, shareware is provided with some restrictions, such as feature limitations or a trial period. This model encourages users to evaluate the software's capabilities, and if they find it valuable, they can then choose to purchase the full version, which may include additional features or no time limitations. This approach benefits both developers and users, as it allows developers to showcase their products and potential customers to assess the software's fit for their needs. The trial period or limited features create a sense of urgency and encourage the decision to buy, while also helping to protect intellectual property since the software is not freely available in its entirety from the start.