1. (12 %)

(1) Accountability, as one of the primary goals of computer security, is about the capability of _____. (4 %)

    a. preventing, detecting or deterring the improper disclosure of information

    b. preventing, detecting, or deterring the improper modification of data

    c. ensuring that users of data/resources are the persons they claim to be

    d. tracing breach of security back to responsible party

    e. preventing, detecting, or deterring the unauthorized denial of service or data to legitimate users

(2) Which of the following is NOT one of the main purposes of cryptography? (4 %)

    a. Protecting the meaning of a message so that it can not be understood by anyone other than the intended recipient.

    b. Concealing the existence of a message so that it can not be read by anyone other than the intended recipient.

    c. Ensuring that users of data/resources are the persons they claim to be.

    d. Ensuring that a message has not been secretly and/or illegally altered.

    e. Preventing unauthorized disclosure of information.

(3). A cipher is a method for encrypting messages. Your job here is to decipher the cipher text below that is encrypted using a polyalphabetic cipher. The polyalphabetic cipher includes two monoalphabetic (single-alphabetic) ciphers: C_1 (key = 3) and C_2 (key = 5) and the sequence of the ciphers is C_1, C_2, C_2.

    Cipher text: "L　GJONJYJ　N　FFS　IQD."

    The plain text is "_____." (4 %)

2. (20 %)

(4) In John's Java code, if he calls a method which does not exist in the indicated class and then compiles the code, the compiler would display an error message. The indicated coding error John has made is called a _____. (4 %)

  a. system error   d. syntax error

  b. logic error   e. run-time error

  c. semantic error

（背面仍有題目，請繼續作答）

(5) Give the results of the following java program. (4 %)

```
int z = -1;
system.out.println(++z);
system.out.println(z--);
system.out.println(z++ + z);
system.out.println(z + z++);
```

a. 0 0 0 1

b. 0 1 0 0

c. 0 0 -2 1

d. 0 0 -2 0

e. 0 0 -1 0

(6) Which of the following addresses the concern of controlling simultaneous updates to the same dataset in a DBMS? (4 %)

a. Atomicity

b. Isolation

c. Duration

d. Concurrency

e. Consistency

(7) Which of the following is true? (4 %)

a. A primary key can be composed of three data fields.

b. Relational DBMS is more powerful in terms of managing data in video/audio format compared to the object-oriented DBMS.

c. A table can have only one primary key and one foreign key.

d. Data Control Language (DCL) is a language used to communicate the structure of a database to the DBMS.

e. None of the above is true.

(8) Assume that a table A contains a foreign key that matches the primary key of table B. If a record in table B is deleted, the records in the table A whose foreign key values are equal to the primary key value of the deleted record in table B will be deleted correspondingly. This control mechanism for maintaining referential integrity of the database is called _____. (4 %)

a. Reference

b. Restriction

c. Nullification

d. Cascade

e. Isolation

本試題是否可以使用計算機：　□可使用　，　☑不可使用　（請命題老師勾選）

3. (18 %)

(9) Which one of the following is NOT one of the differences between IPv4 and IPv6? (4 %)

    a. IPv6 has longer packet header.

    b. IPv4 utilizes fixed-length field headers.

    c. They use different addressing notations.

    d. There is no error checking field in an IPv6 packet header.

    e. IPv4 is more vulnerable to security threats compared to IPv6.

(10) Which of the following can be a useful protective measure for counteracting the network attack of address spoofing? (4 %)

    a. Service filtering

    b. Sequence numbering

    c. Digital signature

    d. Firewalls

    e. None of the above

(11) Which of the following is a protocol with respect to the transport layer of the OSI 7-layer network model? (4 %)

    a. FTP

    b. Telnet

    c. SMTP

    d. UTP

    e. UDP

(12) Briefly answer the following questions:

    a. Describe the difference between the "*pure*" and the "*hybrid*" (server-mediated) peer-to-peer architectures. (2 %)

    b. Describe the pros and cons of these two kinds of peer-to-peer architectures in contrast with each other. (4 %)

4. 單選題：每題5分

(13) What is the cause of the last-mile bottleneck that hampers data transmissions on the PSTN?
(a) People tend to use their computers more heavily during peak times.
(b) There are often more people in a local loop than can be adequately processed.
(c) Many telephones are in rural areas, and signals are slowed due to extra transmission miles.
(d) Most telephones in local loops are using analog technology yet.
(e) None of the above

(14) Which of the following is NOT a wireless specification?
(a) 802.11a
(b) 802.11b
(c) 802.11c
(d) 802.11g
(e) 802.11n

(15) Of the following sorting algorithms, which has a running time that is LEAST dependent on the initial ordering of the input?
(a) Insertion Sort
(b) Quick Sort
(c) Merge Sort
(d) Selection Sort
(e) Shell Sort

(16) Which of the following is/are true?
I. Interpreters generally have a higher execution overhead since the program code is continuously re-examined.

II. Interpreters often have a higher space overhead compared with compilers. For example, the interpreter and all the supported routines must usually be kept available. In contrast, compilers use dynamic linking to link the target routine at run-time. This feature helps to minimize space utilization.

III. Any language that can be interpreted can also be compiled. However, not all languages that can be compiled can be interpreted.
(a) Only I
(b) Only II
(c) Only I and II
(d) Only I and III
(e) I, II, and III

本試題是否可以使用計算機：□可使用 ，☑不可使用 （請命題老師勾選）

5. 問答題：每題5分

(17) On Unix, each file is associated with one user and one group. A limited access list is implemented by assigning a set of permissions for the owner of the file, those in the same group as the file but who are not the owner, and for everyone else. The operations controlled are read, write, and execute access. Assume the system may have up to 2^{16} users and 2^8 groups. How many bits are needed to store each file's access data? Why?

(18) Tom's company has been assigned the network address 163.18.0.0. Currently, she oversees 50 subnets on her network, which will grow to 56 subnets over the next year. Subnets on the network will require up to 800 hosts each. Which subnet mask should Tom assign to the network? Why?

(19) End users may use Microsoft IE, Netscape, FireFox, Mozilla, Thunderbird, Lynx, or Telnet tool to browse HTML documents. Describe how do users browse HTML files via Telnet? What are the pros and cons of this approach?

(20) XML differs from HTML in three major features: extensibility, structure, and validity. Please explain how it differs respectively?

(21) The OSI networking suite is constituent of a protocol stack including physical, transport, data link, presentation, session, network, and application layers. Please explain why the network layer is a lower layer under the transport layer, and the session layer is an upper layer over the transport layer.

(22) How does open-source development differ from beta testing of a software package?