

一、選擇題（單選）24 題，每題 2.5 分，共 60 分，請在每題的選項內選擇最適當的答案。

注意：答錯倒扣 1 分，扣至零分為止。（不答不倒扣）

※ 注意：請用 2B 鉛筆作答於答案卡，並先詳閱答案卡上之「畫記說明」。

- Which of the following technology is not used in Amazon Echo or Google Home? (A) speech recognition (B) image recognition (C) natural language processing (D) control of room devices (E) speech synthesis.
- Which of the following is wrong about object-oriented databases? (A) object-oriented databases are the most widely used database model today (B) object databases store objects rather than data such as integers, strings or real numbers (C) objects basically consist of attributes and methods (D) objects contain both executable code and data (E) all of the above are correct (choose this only if none of the above can be chosen).
- Which of the following is wrong about relational databases? (A) relational databases store data in tables (B) tables consist of rows and columns (C) all table columns depend on a primary key to identify the column (D) a table corresponds to a relation (E) all of the above are correct (choose this only if none of the above can be chosen).
- Which of the following SQL commands returns the number of countries of the records in the "Customers" table (see Table 1)?
 (A) SELECT NUMBER (*) FROM Customers;
 (B) SELECT COUNT (ALL country) FROM Customers;
 (C) SELECT COUNT (DISTINCT country) FROM Customers;
 (D) SELECT NUMBER (ALL country) FROM Customers;
 (E) SELECT NUMBER (DISTINCT * country) FROM Customers;

Table 1 "Customers":

id	name	email	country
1	Jay Liang	jay@gmail.com	Taiwan
2	Vison Li	visionli@hotmail.com	Taiwan
3	Shiao Wang	swong@gmail.com	Japan
4	Shiao Ming	sming@uscc.com	USA

- Which of the following SQL commands lists the number of customers in each country from the "Customers" table (see Table 1)?
 (A) SELECT NUMBER (id), country FROM Customers GROUP BY country;
 (B) SELECT NUMBER (id), country FROM Customers ORDER BY country;
 (C) SELECT COUNT (id), country FROM Customers GROUP BY country;
 (D) SELECT COUNT (id), country FROM Customers ASSEMBLY BY country;
 (E) none of the above.
- Which of the following types of databases has been optimized for data warehousing and OLAP (online analytical processing) for complex analytical and ad hoc queries with a rapid execution time? (A) object-oriented databases (B) multidimensional databases (C) crossed relational databases (D) relational object-oriented databases (E) distributed databases.
- In database terminology, a read of uncommitted data is referred to as a (A) phantom read (B) dirty read (C)

見背面

- non-repeatable read (D) lost update (E) none of the above.
8. Which of the following about Open Systems Interconnection (OSI) reference model is wrong? (A) Layer 3 is Network Layer (B) Layer 6 is Presentation (C) IP belongs to Layer 3 (D) UDP belongs to Layer 4 (E) all of the above are correct (choose this only if none of the above can be chosen).
 9. Which of the following is a computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner? (A) Kerberos (B) Dynamic Host Configuration Protocol (C) Secure Remote Password protocol (SRP) (D) Internet Key Exchange (E) none of the above.
 10. Which of the following is relatively not a main concern of the HTTPS protocol? (A) authentication of the accessed website (B) protection of communication privacy (C) protection of man-in-the-middle attacks (D) fault tolerance (E) protection of tampering of the communication.
 11. Which of the following about digital certificate is wrong? (A) the "Serial Number" field in a digital certificate is used to track revocation information (B) the "Issuer" field specifies the entity that verified the information and signed the certificate (C) it needs to contain the certificate owner's public key (D) X.509 is a standard that defines the format of public key certificates (E) all of the above are correct (choose this only if none of the above can be chosen).
 12. Which of the following about Single Sign-On (SSO) is wrong? (A) it reduces password fatigue from different user name and password combinations (B) it reduces time spent re-entering passwords for the same identity (C) log-in with Facebook account is an example of SSO (D) log-in with Google account is an example of SSO (E) all of the above are correct (choose this only if none of the above can be chosen).
 13. Which of the following enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network? (A) Transport Layer Security (B) Secure Sockets Layer (C) Virtual Private Network (D) Network Address Translation (E) none of the above.
 14. Which of the following is not a file system? (A) Hierarchical File System (HFS) (B) New Technology File System (NTFS) (C) Extended File Allocation Table (exFAT) (D) third extended filesystem (ext3) (E) Microsoft Disk Operating System (MS-DOS).
 15. Which of the following best describes a specialized hardware-dependent computer program which is also operating system specific that enables another program to interact transparently with a hardware device? (A) firmware (B) device driver (C) application programming interface (D) hardware platform interface (E) intelligent platform management interface.
 16. Which of the following is wrong? (A) the primary goal of CISC (Complex Instruction Set Computer) architecture is to complete a task in as few lines of assembly code as possible (B) the RISC (Reduced Instruction Set Computer) approach is designed to execute computing tasks with the simplest instructions in the shortest amount of time possible (C) Intel x86 architecture is typically considered as a CISC approach (D) ARM architecture is typically considered as a RISC approach (E) all of the above are correct (choose this only if none of the above can be chosen).
 17. Which of the following refers to the act of creating a virtual version of something, including virtual computer hardware platforms, storage devices, and computer network resources? (A) virtual reality (B) augmented reality (C) virtualization (D) hypervisor (E) none of the above.
 18. Which of the following about Bitcoin is wrong? (A) "mining" is a process to use a user's computing power to verify and record payments in the system (B) currently, new coins are created through the process of "mining" (C) there is no central administrator involved in the issue of new coins (D) both money sender and receiver do not need to know each other (other than a meaningless number) in money transfer (E) all of the above are correct (choose this only if none of the above can be chosen).
 19. Which of the following about the Blockchain technology used in Bitcoin is wrong? (A) it is a continuously growing list of "blocks" recording transaction history of the Bitcoin system (B) the blocks in a blockchain can be distributed to different peers so that no peer is required to maintain the complete list of the blocks in the system (C) all transactions in the blocks are kept anonymous and encrypted (D) blockchains are inherently resistant to modification of the data that have been recorded into blocks (E) all of the above are correct (choose this only if none of the above can be chosen).
 20. Which of the following is correct about the CIA Triad of information security model? (A) "C" refers to Control (B) "C" refers to Cryptography (C) "I" refers to Identification (D) "A" refers to Anonymous (E) "A" refers to Availability.
 21. Which of the following is not a symmetric encryption mechanism? (A) DES (B) IDEA (C) RSA (D) Caesar

cipher (E) Advanced Encryption Standard (AES).

22. With the advent of Internet of Things (IoT), which of the following types of security attacks become even more challenging to defend than the others? (A) social engineering (B) Distributed Denial of Service (DDoS) (C) Phishing (D) SQL injection (E) Session Hijacking.
23. Which of the following is the best-known standard providing requirements for an information security management system (ISMS)? (A) ISO 9001 (B) ISO 14001 (C) ISO 26000 (D) ISO/IEC 27001 (E) ISO 31000.
24. Which of the following is correct about the ACID Database Properties? (A) "A" refers to Anonymity (B) "C" refers to Continuity (C) "I" refers to Integrity (D) "D" refers to Durability (E) none of the above is correct.

二、問答題 2 題，每題 20 分，共 40 分。

※ 本大題請於試卷內之「非選擇題作答區」標明題號依序作答。

1. You are given an array that stores n objects of three different types: Type 0, Type 1, and Type 2. The array elements are assumed to be indexed from 0 through $n - 1$. Design an algorithm to rearrange the objects so that objects of the same type occupy consecutive locations in the array, with the objects of Type 0 in the front followed by those of Type 1 and then those of Type 2. Please present your algorithm in adequate pseudocode. Give an analysis of its time complexity. The more efficient your algorithm is and the less space it uses, the more points you will be awarded for this problem.

2. The celebrated Prim's algorithm for finding a minimum(-weight) spanning tree of a weighted undirected graph is based on the following theorem:

Theorem: Given a connected weighted undirected graph $G=(V,E)$, let V_1 and V_2 be a partition of V and $E(V_1,V_2)$ be the set of edges connecting nodes in V_1 to nodes in V_2 . One of the edges with the minimum weight in $E(V_1,V_2)$ must belong to a minimum spanning tree of G .

Prove the correctness of the above theorem.

試題隨卷繳回