1. _____ assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
   (A) Availability (B) System Integrity (C) Privacy（隱私） (D) Data Integrity

2. _____ assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
   (A) System Integrity（系統完整性） (B) Data Integrity
   (C) Availability (D) Confidentiality

3. A loss of _____ is the unauthorized disclosure of information.
   (A) confidentiality（機密） (B) integrity
   (C) authenticity (D) availability

4. A _____ level breach of security could be expected to have a severe or catastrophic（災難性地） adverse effect on organizational operations, organizational assets, or individuals.
   (A)low (B) normal (C)moderate (D) **high**

5. A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy is a(n) _____.
   (A) countermeasure (B) vulnerability（脆弱性）
   (C) adversary (D) risk

6. An assault on system security that derives from an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system is a(n) _____.
   (A) risk (B) asset (C) attack（攻擊） (D) vulnerability

7. A(n) _____ is an action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that correct action can be taken.
   (A) attack (B) countermeasure（對策）
   (C) adversary (D) protocol

8. A(n) _____ is an attempt to learn or make use of information from the system that does not affect system resources.
   (A) passive attack（被動攻擊） (B)inside attack
   (C) outside attack (D) active attack

9. Masquerade, falsification, and repudiation are threat actions that cause _____ threat consequences.
   (A) unauthorized disclosure (B) deception（欺騙）
   (C) disruption (D) usurpation

10. A threat action in which sensitive data are directly released to an unauthorized entity is _____.
(A) corruption (B) disruption (C) intrusion (D) exposure（曝光）

11. An example of _____ is an attempt by an unauthorized user to gain access to a system by posing as an authorized user.
(A) masquerade（偽裝） (B) interception (C) repudiation (D) inference

12. The _____ prevents or inhibits the normal use or management of communications facilities.
(A) passive attack (B) traffic encryption
(C) denial of service（阻斷服務） (D) masquerade

13. A _____ is any action that compromises the security of information owned by an organization.
(A) security mechanism (B) security attack（資安攻擊）
(C) security policy (D) security service

14. The assurance that data received are exactly as sent by an authorized entity is _____.
(A)authentication (B) data confidentiality
(C) access control (D) data integrity（資料完整性）

15. _____ is the insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
(A) Traffic padding（訊務填充） (B) Traffic routing
(C) Traffic control (D) Traffic integrity

16. The original message or data that is fed into the algorithm is _____.
(A) encryption algorithm (B) secret key (C) decryption algorithm (D) plaintext（明文）

17. The _____ is the encryption algorithm run in reverse.
(A) decryption algorithm（解密演算法） (B) plaintext
(C) ciphertext (D) encryption algorithm

18. _____ is the scrambled message produced as output.
(A) Plaintext (B) Ciphertext（密文） (C) Secret key (D) Cryptanalysis

19. On average, _____ of all possible keys must be tried in order to achieve success with a brute-force attack.
(A) one-fourth (B) half（一半） (C) two-thirds (D) three-fourths

20. The most important symmetric algorithms, all of which are block ciphers, are the DES, triple DES, and the _____.
(A) SHA (B) RSA (C) AES（進階加密標準） (D) DSS

21. If the only form of attack that could be made on an encryption algorithm is brute-force, then the way to counter such attacks would be to _____ .
(A) use longer keys（使用較長的金鑰） (B) use shorter keys
(C) use more keys (D) use less keys

22. _____ is a procedure that allows communicating parties to verify that received or stored messages are authentic.
(A) Cryptanalysis (B) Decryption
(C) Message authentication（訊息認證） (D) Collision resistance

23. The purpose of a _____ is to produce a "fingerprint" of a file, message, or other block of data.
(A) secret key (B) digital signature
(C) keystream (D) hash function（雜湊函式）

24. _____ is a block cipher in which the plaintext and ciphertext are integers between 0 and *n*-1 for some *n* and its encryption key is different from its decryption key and hence an asymmetric（非對稱） cryptography algorithm .
(A) DSS (B) **RSA** (C) SHA (D) AES

25. A _____ is created by using a secure hash function to generate a hash value for a message and then encrypting the hash code with a private key.
(A) digital signature（數位簽名） (B) keystream
(C) one way hash function (D) secret key

26. Transmitted data stored locally are referred to as _____ .（§2.6,pp.79）
(A) ciphertext (B) DES (C) data at rest（暫歇資料）(D) ECC

27. Digital signatures and key management are the two most important applications of _____ encryption.
(A) private-key (B) public-key（公開金鑰）
(C) preimage resistant (D) advanced

28. A _____ is to try every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained.
(A) mode of operation (B) hash function
(C) cryptanalysis (D) brute-force attack（暴力攻擊）

29. Combined one byte at a time with the plaintext stream using the XOR operation, a _____ is the output of the pseudorandom bit generator.
(A) keystream（金鑰串流） (B) digital signature
(C) secure hash (D) message authentication code

30. A _____ protects against an attack in which one party generates a message for another party to sign.
(A) data authenticator (B) strong hash function（強雜湊函式）
(C) weak hash function (D) digital signature

31. A _____ is a separate file from the user IDs where hashed passwords are kept.
(A) **shadow（影子）** (B) password (C) secret (D) account

32. A password _____ prevents duplicate passwords from being visible in the password file. Even if two users choose the same password the hashed passwords of the two users will differ.
(A) sugar (B) salt（鹽） (C) random (D) hash

33. Presenting or generating authentication information that corroborates the binding between the entity and the identifier is the _____.
(A) identification step (B) verification step（驗證步驟）
(C)authentication step (D) corroboration step

34. Recognition by fingerprint, retina, and face are examples of _____.
(A) face recognition (B) dynamic biometrics
(C) static biometrics（靜態生物識別） (D) token authentication

35. A _____ is a password guessing program.
(A) password hash (B) password cracker（密碼破解器）
(C) password biometric (D) password salt

36. The _____ strategy is when users are told the importance of using hard to guess passwords and provided with guidelines for selecting strong passwords.
(A) reactive password checking (B) proactive password checking
(C) computer-generated password (D) user education（使用者教育）

37. A _____ strategy is one in which the system periodically runs its own password cracker to find guessable passwords.
(A) user education (B) proactive password checking
(C) reactive password checking（反應式密碼檢查） (D) computer-generated password

38. The most common means of human-to-human identification are _____.
(A) facial characteristics（臉部特徵） (B) signatures
(C) retinal patterns (D) fingerprints

39. _____ systems identify features of the hand, including shape, and lengths and widths of fingers.
(A) Signature (B) Hand geometry（手部幾何特徵）
(C) Fingerprint (D) Palm print

40. Each individual who is to be included in the database of authorized users must first be _____ in the system.
(A) verified (B) authenticated (C) identified (D) enrolled（註冊）

41. To counter threats to remote user authentication, systems generally rely on some form of _____ protocol.
(A) eavesdropping (B) Trojan horse
(C) challenge-response（挑戰與回應） (D) denial-of-service

42. A _____ is when an adversary attempts to achieve user authentication without access to the remote host or to the intervening communications path.
(A) client attack（客戶端攻擊） (B) eavesdropping attack
(C) host attack (D) Trojan horse attack

43. A _____ is directed at the user file at the host where passwords, token passcodes, or biometric templates are stored
(A) eavesdropping attack（竊聽攻擊） (B) denial-of-service attack
(C) client attack (D) host attack

44. A _____ attack involves an adversary repeating a previously captured user response.
(A)client (B) replay（重播） (C)Trojan horse (D) eavesdropping

45. An institution that issues debit cards to cardholders and is responsible for the cardholder's account and authorizing transactions is the _____.（§3.8,pp.122）
(A) cardholder (B) auditor (C) issuer（發行者） (D) processor

46. _____ allows an issuer to access regional and national networks that connect point of sale devices and bank teller machines worldwide.（§3.8,pp.122）
(A) **EFT** (B) POS (C) BTM (D) ATF

47. _____ implements a security policy that specifies who or what may have access to each specific system resource and the type of access that is permitted in each instance.
(A) Audit control (B) Resource control
(C) System control (D) Access control（存取控制）

48. _____ is verification that the credentials of a user or other system entity are valid.
(A) Adequacy (B) Authentication（認證） (C) Authorization (D) Audit

49. _____ is the granting of a right or permission to a system entity to access a system resource.
(A) Authorization（授權） (B) Authentication (C) Control (D) Monitoring

50. _____ is the traditional method of implementing access control.（§4.1,pp.131）
(A) MAC (B) RBAC (C) DAC（自由選定存取控制） (D) MBAC

51. _____ controls access based on comparing security labels with security clearances. （§4.1,pp.131）
(A) MAC（強制存取控制） (B) DAC (C) RBAC (D) MBAC

52. A _____ is an entity capable of accessing objects.
(A) group (B) object (C) subject（主體） (D) owner

53. A(n) _____ is a resource to which access is controlled.
(A) object（客體） (B) owner (C) world (D) subject

54. The final permission bit is the _____ bit which restricts a file can only be deleted by its owner.
(A) superuser (B) kernel (C) set user (D) sticky（沾粘）

55. _____ is based on the roles the users assume in a system rather than the user's identity.
(A) DAC (B) RBAC（基於角色的存取控制）
(C) MAC (D) URAC

56. A _____ is a named job function within the organization that controls this computer system.
(A) user (B) role（角色） (C) permission (D)session

57. _____ provide a means of adapting RBAC to the specifics of administrative and security policies in an organization.
(A) Constraints（限制） (B) Mutually Exclusive Roles (C) Cardinality (D) Prerequisites

58. _____ refers to setting a maximum number with respect to roles.
(A) Cardinality（基數） (B) Prerequisite (C) Exclusive (D) Hierarchy

59. Subject attributes, object attributes and environment attributes are the three types of attributes in the _____ model.
(A) DSD (B) RBAC (C) ABAC（基於屬性的存取控制） (D) SSD

60. The _____ component deals with the management and control of the ways that entities are granted access to resources.（§4.7,pp.157）
(A) resource management (B) access management（存取管理）
(C) privilege management (D) policy management

61. A(n) _____ is a structured collection of data stored for use by one or more applications.
(A) attribute (B) database（資料庫） (C) tuple (D) inference

62. The basic building block of a _____ is a table of data, consisting of rows and columns, similar to a spreadsheet.
(A) relational database（關聯式資料庫） (B) query set
(C) DBMS (D) perturbation

63. In relational database parlance, the basic building block is a _____, which is a flat table.
(A) attribute (B) tuple (C) primary key (D) relation（關聯）

64. In a relational database rows are referred to as _____.
(A) relations (B) attributes (C) views (D) tuples（值組）

65. A _____ is defined to be a portion of a row used to uniquely identify a row in a table.
(A) foreign key (B) query (C) primary key（主鍵） (D) data perturbation

66. A _____ is a virtual table.
(A) tuple (B) query (C) view（檢視表） (D) DBMS

67. A(n) _____ is a user who has administrative responsibility for part or all of the database.
(A) administrator（管理員） (B) database relations manager
(C) application owner (D) end user other than application owner

68. An end user who operates on database objects via a particular application but does not own any of the database objects is the _____.
(A) application owner (B) end user other than application owner（非應用擁有者的終端使用者）
(C) foreign key (D) administrator

69. _____ is the process of performing authorized queries and deducing unauthorized information from the legitimate responses received.
(A) Perturbation (B) Inference（推理） (C) Compromise (D) Partitioning

70. A _____ is the portion of the data center that houses data processing equipment.
(A) computer room（主機房） (B) main distribution area
(C) entrance room (D) horizontal distribution area

71. _____ houses cross-connects and active equipment for distributing cable to the equipment distribution area.
(A) Main distribution area (B) Equipment distribution area
(C) Horizontal distribution area（水平分佈區域） (D) Zone distribution area

72. _____ encompasses intrusion detection, prevention and response.
(A) Intrusion management（入侵管理） (B) Security assessments
(C) Database access control (D) Data loss prevention

73. _____ is an organization that produces data to be made available for controlled release, either within the organization or to external users.
(A) Client (B) Data owner（資料擁有者） (C) User (D) Server

74. _____ is an organization that receives the encrypted data from a data owner and makes them available for distribution to clients.
(A) User (B) Client (C) Data owner (D) Server（伺服器）

75. What are the three main categories of SQLi attack?
(A) **out-of-band** (B) **inferential** (C) **inband** (D) online