

Q36. Which of the following is a direct result of SQL injection to a company's web server?

- a) Data packets to and from the web server are modified.
- b) Data that is on the web server but is not accessible via the web application is retrieved or modified.
- c) Every key stroke a user makes in the network is captured.
- d) The IP headers of packets in the network are captured and modified.

Q37. Which of the following is a program that is designed to block access to a computer or encrypt most of the data on that computer until a sum of money is paid?

- a) Adware b) Ransomware c) Rootkit d) Spyware

Q38. In a PKI system, which of the following is an algorithm that creates a key pair?

- a) Hashing algorithm
- b) Key generation algorithm
- c) Signature verification algorithm
- d) Signing algorithm

Q39. Which of the following is an appropriate description of a command and control (C&C) server?

- a) A computer controlled and used by an attacker to send commands to other compromised computers
- b) A computer on a cloud service used to securely control the movement of data between on-premise storage and cloud storage using encrypted communication
- c) A computer used to control the authentication of all users and computers in an organization
- d) A computer used to control the distribution of processing among different computers in a high-performance computing environment, so that processing is not affected by cyber attacks

Q40. Which of the following is an appropriate description of an advanced persistent threat (APT)?

- a) It is a malware attack that keeps recreating malicious files even after repeated deletions.
- b) It is an attack that uses sophisticated techniques and goes undetected over a long time, e.g., months or years.
- c) It is an attack using malware in computer BIOS, affecting multiple operating systems on a computer that allows multi-booting.
- d) It is an attack using malware that disables all of a company's computers and is difficult to delete.

Q41. Which of the following is an appropriate description of footprinting in computer security?

- a) Digital forensic analysis to find the hacker after a hacking incident
- b) Gathering information about an organization and its systems in preparation for an attack
- c) Listing all affected files in the system in order to assess the impact of an attack
- d) Setting up an intrusion detection system in order to detect when an attacker breaks into the internal network

Q42. Which of the following is an appropriate combination of definitions I through IV for authenticity and reliability in ISO/IEC 27000:2018 (Information security management systems – Overview and vocabulary)?

[Definitions]

I Property of consistent intended behavior and results

II Property that an entity is what it claims to be

III Property of being accessible and usable on demand by an authorized entity

IV Property that information is not made available or disclosed to unauthorized individuals, entities, or processes

	Authenticity	Reliability
a)	I	III
b)	II	I
c)	II	IV
d)	IV	I

Q43. When a mirror port is prepared to allow a LAN analyzer to be used for measurement in order to investigate the cause of a network failure, which of the following is a point to consider?

- a) In preparation for a failure, it is necessary to inform network users of the storage location and usage method about the LAN analyzer.
- b) Since LAN cables must be temporarily disconnected during measurement, it is necessary to give network users advance notice of the measurement date and time.
- c) Since the LAN analyzer can display the packets that pass through the network, it is necessary to pay attention to misuse or abuse, such as wiretapping.
- d) Since the LAN analyzer disposes of packets, it is necessary to restrict the use of the non-target computers during measurement.

Q44. There is a network that is divided into three (3) segments, namely an external segment, a DMZ, and an internal segment, by one (1) firewall. In this network, a service for users is published on the Internet using a system comprising a web server and a database server that contains critical data. Which of the following is the most appropriate server installation method for protecting critical data from unauthorized access via the Internet? Here, the web server performs front end processing for the database server, and the firewall allows only a specific protocol for communication between the external segment and the DMZ as well as between the DMZ and the internal segment. Direct communication between the external segment and the internal segment is not allowed.

- a) The web server and the database server are installed in the DMZ.
- b) The web server and the database server are installed in the internal segment.
- c) The web server is installed in the DMZ and the database server is installed in the internal segment.
- d) The web server is installed in the external segment and the database server is installed in the DMZ.

Q45. Which of the following is a system or network that is intentionally made vulnerable in order to investigate the behavior of an intruder or malware?

- a) Botnet b) DMZ c) Honey pot d) SIEM

Q36. Which of the following properties for information security defined in ISO/IEC 27000:2018 refers to a guarantee that the message data received is the same as the message data sent?

- a) Availability
- b) Confidentiality
- c) Integrity
- d) Non-repudiation

Q37. Which of the following is an example of ransomware?

- a) A range of different types of software including adware, spyware, and freeware
- b) Malicious software blocking access to a victimized computer and demanding money to unblock it
- c) Software that assigns randomized MAC addresses to PCs to ensure user privacy on the Internet
- d) Software that generates random numbers needed by computer security application software

Q38. A typical example of security threats is information leakage when a sender sends data containing important information to a receiver. Which of the following is the most appropriate measure to prevent information leakage?

- a) The data is encrypted with a private key before being sent to the receiver via email. In a separate email, the private key is sent to the receiver so that the receiver can decrypt the data.
- b) The data is password-locked, and it is attached in an email that includes the password in the text part of the email. Before the email is sent, the receiver address is checked to make sure that the email is sent to the correct address.
- c) The receiver creates a pair of public/private keys and sends the public key to the sender. The data is encrypted with the public key and sent to the receiver via email. The receiver then decrypts the data with the private key.
- d) The sender compresses the data on a USB memory as much as possible before giving the USB memory to the receiver so that the receiver can utilize the rest of the memory space effectively.

Q39. Which of the following is a type of malware that embeds itself within a program and inserts its copy into other programs?

- a) Backdoor b) Trojan horse c) Virus d) Worm

Q40. According to ISO/IEC 27000:2018 (Information security management systems - Overview and vocabulary), which of the following is the definition of “level of risk”?

- a) Magnitude of a risk expressed in terms of the combination of consequences and their likelihood
- b) Terms of reference for evaluating the significance of a risk
- c) The priority order assigned to the risks to be handled
- d) Weakness of an asset or control that can be exploited by threats

Q41. Which of the following is dynamic analysis of malware?

- a) Malware is identified by calculating the hash value of the subject for analysis and cross-checking it against a list of known malware hash values that are registered in an online database.
- b) On the basis of the file extensions and content of file headers on a hard disk, malicious program files with false extensions are detected.
- c) The subject for analysis is extracted from communication data on a network and reverse compiled, and the functions of the subject for analysis are investigated from the code obtained.
- d) The subject for analysis is run in a sandbox, and its behavior and external communication are observed.

Q42. Which of the following technologies is the most suitable to divide the whole company network into networks by department?

- a) DMZ (DeMilitarized Zone)
- b) NAT (Network Address Translation)
- c) VLAN (Virtual Local Area Network)
- d) VPN (Virtual Private Network)

Q43. An SQL injection attack caused the SQL statement below to be executed. Which of the following does the SQL statement do? Here, the accounts table contains account information in each row.

```
SELECT * FROM accounts WHERE username='1' or '1'='1'; DROP TABLE accounts;
```

- a) It creates a new user '1'.
- b) It creates a pop-up box that shows the first username in the “accounts” table.
- c) It selects all the records in the “accounts” table and deletes the “accounts” table from the database.
- d) It selects one record from the “accounts” table and drops the rest of the records in the table.

Q44. To provide a guarantee to its online customers that all credit card information is protected when transferred between their PC and the web service over public networks, which of the following technologies should be used?

- a) S/MIME b) SSH c) TLS d) VPN

Q34. Which of the following is classified as a web beacon?

- a) A potential error of an application program used for a website
- b) A technique to collect user information, such as access trends, by embedding a small image in a web page
- c) A virus that is downloaded from a website that deletes image files on a PC
- d) An abusive method of using a malicious script that is harmful to both client PC and web server

Q35. When risk treatment is classified as risk avoidance, risk reduction, risk acceptance, and risk sharing, which of the following risk treatments is risk avoidance?

- a) Applying appropriate controls to lower a risk
- b) Discontinuing some operations that have a risk
- c) Knowingly and objectively not taking any action on a risk
- d) Transferring a risk to other parties

Q36. Which of the following is installed into an in-house network or server by an intruder to enter through an access path other than the normal path?

- a) Backdoor
- b) Forensic
- c) Strict routing
- d) Thin client agent

Q37. Biometric authentication includes a verification method that extracts physical characteristics and another verification method that extracts behavioral characteristics. Which of the following is the method that uses behavioral characteristics?

- a) Performing authentication by extracting characteristics from pen speed and pressure when a signature is provided
- b) Performing authentication by extracting characteristics from the bifurcation angle of the bifurcation point of a blood vessel or from the distance between adjacent bifurcation points
- c) Performing authentication by extracting the characteristic point called minutia from the pattern formed by ridges
- d) Performing authentication by extracting the characteristics of chaotic wrinkles in the eye from the pupil to the outside

Q38. Which of the following is an encryption method that can be used for encrypting data managed in a database using the same key for encryption and decryption?

- a) AES b) PKI c) RSA d) SHA-256

Q39. A given application only has the functions of retrieving and displaying user information from a database that stores such information. Considering information security management, which of the following is the appropriate database access right assigned to an account that the application uses when it accesses the database? The names and scopes of rights are listed below.

[The names and scopes of rights]

Reference right:	Permits a record to be selected
Update right:	Permits a record to be inserted, updated, and dropped
Administrator right:	Permits a table to be displayed, created, altered, and dropped

- | | |
|------------------------|-------------------------------------|
| a) Administrator right | b) Reference right |
| c) Update right | d) Update right and reference right |

Q40. A cybersecurity incident response plan is defined as a set of instructions to aid the cybersecurity team to detect, respond to, and recover from cybersecurity incidents. The cybersecurity incident response plan resolves issues, such as cybercrime, data loss, and service outages that threaten daily work. Which of the following is part of the cybersecurity incident response plan?

- a) Attacking systems with scripts
- b) Containment
- c) Social engineering activities
- d) Stealing user credentials

Q41. Between a client and web server, which of the following is used for inspecting the data that is sent from the client to the web server and blocking attacks, such as SQL injections?

- a) Cluster configuration
- b) Load balancing function
- c) SSL-VPN function
- d) WAF

Q42. Which of the following is an appropriate description of SSH?

- a) It cannot use public key pairs, and it uses a password for authentication.
- b) It helps in securely loading web site pages over HTTPS.
- c) It provides a secure channel for server maintenance over a public network.
- d) Its use is required in the Intranet.

Q43. Which of the following is an appropriate description concerning Sender Policy Framework (SPF) for email communication?

- a) It is a policy of the public relations department to designate a specific person to send emails.
- b) It is an email sent from a spoofed email address without authorization.
- c) It matches the sender mail server IP address with the information from the domain server and accepts or rejects email.
- d) It sends an email to the address of a specific person instead of sending them to multiple email addresses.

Q44. Which of the following is an appropriate explanation of OP25B for email communication?

- a) Blocking communication to port 25 to reduce mass-scale delivery of spam or junk emails
- b) Blocking emails that are sent to more than 25 recipients at once due to organizational policy
- c) Blocking Simple Mail Transfer Protocol (SMTP) communication except those sent to port 25
- d) Blocklisting email addresses that send spams by monitoring email communication to port 25

Q34. Which of the following is an Internet standard that extends the format of email header fields to handle not only text messages but also audio and image files?

- a) HTML b) MHS c) MIME d) SMTP

Q35. Which of the following attacks is classified as DNS cache poisoning?

- a) False domain information is injected into the DNS server that is referenced by a PC, and it leads the user to a fake server.
- b) The version information of the DNS server software is obtained to identify a security hole.
- c) To interrupt the target service, the attacker uses the DNS server as a steppingstone to send a large number of recursive queries.
- d) To obtain internal information, the zone information stored in the DNS server is compiled and transferred.

Q36. Which of the following is a type of public-key cryptography that utilizes the difficulty of factorizing extremely large numbers into primes?

- a) AES b) DH c) DSA d) RSA

Q37. Which of the following is appropriate conduct for a white-hat hacker?

- a) Breaking into a system and changing one of the files without permission and reporting the weaknesses to the owner
- b) Breaking into a system to analyze its vulnerabilities with the owner's permission and within the prescribed rules of engagement
- c) Logging into a system to show fellow hackers real-life examples of deleting a file without the owner's permission
- d) Looking at secret data on a system with the motivation of personal or financial objectives, protest, or espionage

Q38. Which of the following is an appropriate explanation of an SQL injection attack?

- a) It is an attack in which a command for performing a malicious query or operation is entered in the website where there is a vulnerability in a web application to acquire or falsify data without authorization.
- b) It is an attack in which a commercial DBMS vulnerability is exploited to search the host database server and cause repeated infections in order to cause a sudden rise in Internet traffic.
- c) It is an attack in which a malicious script is executed on the visitor's web browser by sending the malicious code to the website displaying the visitor's input data.
- d) It is an attack in which a website visitor is made to view a web page containing an embedded malicious script, and the visitor is then made to perform an unintentional operation on another website.

Q39. Which of the following is an appropriate use of a private key for a digital signature?

- a) The recipient can use the private key to restore an encrypted message to its original status.
- b) The sender can use the private key to create a signature and attach it to a message, and the recipient can confirm the sender.
- c) The sender can use the private key to encrypt a message with an attached fixed string, and the recipient can identify sections that are falsified.
- d) The sender can use the private key to encrypt a message, and the content of the message cannot be understood by unrelated parties.

Q40. Which of the following is a characteristic of a worm, as compared with a Trojan horse?

- a) Arbitrarily encrypting files so that they cannot be read normally
- b) Causing an infection to spread by itself by using the network and removable media
- c) Performing an unauthorized action as an individual program
- d) Waiting without performing any activity until a specific condition is established

Q41. Which of the following is an appropriate explanation of CSIRT?

- a) It is a generic term for an organization that is established within a company, organization, or government agency, and it receives reports on information security incidents for investigation and response.
- b) It is a generic term for people or an organization whose aim is to achieve a religious or political goal by utilizing IT.
- c) It is an organization that creates technical documents concerning the Internet, and it investigates standardization issues.
- d) It is an organization that defines the IP-address allocation policy. It operates and monitors DNS root servers and coordinates DNS management and other such matters on a global scale.

Q42. There is a network that is divided into three (3) segments (i.e., external segment, DMZ, and internal segment) by one (1) firewall. In this network, a service for users is to be made available over the Internet by using a system comprising a web server and a database server containing important data. Which of the following is the most appropriate method of server installation that can protect important data from unauthorized access from the Internet? Here, only a specific protocol is allowed for communications between the external segment and the DMZ, and between the DMZ and the internal segment by the firewall. Direct communication between the external segment and the internal segment is not allowed.

- a) Installation of the web server and database server in the internal segment
- b) Installation of the web server and the database server in the DMZ
- c) Installation of the web server in the DMZ and the database server in the internal segment
- d) Installation of the web server in the external segment and the database server in the DMZ

Q43. Which of the following is a purpose of using a port scanner during an inspection of a web server?

- a) Detecting the vulnerability of contents by logging in with a valid user ID and directly checking the contents of the web server
- b) Detecting unauthorized use by analyzing the access history of the web server
- c) Ensuring that no unnecessary service is operating by enumerating services on the web server
- d) Ensuring that there is no deviation from the information-security policy by checking the management status of the web-server user IDs with the operator

Q36. Which of the following is an attack using a trial-and-error method to obtain confidential information such as a user password or personal identification number (PIN)?

- a) Brute force
- b) Denial of service
- c) Man-in-the-middle
- d) Sniffing

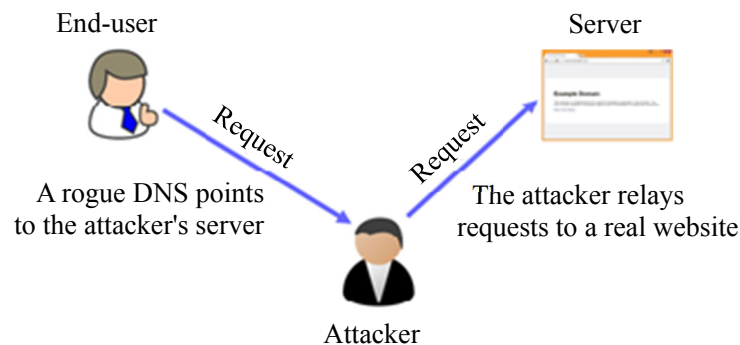
Q37. Which of the following is an appropriate description of clickjacking?

- a) An attacker gains remote control of the mouse of a computer and maliciously operates the computer.
- b) An attacker misleads the user to interact with a user interface and to perform unintended operations.
- c) An attacker remotely locks the mouse pointer to prevent the user from moving the pointer anymore.
- d) An attacker removes the mouse device driver of the system so that the user cannot stop doing malicious actions.

Q38. Which of the following activities targets the DHCP server and exhausts all its available IP address pool so that it cannot provide any IP addresses to its clients?

- a) DHCP MAC filtering
- b) DHCP snooping
- c) DHCP spoofing
- d) DHCP starvation

Q39. Man-in-The-Middle (MITM) attack means the attacker intercepts and alters the communication between the end-user (victim) and the server, which is shown below. In an MITM attack, when the victim sends packets to the server, the attacker receives the packets and then forwards them to the server while the server sends the packets to the victim via the attacker. In this communication channel, which of the following is the appropriate description concerning the MITM attack?



- a) The attacker always uses the server IP during the communication and never uses the victim's IP.
- b) The attacker always uses the victim's IP during the communication and never uses the server's IP.
- c) The attacker always uses the victim's IP during the communication with the server and always uses the server IP during the communication with the victim.
- d) The attacker always uses the victim's IP during the communication with the victim and always uses the server IP during the communication with the server.

Q40. Which of the following is the result when person A sends an e-mail that is encrypted by person B 's public key to person B and person C ? Here, these three persons have the public keys of all three persons, and all of them have their own private keys.

- a) Both B and C can decrypt the encrypted e-mail using B 's public key.
- b) Both B and C can decrypt the encrypted e-mail using their own private keys.
- c) Only B can decrypt the encrypted e-mail using A 's public key.
- d) Only B can decrypt the encrypted e-mail using B 's own private key.

Q41. Which of the following is a package of unauthorized programs and tools that have functions such as creating a back door on a server and hiding the evidence of intrusion inside a server?

- a) RFID b) Rootkit c) TKIP d) Web beacon

Q42. Which of the following is the most appropriate countermeasure against cross-site scripting (XSS) attacks?

- a) Avoiding running a program received in an e-mail from an unknown sender
- b) Closing all unnecessary ports apart from standard web server ports
- c) Filtering out the input that can be interpreted as a script
- d) Using HTTPS instead of HTTP as the default protocol on the web server

Q43. Which of the following is a method to prevent damage caused by an SQL injection attack?

- a) Preventing input characters from being interpreted as characters that have a special meaning in querying or manipulating data in a database
- b) Rejecting any input that contains a character string that specifies a higher-level directory (../)
- c) Rejecting any input whose total length exceeds the limit
- d) Replacing an HTML tag with another character string that is not interpreted as an HTML tag if any input contains an HTML tag

Q44. Which of the following is the network security tool that is usually deployed by a network or system administrator and presents itself as a target machine trying to lure attackers to observe their behavior and attack methodology without harming other systems?

- a) Honeypot
- b) Logic analyzer
- c) Protocol analyzer
- d) Rootkit

Q45. SSL/TLS is the industry-standard security technology creating encrypted connections between a web server and a web browser. This is used to maintain data privacy and to protect the information in online transactions. The steps for establishing an SSL/TLS connection are randomly listed as follows:

1. The web server sends a copy of its SSL/TLS certificate to the web browser.
2. SSL/TLS encrypted communication takes place between the web browser and the web server.
3. The web server sends the web browser an acknowledgment to start an SSL/TLS encrypted connection.
4. The web browser checks if the SSL/TLS certificate is trustworthy or not. If it is trustworthy, then the web browser sends a message to the web server requesting to establish an encrypted connection.
5. A web browser tries to connect to the web server secured with SSL/TLS.

Which of the following is the correct step sequence?

- a) 1 → 5 → 2 → 3 → 4
- b) 1 → 5 → 4 → 3 → 2
- c) 5 → 1 → 2 → 3 → 4
- d) 5 → 1 → 4 → 3 → 2

Q46. Which of the following is an appropriate description of a UML use case diagram?

- a) It shows the behavior that occurs during object life cycle using finite state transitions.
- b) It shows the exchange of messages among objects, and message transmissions and object lifelines in a time series.
- c) It shows the flow from one activity to another activity in systems and work.
- d) It shows the scenarios for what the system will do, from the point of view of actors (i.e., external users or machines).

Q37. Which of the following is an attack that threatens the “integrity” of information?

- a) A DoS attack by which the system is set to an overloaded state
- b) Falsification of a web page
- c) Tapping of communication content
- d) Unauthorized copying of data saved in a system

Q38. Which of the following is the purpose of using a message digest in a message authentication code?

- a) To check the encryption method of a message
- b) To check the overview of a message
- c) To confirm that there is no falsification of a message
- d) To secure the confidentiality of a message

Q39. Which of the following is a role that a PKI certification authority performs as a reliable third party?

- a) Allocating a digital signature to an e-mail body as requested by a user
- b) Enabling the synchronization of time by returning an accurate time to a user's request
- c) Issuing a digital certificate that certifies the private key of a user or server
- d) Issuing a digital certificate that certifies the public key of a user or server

Q40. Which of the following is a description of a directory traversal attack?

- a) By specifying a file including the path name, the attacker illegally reads an unauthorized file.
- b) The attacker enters database command statements as input data for a web application and executes unexpected SQL statements.
- c) The attacker guides a user to a website, where vulnerability in the escape processing of HTML output by a web application can be exploited, and then executes a malicious script on the user's browser.
- d) The attacker illegally obtains the session ID of a user who has logged into a session managed by a session ID, and then accesses the server by spoofing the identity of the user.

Q41. In ISO/IEC 27000:2018 (Information Security Management Systems – Overview and Vocabulary), which of the following is defined as the “property that an entity is what it claims to be”?

- a) Accountability
- b) Authenticity
- c) Nonrepudiation
- d) Reliability

Q42. Which of the following is the purpose of port scanning when an attacker intrudes into the system?

- a) To investigate if evidence of attack remains in the system log at the post-processing stage
- b) To investigate if there is a service that can be attacked at the preliminary investigation stage
- c) To investigate if there is an account whose privileges can be deprived at the privilege acquisition stage
- d) To investigate if there is user information that is beneficial to the attacker at the performance stage of a fraudulent act

Q43. Which of the following is a description that corresponds to two-factor authentication?

- a) Authentication is performed by two (2) different passwords.
- b) Authentication is performed by using a password that contains two (2) different types of special characters.
- c) Authentication is performed by using the fingerprints of two (2) fingers.
- d) Authentication is performed by using the iris and a password.

Q44. Which of the following is the combination of processes that constitutes risk assessment?

- a) Risk analysis, risk evaluation, and risk response
- b) Risk analysis, risk response, and risk acceptance
- c) Risk identification, risk analysis, and risk evaluation
- d) Risk identification, risk evaluation, and risk acceptance

Q45. Which of the following is the malware that is used to gain unauthorized privileged access, to hide its own presence, and to perform malicious activities in a computer system?

- a) Botnet b) Ransomware c) Rootkit d) Security hole

Q46 Which of the following is a method for preventing an SQL injection attack?

- a) If an input text contains HTML tags, replacement of these tags with other character strings that are not interpreted as HTML tags
- b) Nonacceptance of an input text if the overall length of the text exceeds the limit
- c) Nonacceptance of an input text that contains a character string that specifies a higher-level directory (. . /)
- d) Preventing input characters from being interpreted as characters that have a special meaning in an inquiry or operation on the database

Q36. The IP address of Server *X* prepared by an attacker was stored in a DNS cache server of Company *B* as the IP address corresponding to the FQDN of the web server of Company *A*. Which of the following users will be unintentionally guided to Server *X* because of this attack? Here, each employee of Company *A* and Company *B* performs name resolution by using the DNS cache server of his/her own company.

- a) An employee of Company *A* who wishes to access the web server of Company *A*
- b) An employee of Company *A* who wishes to access the web server of Company *B*
- c) An employee of Company *B* who wishes to access the web server of Company *A*
- d) An employee of Company *B* who wishes to access the web server of Company *B*

Q37. Which of the following is a description of a directory traversal attack?

- a) An attacker enters data consisting of database command statements as the input data for a web application and forces the execution of SQL statements that are not intended by the administrator.
- b) An attacker guides a user to a web site, where a defect in the escape processing of the HTML output by a web application is exploited, and forces the execution of a malicious script on the user's web browser.
- c) An attacker illegally obtains the session ID for a user, who has logged into a session managed by the session ID, and accesses the server by spoofing the identity of the user.
- d) An attacker specifies a file by using the path name and illegally views a file that is not intended for viewing by the administrator.

Q38. Which of the following is a description of a brute force attack by which an attempt is made to find the key of private key cryptography?

- a) Finding the key by observing the ciphertext change when the plaintext is changed by a certain amount
- b) Finding the key by testing all key combinations sequentially when a set of plaintext and ciphertext is given
- c) Finding the key by using as a clue the algebraic expression representing the relationship between the plaintext, ciphertext, and key
- d) Finding the key by using as a clue the statistical correlation between a part of the information of the plaintext and part of the information of the ciphertext

Q39. Which of the following is an explanation of the time stamp service in information security?

- a) It is a service that authenticates biometric information, such as fingerprint, voice print, vein patterns, retina, and iris, by using the date and time when the information is registered in the authentication system.
- b) It is a service that certifies that electronic data certainly exist on a particular date and time and that the data have not been falsified since that date and time.
- c) It is a service that securely notifies that the date and time information is not falsified midway for setting the clock of the PCs and servers on the network.
- d) It is a web service that securely displays the global date and time information used in the official records by using encrypted communication.

Q40. Which of the following is an encryption algorithm for public key cryptography?

- a) AES b) KCipher-2 c) RSA d) SHA-256

Q41. Which of the following is a security attack that prevents users from accessing their accounts?

- a) Brute force b) Denial of Service c) Man in the middle d) Sniffing

Q42. Which of the following is an appropriate description of a botnet?

- a) A collection of internet-connected devices, including IoT devices, infected and controlled by a common type of malware
- b) A scalable and reliable network of self-driving vehicles communicating with each other to avoid accidents/collisions
- c) A set of honeypots designed to detect and analyze malicious activities by hackers to secure the production systems in the future
- d) A wireless network for industrial robots created for collaborative manufacturing in a factory to ensure quality at all levels

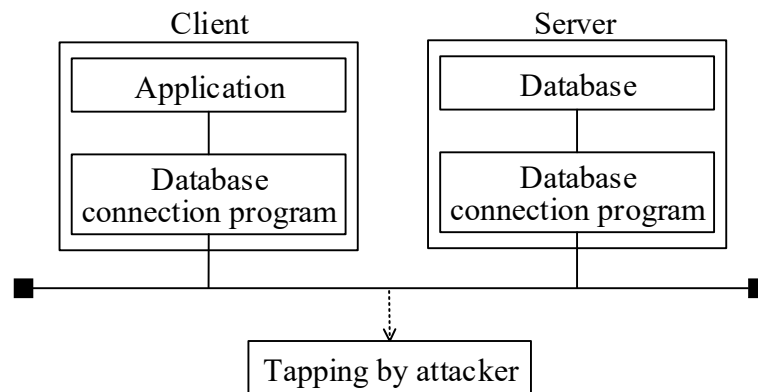
Q43. An attacker captures unencrypted network traffic with a tool and later analyzes it offline to learn about the information contained in those transmissions. Which of the following is this attack?

- a) Buffer overflow attack
- b) Phishing attack
- c) Smurf attack
- d) Sniffing attack

Q44. Which of the following is the technique of actually attempting an attack and intrusion on a system to detect the security-related vulnerabilities of a computer or network?

- a) Penetration test
- b) Regression test
- c) Software inspection
- d) Walk-through

Q45. As shown in the figure below, an application on a client accesses the data of the database on a server via database connection programs. Which of the following is a measure for preventing the leakage of the commands and execution results transmitted between the application and database?



- a) Changing the port number from its initial value that the database connection programs use for communication in the database management system
- b) Encrypting the communication between the database connection programs
- c) Restricting the IP addresses of the clients that can access the database connection program on the server to only those that are required
- d) Setting a password for starting or stopping the database connection program on the server

Q37. Which of the following is a password attack that makes use of the possible combination of pre-computed hashes and passwords?

- a) Brute force attack
- b) Malware attack
- c) Rainbow table attack
- d) Zero-day attack

Q38. Which of the following is a spoofing attack?

- a) An attack by encrypting victim's data and demanding ransom
- b) An attack by looking at someone's keyboard while the victim entering a password
- c) An attack by masquerading as someone such as a superior person from an information systems department, or customer
- d) An attack by sending excessive requests from multiple computers in an attempt to overload the victim's computer

Q39. An administrator captures network packets and discovers that hundreds of ICMP packets have been sent to the host. However, it is not a particularly busy time of the day. Which of the following is the most likely the attack executed against the computer in this situation?

- a) Denial of service
- b) Man-in-the-middle
- c) Spoofing
- d) Worm

Q40. Which of the following is a description of spyware?

- a) A program that attempts to identify a user's password by accessing a server and trying to match with all the words in a dictionary
- b) A program that extracts HTML tags, JavaScript, and SQL statements in the input data from input forms on a website, and rewrites them to other character strings in order to eliminate malicious input to a website
- c) A program that is installed on a PC against the user's intention and collects information such as the user's personal information and access history
- d) A program that sequentially accesses TCP ports of a server from an attacker's PC in order to find a vulnerable port that can be a point of intrusion to the server

- Q41.** A security question is used to authenticate a user who forgets his/her password for a web system. After the correct answer is given, which of the following is the most appropriate process in terms of security?
- a) Making the user enter an e-mail address again, and sending a URL that is difficult to guess so that the user can access a password reset page
 - b) Making the user enter an e-mail address again, and sending the current password to that address
 - c) Sending a URL that is difficult to guess to the user's pre-registered e-mail address so that the user can access a password reset page
 - d) Sending the current password to the user's pre-registered e-mail address

Q42. Which of the following is a role that a PKI certification authority performs as a reliable third party?

- a) It allocates a digital signature to an e-mail body by a user's request.
- b) It enables to synchronize the time by returning an accurate time to a user's request.
- c) It issues a digital certificate that certifies a private key of a user or a server.
- d) It issues a digital certificate that certifies a public key of a user or a server.

Q43. Which of the following is an appropriate description concerning corporate security management when Software as a Service (SaaS) is used?

- a) No system access management needs to be performed, and no consideration concerning the procedure for password initialization or a password policy that satisfies complexity requirements is required.
- b) No system construction needs to be performed, and neither the definition of security requirements for application software development nor the design of storage volume for system logs is required.
- c) No system operation needs to be performed, and no consideration concerning work procedures at the time of a failure or backup is required.
- d) No system security management needs to be performed, and neither the creation of information security management rules nor the assignment of an administrator is required.

Q44. Which of the following is an appropriate description concerning BYOD and the associated information security risk?

- a) An employee takes home an information terminal provided by his or her company and uses it privately, which causes an increase in information security risks such as information leakage.
- b) An employee uses an information terminal provided by his or her company to work while in transit to another location such as a customer office, which causes an increase in information security risks such as shoulder hacking.
- c) An employee uses his or her own personal terminal for business purposes, which causes an increase in information security risks such as virus infections due to inadequate security settings.
- d) An employee uses his or her own personal terminal privately during non-working time such as breaks, which causes an increase in information security risks such as a reduction in awareness of security.

Q45. Between a client and a web server, which of the following is used for inspecting the data that is sent from the client to the web server and blocking attacks such as SQL injection?

- a) Cluster configuration
- b) Load balancing function
- c) SSL-VPN function
- d) WAF

Q46. Which of the following is an appropriate description of honeypots?

- a) Antivirus software to detect and clean or quarantine virus-infected programs
- b) Computer system designed to detect or counteract unauthorized access
- c) Firewall to detect and prevent unauthorized access to computer systems
- d) Security mechanism to run untrusted programs without risking the computer

Q36. Which of the following is a technology that prevents automated input by a program by requiring input of characters from a warped image or an image some parts of which are hidden? The technology is based on the differences of recognition of those images between humans and programs.

- a) CAPTCHA
- b) QR code
- c) Short URL
- d) Trackback ping

Q37. Which of the following is an attack that threatens the “integrity” of information?

- a) A DoS attack which sets the system to an overloaded state
- b) Falsification of a web page
- c) Tapping of communication content
- d) Unauthorized copying of data saved in a system

Q38. Which of the following is the name of an attack where manipulation is made to place a malicious website near the top of the results of a search website?

- a) Cross-site scripting
- b) DNS cache poisoning
- c) SEO poisoning
- d) Social engineering

Q39. Which of the following is an appropriate explanation of a SQL injection attack?

- a) An attack in which a large volume of packets is sent to a website via another website in order to make the provision of services impossible due to the abnormally high network traffic
- b) An attack in which a program is forced to end abnormally, malicious code that is inserted into the data area is executed, or other such actions are performed by reading and writing data beyond the upper or lower limit of an area of memory that is secured for the buffer
- c) An attack in which if there is a defect in the way database is called from a web application, an attacker can perform unauthorized retrieval, modification, and deletion of data in a database by entering a malicious character string in the data manipulation language for the call
- d) An attack in which when a user views a website on which an attacker has placed a trap and clicks a link to another website that has a vulnerability, a character string that contains a malicious script is sent to the linked website, and when the malicious script that is embedded in the response is executed in the user's browser, information leakage occurs

Q40. In an e-commerce transaction that uses public key cryptography, which of the following is the role of a certificate agency (CA)?

- a) To encode plain text with the public keys that are shared between the parties involved in the transaction
- b) To issue digital certificates for the public keys of the parties involved in the transaction
- c) To manage the passwords of the parties involved in the transaction
- d) To manage the private key that is shared between the parties involved in the transaction

Q41. Which of the following is an appropriate purpose of using a hash value in digital forensics?

- a) To convert a password with a one-way function so that recovery is not possible, then store it
- b) To prove the identicalness between the original and the duplicate copy of the data that can be used as evidence
- c) To restore altered data to its original form so that it can be used as evidence
- d) To verify whether password tapping occurred or not

Q42. Which of the following is an appropriate operation for user authentication that uses an IC card and a PIN?

- a) Given that each user can be identified by an IC card, a common PIN is set for all users in order to reduce the management workload.
- b) If an IC card is lost, a new IC card is issued, and after the PIN is reset, the lost IC card is deactivated.
- c) The PIN is set by combining the numeric information imprinted on the surface of the IC card.
- d) When an IC card is delivered, the PIN is not enclosed, but is notified to the user through another channel.

Q43. When malware that has made a successful intrusion into a PC communicates with a command-and-control server on the Internet, which of the following is a reason for using the TCP port number 80 as the destination port in most cases?

- a) Given that this port is used for browsing websites, there is a high probability that communication is allowed by the firewall.
- b) Given that this port is used for browsing websites through HTTPS communication, there is a low probability that this port is detected by an intrusion detection system.
- c) Given that this port is used for the name resolution of a domain name, there is a low probability that this port is detected by an intrusion detection system.
- d) Given that this port is used in a DNS zone transfer, there is a high probability that communication is allowed by the firewall.

Q44. When a normally functioning hard disk of a PC on which confidential files are stored is handed over to an industrial waste disposal vendor, which of the following is an appropriate countermeasure against information leakage?

- a) Changing the filename of each confidential file to a random character string multiple times
- b) Compressing the confidential files multiple times with different compression techniques
- c) Erasing the master boot record of the hard disk multiple times with a specialized erasing tool
- d) Overwriting all areas of the hard disk with a random bit string multiple times

Q35. Which of the following is a form of malware that requires a host in order to propagate from one computer to another?

- a) Trojan horses
- b) Viruses
- c) Worms
- d) Zombies (Bots)

Q36. Which of the following is the term used to describe an attack where attackers exploit a vulnerability of computer systems before a patch fixes the vulnerability?

- a) Backdoor attack
- b) Man-in-the-middle attack
- c) Rootkit attack
- d) Zero-day attack

Q37. Which of the following is an appropriate description of a buffer overflow attack?

- a) An attack that floods the memory area secured by a program by continuously sending long character strings or data to seize access privileges from the program, and causes malfunctions
- b) An attack that fraudulently overwrites cache information
- c) An attack that sends a large amount of data continuously to the target server to place an excessive load on the server's CPU and memory, and obstructs its service
- d) An attack that takes advantage of the vulnerabilities in software before the software vendor can provide a fix for the vulnerability

Q38. A typical example of personal security threats is information leakage. Which of the following is the most appropriate measure to prevent information leakage?

- a) Data containing important information is encrypted with a private key before sending it to the receiver via email. In a separate email, the private key is sent to the receiver so that the receiver can decrypt the data.
- b) Data containing important information is encrypted with the public key received in advance from the receiver before sending it to the receiver via email. The receiver then decrypts the data with the private key that the receiver has created as the pair of public/private keys.
- c) Data containing important information is password-locked, and it is attached in an email that includes the password in the text part of the email. Before sending the email, the receiver address is checked to make sure that the email is sent to the correct address.
- d) Stored data containing important information is compressed as much as possible before giving a USB memory to someone so that the new user can utilize the rest of the memory space effectively.

Q39. When the process shown in the procedure below is performed, in addition to the detection of message falsification, which of the following is what recipient B is able to do?

[Procedure]

Process of sender A

- (1) A hash function is used to generate a digest from a message.
- (2) The digest generated in (1) is encrypted with the sender A 's private key to generate a digital signature.
- (3) The message and the digital signature generated in (2) are sent to recipient B .

Process of recipient B

- (4) The same hash function in the process of sender A is used to generate a digest from the received message.
- (5) The received signature is verified by comparing the digest generated in (4) and the digest generated by decrypting the received digital signature with the sender A 's public key that recipient B received in advance from sender A .

- a) Confirming that the message is from sender A
- b) Detecting wiretapping on the message
- c) Identifying the areas of falsification
- d) Preventing leakage of the message

Q40. Among the techniques for code breaking given below, which of the following is classified as a brute force attack?

- a) By observing the difference between two different items of plain text and their encrypted text, the key is identified.
- b) For a given set of plain text and encrypted text, the key is identified by using all possible combinations.
- c) The encrypted text is decoded by analyzing the electromagnetic waves that an encryption device emits during the operation.
- d) The statistical bias of an encryption function is approximated with a linear function, and the encrypted text is decoded.

Q41. Which of the following is an appropriate terminology concerning the behavior that documents retrieved from distinct origins are isolated from each other?

- a) Clickjacking
- b) Cross-Origin Resource Sharing (CORS)
- c) Cross-Site Request Forgery (CSRF)
- d) Same-Origin Policy

Q42. When a mirror port is prepared to allow a LAN analyzer to be used to investigate the cause of a network failure, which of the following is a point to consider?

- a) In preparation for a failure, it is necessary to inform network users of the storage location and usage method of the LAN analyzer.
- b) Since LAN cables must be temporarily disconnected during measurement, it is necessary to notify network users in advance of the date and time of measurement.
- c) Since the LAN analyzer can display the packets that pass through the network, it is necessary to pay attention to misuse or abuse such as wiretapping.
- d) Since the LAN analyzer disposes of packets, it is necessary to restrict the use of the non-target computers during measurement.

Q43. Which of the following is an appropriate term for an organized and highly skilled team, whose mission is to continuously monitor and improve the organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents with the aid of both technology and well-defined processes and procedures?

- a) Cybersecurity
- b) Incident Management Center (IMC)
- c) Network Operations Center (NOC)
- d) Security Operations Center (SOC)

Q37. Alan would like to send an encrypted message to Bob using an asynchronous encryption scheme. Which of the following must occur before Alan sends the encrypted message to Bob? Here, Alan has already proven to Bob with the digital signature that Alan is the person who sends the message to Bob.

- a) Alan provides his private key to Bob.
- b) Alan provides his public key to Bob.
- c) Bob provides his private key to Alan.
- d) Bob provides his public key to Alan.

Q38. Which of the following is an appropriate term associated with the fraudulent action of impersonating an authorized person?

- a) Destruction b) Falsification c) Spoofing d) Tapping

Q39. An attacker calls a corporate help desk, masquerading as an employee who has lost their password. The help desk staff resets the password to the company default "password1." The attacker then uses this password to access the company network and information in the server. What is this type of attack called?

- a) Buffer overflow attack
- b) Denial-of-Service attack
- c) Shoulder surfing
- d) Social engineering

Q40. A man-in-the-middle attack happens when an attacker intercepts communication and spoofs the identities of either of the two parties involved. How can such an attack be effectively countered?

- a) Such an attack can be countered by a cyclic redundancy check (CRC).
- b) Such an attack can be countered by having an authentication through a digital signature before accepting someone's public key.
- c) Such an attack can be countered by using a parity bit.
- d) Such an attack can be countered by using hashing algorithms.

Q41. Bob and Alice encrypt all of their communications with each other. Because of the high level of sensitivity of the information they are sharing, they have implemented a cryptographic mechanism that offers secrecy to their messages. However, the trade-off of this encryption is that it is impossible for Bob or Alice to be 100% sure that they are communicating with each other, nor can they be 100% certain of the integrity of the content of the messages. Which of the following types of encryption methods are Bob and Alice using?

- | | |
|---------------------------------------|-----------------------------------|
| a) AES (Advanced Encryption Standard) | b) DES (Data Encryption Standard) |
| c) One-time pad | d) Stream cipher |

Q42. A user has just received a file named “image.jpg.” When inspected more closely, it is revealed that the file name is actually “image.jpg .exe,” with spaces between the fake .jpg suffix and the real .exe suffix. Which of the following is the most appropriate term used to describe this type of attack?

- a) Backdoor b) Trojan horse c) Virus hoax d) Worm

Q43. A data backup system must support restoring all transactions until 5 minutes before a disaster happens. What type of goal is this?

- a) Maximum tolerable downtime
- b) Recovery point objective
- c) Recovery time objective
- d) Service level agreement

Q44. Which of the following is an appropriate test to verify the efficacy of security measures by attempting an actual intrusion?

- a) Exception test
- b) Functional test
- c) Penetration test
- d) Stress test

Q45. Which of the following is an appropriate method to prevent a buffer overflow attack?

- a) Performing input filtering and removing browser scripts from all user input on web applications
- b) Performing input filtering and removing structural query language commands from all user input
- c) Performing the boundary check on all integer variables in the program to confirm that the resulting value from each calculation does not exceed the limit of its destination variable
- d) Performing the boundary check on all string variables in the program to confirm that the length of the input string does not exceed the size of the designated variable

Q46. Companies usually provide a means for their mobile workforce to access the corporate network securely over the Internet through insecure channels such as open wireless networks in hotels or coffee shops. Which of the following is the appropriate technology that can be used for this purpose?

- a) DMZ (DeMilitarized Zone)
- b) SNMP (Simple Network Management Protocol)
- c) VoIP (Voice over Internet Protocol)
- d) VPN (Virtual Private Network)

Q36. Which of the following is a secure communication protocol that provides a hybrid cryptosystem where public key cryptography is used to transfer a shared private key securely to the other side, and private key cryptography is used to encrypt subsequent communications for the remaining session?

- a) AES (Advanced Encryption Standard)
- b) RSA
- c) SSL/TLS (Secure Socket Layer/Transport Layer Security)
- d) WAF (Web Application Firewall)

Q37. In a meeting session, the security administrator provides a presentation regarding risks on social media and recommends that the attendees not give unnecessary personal information on social media websites. From which of the following attacks do the social media users effectively reduce the security risk most by following this recommendation?

- a) Brute-force attack
- b) Cognitive password attack
- c) DoS (Denial of Service) attack
- d) Phishing attack

Q38. Which of the following is an appropriate description of a Trojan horse used for security attacks in computing?

- a) It is a brute force attack algorithm.
- b) It is an effective way to detect an intruder.
- c) It is a rogue program that tricks users.
- d) It is a user who steals valuable information.

Q39. Which of the following is an appropriate combination of the usage method of a signature key in a digital signature, and the purpose of a digital signature?

- a) By the sender creating a digital signature with the signature key and attaching it to a message, the recipient can confirm the identity of the sender.
- b) By the sender encrypting a message to which a fixed string is added with the signature key, the recipient can identify sections that have been falsified.
- c) By the sender encrypting a message with the signature key, the content of the message cannot be understood by unrelated parties.
- d) The recipient can use the signature key to decrypt an encrypted message to the plain text message.

Q40. Which of the following is an example of improper use of a key logger?

- a) It interrupts the communication between two parties, and then collects and falsifies the information being exchanged.
- b) When Internet banking is used, it collects the password entered by the user.
- c) When the browser is initiated, it arbitrarily displays a tool bar that the user has not installed.
- d) When the user browses movies on a browser, it arbitrarily displays unintended advertisements for the user.

Q41. Biometric authentication includes a method of authentication by extracting physical characteristics, and a method of authentication by extracting behavior characteristics. Which of the following has behavior characteristics?

- a) Performing authentication by extracting characteristics from the branching angle of the branching point of a blood vessel, and the length between the branching points
- b) Performing authentication by extracting characteristics from the speed of and pressure on a pen when a signature is written
- c) Performing authentication by extracting characteristics of chaotic wrinkles spreading out from the pupil
- d) Performing authentication by extracting the characteristic points called minutiae from the patterns formed by ridge lines

Q42. Which of the following is the most effective method of detecting falsification of the contents of a web server?

- a) Communications to the web server are monitored to ensure that there is no communication other than HTTP and HTTPS.
- b) The hash value of each file of the contents of the web server is stored and periodically compared with the hash value generated from each file.
- c) The memory usage of the web server is checked periodically to ensure that a buffer overflow has not occurred.
- d) The updated date of each file of the contents of the web server is stored and compared periodically with the updated date of each file.

Q43. When a digital certificate has been installed in an in-house system accessed from a smartphone by an employee, which of the following can be checked using the in-house system?

- a) Ensuring that the applications on the smartphone are the latest versions of the applications
- b) Ensuring that the most recent security patch has been applied to the OS of the smartphone
- c) Ensuring that the smartphone has been allowed to access the in-house system
- d) Ensuring that the smartphone is not infected by a virus

Q44. Which of the following is a technique where a system is actually attacked and an intrusion attempt is made in order to detect security-related vulnerabilities of a computer or network?

- a) Penetration test
- b) Regression test
- c) Software inspection
- d) Walk-through

- Q45.** Which of the following can be used to detect worms by using SHA-256 to calculate a hash value from a subject file, and then cross-checking this against a database of hash values from files containing specimens of known worms?
- a) A worm that has the same file size as a worm specimen
 - b) A worm that is in the same subspecies as a worm specimen
 - c) A worm with code strings that have the same characteristics as a worm specimen
 - d) The same worm as a worm specimen

Q39. Which of the following is an appropriate method of authenticating users by using a password?

- a) The hash value of the user ID corresponding to the password is registered, and the password entered during authentication is converted by the hash function and compared.
- b) The hash value of the user ID corresponding to the password is registered, and the user ID entered during authentication is converted by the hash function and compared.
- c) The password is converted to a hash value and registered, and the password entered during authentication is converted by the hash function and compared.
- d) The password is converted to a hash value and registered, and the user ID entered during authentication is converted by the hash function and compared.

Q40. When malware that has made a successful intrusion into a PC communicates with a command-and-control server on the Internet, which of the following is a reason for using the TCP port number 80 as the destination port in most cases?

- a) As this port is used for browsing websites, there is a high probability that communication is allowed by the firewall.
- b) As this port is used for browsing websites through the HTTPS protocol, there is a low probability that this port is detected by an intrusion detection system.
- c) As this port is used for name resolution of a domain name, there is a low probability that this port is detected by an intrusion detection system.
- d) As this port is used in a DNS zone transfer, there is a high probability that communication is allowed by the firewall.

Q41. Which of the following is a technique that is classified as social engineering?

- a) Acquiring a password by calling a user and pretending to be a system administrator
- b) Analyzing a password by using a round-robin attack tool
- c) Entering a system by using software vulnerabilities, such as a buffer overflow
- d) Entering a system from a back door created automatically by a virus infection

Q42. When Mr. *A*, who has a digital certificate, uses an e-mail to place an order with store *B*, he uses his own private key and digitally signs the e-mail. Store *B* then uses Mr. *A*'s public key to confirm the signature. Which of the following can be achieved using this method? Here, only Mr. *A* can use his private key.

- a) It can be confirmed that store *B* is permitted to sell products to Mr. *A*.
- b) It can be confirmed that the order arriving at store *B* is an order from Mr. *A*.
- c) The order details sent from Mr. *A* to store *B* can be prevented from being leaked to third parties.
- d) The order sent from Mr. *A* can be made to arrive at store *B*.

Q43. Which of the following is an appropriate description of risk assessment?

- a) As the purpose of risk assessment is to prevent a future loss, referencing of data used in the past risk assessment is avoided.
- b) Risk assessment is implemented after a risk is identified and the budget for responding to the risk is decided according to the amount of loss.
- c) The implementation of risk assessment is avoided before the response to all risks identified beforehand is complete.
- d) The priority order of the response to risks is determined by the size of the risk based on the expected amount of loss and occurrence probability.

Q44. Which of the following is a description of measures against information leakage?

- a) A checksum is added to the data to be sent.
- b) A copy of the data backup medium is stored at a remote location.
- c) The contents of the hard disk of a notebook PC are encrypted.
- d) The hard disk in which data are stored is mirrored.

Q46. Which of the following is a purpose of using a WAF (Web Application Firewall)?

- a) An attack on a vulnerability attributed to a Web server and a Web application is blocked.
- b) The entry of a worm into a Web server is detected, and the worm is automatically exterminated.
- c) The security hole of a Web server is identified, and an OS security patch is applied.
- d) The vulnerabilities and inconsistencies of a Web application are detected during the integration test of content development of the Web server.

Q47. Which of the following is an explanation of the pattern-matching method used by antivirus software?

- a) A virus is detected by collating information with the checksum of a file.
- b) A virus is detected by comparing a file before and after infection, and examining whether any change has been made to the file.
- c) A virus is detected by monitoring an abnormal phenomenon that is caused by a virus in a system.
- d) A virus is detected through comparison with the signature of an already-known virus.

Q48. Which of the following can be implemented with the functions of HTTPS (HTTP over SSL/TLS)?

- a) Blocking of communication aside from TCP port numbers 80 and 443
- b) Encryption of communication between a Web server and a browser
- c) Restriction of unauthorized access to a Web server through packet filtering in the Network Interface layer
- d) Prevention of an attack on a Web server from an SQL injection

Q36. Which of the following is the most appropriate case example of social engineering?

- a) A person scans for open wireless networks available in his/her home area by using his/her portable computer, and then he/she posts the names and locations of the networks found on the website in order to allow his/her friends to have access to free Wi-Fi networks.
- b) A phone call was made to a helpdesk of a computer center. By using the personal information scavenged from a trash bin, the caller convinces the helpdesk staff that he/she is a legitimate user, in order to have the password initialized and then break into the system.
- c) Advertising messages selling illegal products are sent to an unspecified large number of recipients without prior consent. Even though most recipients ignore or discard the messages, some of them are interested and decide to contact the sender to buy the products.
- d) Although a company's computer network is protected by the firewall, malware is able to spread throughout the company because an employee may unintentionally infect a computer with a virus from his/her personal USB flash memory.

Q37. Which of the following is a purpose of using message digest in a message authentication code?

- a) To check the encryption method of a message
- b) To check the overview of a message
- c) To confirm that there is no falsification of a message
- d) To secure the confidentiality of a message

Q38. Which of the following is an attack that threatens the “integrity” in information security?

- a) A DoS attack by which the system is set to an overloaded state
- b) Falsification of a Web page
- c) Tapping of communication content
- d) Unauthorized copying of data saved in a system

Q39. Which of the following is an explanation of SQL injection?

- a) It is an attack by sending data containing a malicious script to a website where a visitor views the visitor's input data on the screen as it is, and making the script executed in the visitor's browser.
- b) It is an attack where a command for performing a malicious query or operation in the database is entered when there is a problem in a Web application, and the data of the database is modified or acquired without authorization.
- c) It is an attack where a vulnerability of a commercial DBMS (DataBase Management System) is exploited to search the host database server and cause repeated self-infection in order to cause a rapid increase in Internet traffic.
- d) It is an attack where a website visitor is made to view a Web page containing an embedded malicious script, and the visitor is then made to perform an unintentional operation on another website.

Q40. Which of the following is an appropriate operation in user authentication that uses an IC card and PIN?

- a) If an IC card is lost, a new IC card is issued, and after the PIN is reset, the lost IC card is deactivated.
- b) Since each user can be identified by an IC card, a common PIN is set for all users in order to reduce the management workload.
- c) The PIN is set by combining the numeric information imprinted on the surface of the IC card.
- d) When an IC card is delivered, the PIN is not enclosed, but is notified to the user through another channel.

Q41. In a database that manages user information, there exists an application that searches for user information and displays it. In terms of security management, which of the following is an appropriate level of privilege for access to the database to be assigned to this application? Here, the scope of each privilege is as below.

[Scope of privilege]

Reference privilege: Records can be referred to.

Update privilege: Records can be registered, changed, and deleted.

Administrator privilege: Tables can be referenced, registered, changed, and deleted.

- | | |
|---|------------------------|
| a) Administrator privilege | b) Reference privilege |
| c) Reference privilege and update privilege | d) Update privilege |

Q42. When a biometric authentication system is installed, which of the following is the most appropriate point to be considered?

- a) Adjusting the system in consideration of both the probability of incorrectly rejecting an authorized user and the probability of incorrectly accepting an unauthorized user
- b) Combining various measures, such as heuristics, in addition to frequent updates of the pattern file
- c) Getting a reliable third party to issue the digital certificate of the concerned person
- d) Using a library having the function of sanitizing data that may initiate system malfunction

Q43. Which of the following technology is the most suitable to divide the whole company network into the networks by department?

- a) DMZ (DeMilitarized Zone)
- b) NAT (Network Address Translation)
- c) VLAN (Virtual Local Area Network)
- d) VPN (Virtual Private Network)

Q44. When a packet filtering firewall is installed at the point of connection between a company's internal network and the Internet, and PCs on the company's internal network are allowed to access port 80 of Web servers on the Internet, which of the following is an appropriate combination of rules for filtering to grant permission?

a)

Source	Destination	Source Port number	Destination Port number
PC	Web server	80	1024 or more
Web server	PC	80	1024 or more

b)

Source	Destination	Source Port number	Destination Port number
PC	Web server	80	1024 or more
Web server	PC	1024 or more	80

c)

Source	Destination	Source Port number	Destination Port number
PC	Web server	1024 or more	80
Web server	PC	80	1024 or more

d)

Source	Destination	Source Port number	Destination Port number
PC	Web server	1024 or more	80
Web server	PC	1024 or more	80

Q45. There exists an OS that can independently set the reading, writing, or execution rights for a file as the attribute information of the file. One bit is used for each of these three rights to set whether they are permitted or not. When these three bits are set using an octal value from 0 through 7, which of the following is an appropriate description considering the trial results below?

[Trial results]

- (i) When 0 is set, reading, writing, and execution are not permitted.
 - (ii) When 3 is set, reading and writing are permitted, but execution is not permitted.
 - (iii) When 7 is set, reading, writing, and execution are permitted.
-
- a) When 2 is set, reading and execution are permitted.
 - b) When 4 is set, only execution is permitted.
 - c) When 5 is set, only writing is permitted.
 - d) When 6 is set, reading and writing are permitted.

Q37. Which of the following is an appropriate description concerning “HTTP cookie”?

- a) HTTP cookies are created by a web browser and stored in the web server.
- b) HTTP cookies are used to contain data sent from a web server as plain text only.
- c) HTTP cookies can contain executable codes to perform some specific tasks.
- d) HTTP cookies cannot notify the visiting website about user’s previous activities.

Q38. In the context of information security defined by ISO/IEC 27001, which of the following is the property of safeguarding the accuracy and completeness of information assets?

- a) Authentication
- b) Availability
- c) Confidentiality
- d) Integrity

Q39. Which of the following is an appropriate characteristic of MAC (Message Authentication Code) that is used to authenticate a message and provide its integrity in cryptography?

- a) It is calculated by performing polynomial manipulations.
- b) It is constructed from cryptographic hash functions.
- c) It is generated and verified using both private and public keys.
- d) It is used with the receiver's public key to encrypt a message.

Q40. Which of the following is a characteristic of the hash function that is used for a digital signature?

- a) Even if messages are different, the message digests are all the same.
- b) It is difficult to restore an original message from the message digest.
- c) The length of a message digest differs depending on the length of the message.
- d) Two different messages that generate the same message digest are easily obtained.

Q41. Which of the following is the salami technique that is used in computer crime?

- a) It is a technique where data that is being sent or received over a network is illegitimately intercepted.
- b) It is a technique where information that remains in a computer or its surrounding area after the execution of a program is searched to obtain necessary information.
- c) It is a technique where part of a communication line is accessed secretly, and another person's ID and password are stolen and used to steal data.
- d) It is a technique where theft is performed in small increments from many assets so that this fraudulent behavior is not noticed.

Q42. Mr. *X* sends an e-mail to Mr. *Y* by using the Internet. The contents of the e-mail must be kept confidential, so Mr. *X* uses public key cryptography to encrypt the e-mail. Which of the following is the key that is used to encrypt the contents of the e-mail?

- a) Mr. *X*'s private key
- b) Mr. *X*'s public key
- c) Mr. *Y*'s private key
- d) Mr. *Y*'s public key

Q43. Which of the following is the security attack that is used for an illegal attempt to manipulate the people of an organization into divulging the password and confidential information under the pretext of an emergency?

- a) Password cracking
- b) Social engineering
- c) Springboard attack
- d) Trojan horse

Q44. Which of the following is a feature that is incorporated by an attacker to enter the network or server of a company?

- a) Back door
- b) Digital forensics
- c) Strict routing
- d) Thin client agent

Q45. Which of the following is an explanation of BYOD (Bring Your Own Device)?

- a) An employee brings his or her own personal terminal to the office for personal use during non-working time such as breaks, which causes an increase in security risks such as a reduction in awareness of security.
- b) An employee brings his or her own personal terminal to the office to use for work, which causes an increase in security risks such as virus infections caused by inadequate security settings.
- c) An employee takes home an information terminal provided by his or her company and uses it for personal reasons, which causes an increase in security risks such as information leakage.
- d) An employee uses an information terminal provided by his or her company to work while in transit to another location such as a customer office, which causes an increase in security risks such as shoulder hacking.

Q46. Which of the following is a mechanism by which a company or organization centrally manages the usage status of smartphones or such other devices that are lent to its staff members by making integrated settings according to the security policy, or by delivering business applications?

- a) BYOT (Bring Your Own Technology)
- b) ECM (Enterprise Content Management)
- c) LTE (Long Term Evolution)
- d) MDM (Mobile Device Management)

Q47. Which of the following is an appropriate preventive measure against malware that is taken on a client PC?

- a) In a periodic manual inspection for viruses on a PC, a virus scan is performed only on the files created after the signature file of the anti-virus software is updated.
- b) In order that no PC is infected with a virus attached to an e-mail, communication with unused TCP ports is prevented.
- c) In order that no PC is invaded by a worm, a global IP address is dynamically assigned to a client PC.
- d) In order that no virus exploits a vulnerability and infects a PC, revised software modules or patches are appropriately applied to the OS and applications.

Q36. When Mr. *A* sends Mr. *B* an e-mail with a digital signature created by using public key cryptography, which of the following is the appropriate combination of the keys that are used by Mr. *A* and Mr. *B*?

	Key that Mr. <i>A</i> uses to create digital signature	Key that Mr. <i>B</i> uses to verify digital signature
a)	Mr. <i>A</i> 's private Key	Mr. <i>A</i> 's public Key
b)	Mr. <i>A</i> 's public Key	Mr. <i>A</i> 's private Key
c)	Mr. <i>B</i> 's private Key	Mr. <i>B</i> 's public Key
d)	Mr. <i>B</i> 's public Key	Mr. <i>B</i> 's private Key

Q37. When security attacks to a computer system are classified into three categories (i.e., reconnaissance attack, access attack, and DoS attack), which of the following is classified as a reconnaissance attack?

- a) Attempting to discover and map out systems, services, or vulnerabilities
- b) Compromising the availability of a network, host, or application
- c) Exploiting known vulnerabilities in authentication services or other Web services
- d) Sending an extremely large number of requests over a network or the Internet

Q38. Which of the following is an appropriate explanation concerning the security attack that is classified as DNS cache poisoning?

- a) In order to block the service that is an attack target, an attacker sends a large number of recursive queries by using the DNS server as a stepping stone.
- b) In order to obtain internal information, the zone information stored in the DNS server is transferred all at once.
- c) Incorrect domain information is injected into the DNS server referenced by a PC, which leads the PC user to a fake Web server.
- d) The version information of the software used by a DNS server is obtained to identify a security hole in the DNS server.

Q39. Which of the following is a method for preventing an SQL injection attack?

- a) Ensuring that the input characters are not interpreted as characters that have a special meaning in an inquiry or operation to the database
- b) Rejecting an input text if the overall length of the input text exceeds the applicable maximum size limit
- c) Rejecting an input text that contains the character string (. . /) that specifies a higher level directory
- d) Replacing the HTML tags of an input text with other character strings that are not interpreted as HTML tags

Q40. When the procedure below is performed in terms of security, which of the following can be done by recipient B , in addition to the detection of message falsification?

[Procedure]

Process of sender A

- (1) A hash function is used to generate a digest from a message.
- (2) The sender's secret signature generation key is used to generate a signature for the message from the digest generated in (1).
- (3) The message and the data generated in (2) are sent to recipient B .

Process of recipient B

- (4) A hash function is used to generate a digest from the received message.
- (5) The received data, the digest generated in (4), and sender A 's signature verification key are used to verify the signature.

- a) Confirming that the message is from sender A
- b) Detecting wiretapping on the message
- c) Identifying the areas of falsification
- d) Preventing leakage of the message

Q41. Which of the following is the security attack that is shown in the procedure below?

[Procedure]

- (1) An attacker creates a bogus Web site under the disguise of a financial institution.
- (2) The attacker pretends to be an employee of the financial institution and sends an e-mail that describes a URL leading to the bogus Web site.
- (3) The recipient of the e-mail trusts the e-mail and clicks on the URL. The recipient is then led to the bogus Web site.
- (4) The recipient does not notice that the Web site is bogus, and the entered authentication information is passed to the attacker.

- | | |
|--------------------------|----------------|
| a) Bot | b) DDoS attack |
| c) Mail header injection | d) Phishing |

Q42. Which of the following is regarded as risk sharing or risk transfer?

- a) Breaking down or aggregating risks into manageable units
- b) Distributing risk to other parties by purchasing insurance
- c) Eliminating the source of a risk
- d) Reducing the rate of occurrence of loss or damage

Q44. Which of the following is a method that is used for encrypting e-mail?

- a) BASE64
- b) GZIP
- c) PNG
- d) S/MIME

Q41. Which of the following is the most appropriate term that corresponds to the method of illegally intercepting audio and/or data being transmitted or received via a network?

- a) Salvaging b) Scavenging c) Sniffing d) Spoofing

Q42. Which of the following is a computer network attack that can be classified as a DDoS attack?

- a) A destructive computer program bores its way through a computer's files or through a computer network and is activated on a predetermined event or at a particular date or time.
- b) A program installed by a virus or even by legitimate programs allows an attacker to manipulate the compromised computer to bypass security controls and perform single or even strategic attacks against other people's computers.
- c) A set of software tools is used to hide presence of a malicious program on a computer and to help an attacker obtain administrator-level access to the computer without the user's knowledge or consent.
- d) All the computers infected by a virus send a large number of recursive queries simultaneously to a target computer when receiving a command from an attacker who is in a remote location.

Q43. When information, such as an e-mail or a document file, is sent or received with a digital signature via the Internet, which of the following is the appropriate combination of security properties that ensure that such information has not been altered or tampered with during transmission?

- a) Atomicity and consistency
- b) Authenticity and integrity
- c) Availability and confidentiality
- d) Durability and isolation

Q44. Which of the following is the most appropriate explanation of a digital certificate that is authorized by a trusted third party known as a CA (Certification Authority)?

- a) A document that verifiably associates a public key with a particular person or party
- b) A technique that is used to hide the secret data into a digital image, audio, or video file
- c) A tool that serves to protect the copyright and authenticity of multimedia content
- d) An electronic signature that protects the integrity and authenticity of a document

Q45. Which of the following is a biometric recognition technique that is used for identifying a person by using the person's own behavioral features as well as physiological features?

- a) Fingerprint recognition
- b) Iris recognition
- c) Vein recognition
- d) Voice recognition

Q46. Which of the following is an appropriate description concerning social engineering?

- a) An attacker creates IP packets that appear to originate from valid addresses inside a trusted network.
- b) An attacker intercepts and modifies the data in the packet without the knowledge of the sender or receiver.
- c) An attacker manipulates people into providing inappropriate access to sensitive or confidential data.
- d) An attacker searches for a valid combination of user ID and password by using a brute force attack tool.

Q47. Which of the following is a technique where a system is actually attacked and an intrusion attempt is made, with the aim of discovering security-related vulnerabilities of a computer or network?

- a) Penetration test
- b) Regression test
- c) Software inspection
- d) Walk-through

Q48. Which of the following is a network segment that is isolated from the external network (WAN) and the internal network (LAN) via firewalls in order to ensure that publicly accessible servers cannot contact other internal network segments in the event that such a server is compromised?

- a) DMZ
- b) DNS
- c) Proxy
- d) VLAN

Q42. Which of the following is the attack where malicious input data is given to a Web application to construct a database query or other data manipulation statements with the aim of falsifying data or illegally acquiring information?

- a) Cross site scripting
- b) Directory traversal
- c) Session hijacking
- d) SQL injection

Q43. Which of the following is an appropriate description of a directory traversal attack?

- a) The attacker enters database command statements as input data for a Web application, and executes unexpected SQL statements.
- b) The attacker illegally obtains the session ID of a user, who has logged into the session, and has access to the server by spoofing the identity of the user.
- c) The attacker leads a user to a Web site where vulnerability in input data processing is exploited, and executes a malicious script on the user's browser.
- d) The attacker specifies files on the server by using a path that is unexpected by an administrator, and gains unauthorized access to classified files.

Q44. Which of the following is the most appropriate term that refers to the way in which a company collects any personal information about users via the company's website and also the way in which the company uses and protects such personal information?

- a) Acceptable use policy
- b) Human resources policy
- c) Privacy policy
- d) Security policy

Q45. Which of the following is the most appropriate method of determining whether to enable or disable communication that can be achieved by using the ARP mechanism for a PC in which communication is requested?

- a) The MAC address of the PC is checked, and communication is permitted only when the MAC address has been registered beforehand.
- b) The patch application status in the OS of the PC is checked, and communication is permitted only when the latest patch has been applied.
- c) The programs installed in the PC are checked, and communication is permitted when only the registered programs have been installed.
- d) The signature file for the anti-malware program of the PC is checked, and communication is permitted only when the latest file has been installed.

Q46. Which of the following is the most effective method for detecting the falsification of content on a Web server?

- a) The entire communication with the Web server is monitored to ensure that there is no communication other than HTTP and HTTPS.
- b) The hash value of each file containing the content of the Web server is stored and is periodically compared with the hash value generated from each file.
- c) The memory utilization of the Web server is checked periodically to ensure that there is no occurrence of a buffer overflow.
- d) The updated date of each file containing the content of the Web server is stored and is periodically compared with the updated date of each file in the directory.

Q41. A PKI involves two types of key pairs: signature key pairs, in which the private key is used for signing and the public key for checking; and exchange key pairs, in which the public key is used by an application to encrypt data, and the private key is used to decrypt the encrypted data. Which of the following is the key pair(s) that may be escrowed or backed up to prevent the loss of important data even when the corresponding key or keys are forgotten?

- a) Both exchange key pair and signature key pair
- b) Either exchange key pair or signature key pair depending on conditions
- c) Exchange key pair
- d) Signature key pair

Q42. Which of the following can be achieved by receiving an e-mail text and its hash value from the sender, and then comparing this hash value with another hash value calculated by the recipient from the e-mail text? Here, the hash value that the recipient receives from the sender is correct.

- a) Checking the delivery of the e-mail
- b) Detecting the presence or absence of falsification in the e-mail text
- c) Preventing spoofing
- d) Preventing wiretapping of the e-mail text

Q43. Which of the following is a security measure where it is effective to confirm the destination address with the sender when an e-mail is sent?

- a) A preventive measure against unauthorized relay of e-mail
- b) A preventive measure against wrong transmission of e-mail
- c) Anti-spam measure using OP25B
- d) Anti-spam measure using SPF

Q44. Which of the following is the purpose of using a WAF (Web Application Firewall)?

- a) To block attacks to a vulnerability arising from a Web server and an application
- b) To detect the intrusion of a worm in a Web server and remove the worm automatically
- c) To detect vulnerabilities and inconsistencies of applications in an integration test during content development for a Web server
- d) To find security holes of a Web server and apply OS security patches

Q45. As a security measure on the Internet, a type of challenge-response test called a CAPTCHA can be used to determine whether the client is a human or a computer program. Which of the following is an appropriate purpose of using such a measure?

- a) To protect against a relay attack
- b) To protect against a virus or a worm
- c) To protect against automated spamming
- d) To protect against spyware or adware

Q43. From a viewpoint of security measures, which of the following is an appropriate purpose of confirming the destination address with the sender at the time of sending e-mail?

- a) To prevent any delay or wrong relay of e-mail
- b) To prevent e-mail from being sent to a wrong recipient
- c) To prevent spam e-mail by using OP25B (Outbound Port 25 Blocking)
- d) To prevent spam e-mail by using SPF (Sender Policy Framework)

Q44. Which of the following is the public key cryptography algorithm that is named after the initials of its three researchers and is based on the difficulty of factorizing extremely large numbers into prime factors?

- a) AES b) DES c) DSA d) RSA

Q45. Which of the following is the most appropriate tool that is used to emulate a real hacker by looking for security holes and other weaknesses from the outside of an organization's network?

- a) Malware scanner
- b) Network stumbler
- c) Port scanner
- d) Vulnerability scanner

Q46. Which of the following is an explanation of the pattern matching technique for antivirus software?

- a) Viruses are detected by collating data with the checksum of a file.
- b) Viruses are detected by comparing data with a collection of known virus signatures.
- c) Viruses are detected by comparing files before and after infection to check whether there is any change.
- d) Viruses are detected by monitoring the malfunction of a system that is caused by them.

Q47. Which of the following is the most appropriate mechanism that allows a Web server to temporarily store user information in a PC browser so that the Web server can check whether the PC (and probably its user) has visited the Web site before and thereby can provide certain personalized services?

- a) Applet b) Cookie c) Plug-in d) Servlet

Q41. Which of the following is used for encoding and interpreting binary files, images, video, and non-ASCII character sets within an e-mail message on the Internet?

- a) IMAP b) MIME c) POP3 d) SMTP

Q42. Which of the following is the protocol that is expanded and standardized based on SSL (Secure Sockets Layer) v3 but cannot interoperate with SSL?

- a) IPsec (Internet protocol security)
- b) RSH (Remote shell protocol)
- c) SSH (Secure shell protocol)
- d) TLS (Transport layer security protocol)

Q43. Which of the following provides a baseline of security requirements for the operations of CA (Certification Authority) and RA (Registration Authority)?

- a) Certificate policy
- b) Certificate practice statement
- c) Statement of applicability
- d) System security policy

Q44. Which of the following is an appropriate description concerning a digital envelope?

- a) The sender and recipient must securely share a single private key in advance, and the key is used for both encryption and decryption.
- b) The sender encrypts a hash of the data with the sender's private key. The recipient decrypts it by using the sender's public key, and checks if it matches a hash the recipient computes.
- c) The sender encrypts the message by using symmetric key cryptography and then encrypts the symmetric key by using public key cryptography.
- d) The sender encrypts the message by using the recipient's public key prior to sending it. The recipient decrypts the message with the recipient's private key.

Q45. There are two methods of biometric authentication: one extracts physical characteristics and the other extracts behavioral characteristics. Which of the following uses behavioral characteristics?

- a) Authentication is performed by extracting characteristics from the branch angle of a branch point of a blood vessel and from the distance between branch points.
- b) Authentication is performed by extracting characteristics from the chaotic pattern of wrinkles spreading out from the pupil.
- c) Authentication is performed by extracting characteristics from the writing speed and pen pressure used when a signature is produced.
- d) Authentication is performed by extracting characteristic points called minutiae from the pattern formed by ridge lines.

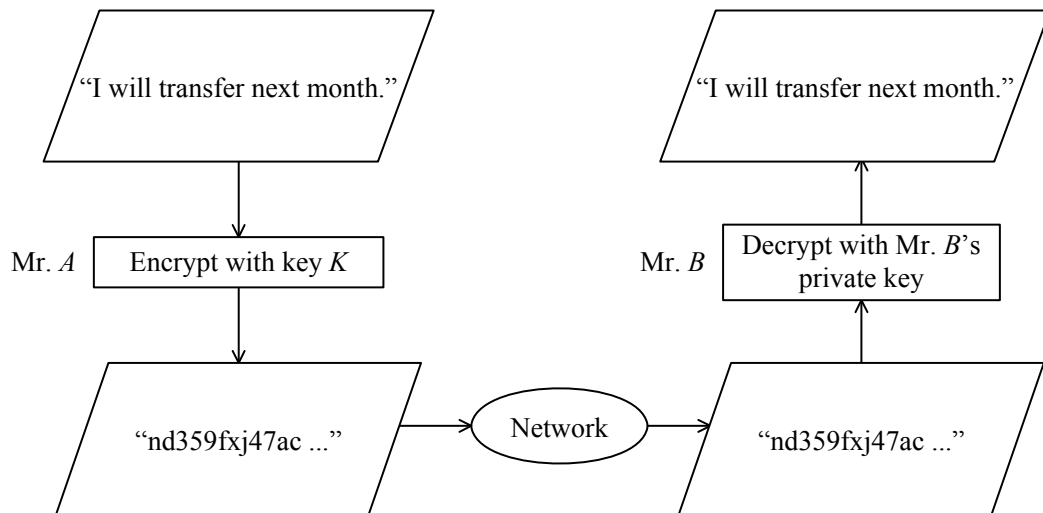
Q46. Which of the following is a method that is used to check if an image or other digital content has been illegally copied and resold?

- a) Digital certificate
- b) Digital preservation
- c) Digital signature
- d) Digital watermark

Q43. A message with a digital signature is received via e-mail. Which of the following can be checked by verifying the digital signature of the received message?

- a) The e-mail has not been leaked.
- b) The e-mail has not been relayed improperly.
- c) The message has not been falsified.
- d) The message has not been retransmitted on a specific date and time.

Q44. When Mr. *A* sends his confidential message to Mr. *B* by using public key cryptography as shown in the figure below, which of the following is the appropriate key *K* used for encryption?



- a) Common private key
- c) Mr. *A*'s public key

- b) Mr. *A*'s private key
- d) Mr. *B*'s public key

Q45. Which of the following is a technique of social engineering that obtains sensitive or confidential data by searching for residual data left in a computer after job execution or by examining discarded or stolen media such as printed papers, tapes, and discs?

- a) Salami technique
- b) Scavenging
- c) Sniffing
- d) Spoofing

Q46. Which of the following is a collection of infected computers that have been compromised without their owners realizing it and are being remotely controlled by attackers, in order to typically send spam or attack other computers?

- a) Botnet
- b) Honeynet
- c) Rootkit
- d) Web beacon

Q47. A packet filtering-type firewall is installed at the connection point between an in-house network and the Internet. When the firewall makes possible access to the Web server (port number 80) on the Internet from a PC on the in-house network, which of the following is the appropriate combination that is permitted by the packet filtering rules?

		Source	Destination	Source port number	Destination port number
a)	Outgoing packet	PC	Web server	80	1024 or more
	Response packet	Web server	PC	1024 or more	80
b)	Outgoing packet	PC	Web server	1024 or more	80
	Response packet	Web server	PC	80	1024 or more
c)	Outgoing packet	Web server	PC	80	1024 or more
	Response packet	PC	Web server	80	1024 or more
d)	Outgoing packet	Web server	PC	1024 or more	80
	Response packet	PC	Web server	80	1024 or more

Q41. Which of the following is an algorithm that can be used for asymmetric (or public key) cryptography?

a) AES

b) DES

c) RC4

d) RSA

Q42. In e-commerce such as mail-order business, there is a risk that dealers or users are damaged by falsifying, spoofing, and repudiation at the time of sales order or purchase order. Which of the following is an appropriate security technology that can cope well with all of these three threats?

- a) Digital signature
- b) Firewall
- c) Junk mail filter
- d) Virus check

Q43. Which of the following is an appropriate description concerning the PIN (Personal Identification Number) of an IC card used for user authentication?

- a) Every PIN is set by combining the number information stamped on the surface of an IC card.
- b) Since each user can be identified with an IC card, all users have a common PIN to reduce administrative burden.
- c) When an IC card is lost, a new one is issued and a PIN is set. After that, the lost IC card is canceled.
- d) When an IC card is sent, its PIN is not sent under the same cover. The user is notified of the PIN in another way.

Q44. When a biometric authentication system is installed, which of the following is the most appropriate point to be considered?

- a) Combining various measures, such as heuristics, in addition to frequent update of pattern files
- b) Requesting a trusted third party to issue an individual user's digital certificate
- c) Setting up the system in consideration of both the probability of incorrectly rejecting an authorized user and that of incorrectly accepting an unauthorized user
- d) Using a library capable of sanitizing data which can cause a system malfunction

Q45. Which of the following is an explanation of a risk transfer?

- a) Breaking down or aggregating risks into components that can be easily handled
- b) Eliminating risk factors
- c) Reducing the incidence of losses
- d) Taking financial measures such as purchasing insurance

Q41. When a message is sent to Person A from Person B using public key cryptography, which of the following keys should be used for encrypting the message?

- a) A's private key
- b) A's public key
- c) B's private key
- d) B's public key

Q42. Which of the following is the function of S/MIME used for e-mails?

- a) Compressing e-mails
- b) Encrypting e-mails and attaching a signature
- c) Notifying senders that e-mails have been delivered and opened
- d) Resending e-mails

Q43. Which of the following can be achieved by using SSL/TLS?

- a) Communication between clients and servers is encrypted.
- b) Processing time is shortened in communication between clients and servers.
- c) The SMTP connection from mail software to a Web server is enabled.
- d) The trails of communication between browsers and Web servers are secured.

Q44. Which of the following refers to online scams where thieves attempt to entice e-mail recipients into clicking on a link that takes them to a bogus website, and the website may prompt the recipient to provide personal information such as social security number, bank account number, and credit card number, and/or it may download malicious software onto the recipient's computer?

- a) Cross site scripting
- b) DoS attack
- c) Phishing
- d) Trojan horse

Q45. A government website accepts passport applications using HTTP forms to collect information. Users provide complete personal information in the forms to help expedite processing of face-to-face transactions, and payments are done offline. The information collected enters a secure server for processing and document releasing. In this system environment, which of the following is the most likely security attack?

- a) Password-guessing attack
- b) Sniffing traffic for identity theft
- c) Spamming to attain denial of service
- d) Spoofing attack

Q46. Which of the following explains the pattern matching method that is used by antivirus software?

- a) Viruses are detected by comparing files before infection with files after infection to investigate whether any change has been made to the files.
- b) Viruses are detected by comparison with the file checksum.
- c) Viruses are detected by comparison with the signature codes of known viruses.
- d) Viruses are detected by monitoring the system for abnormal phenomena caused by viruses.

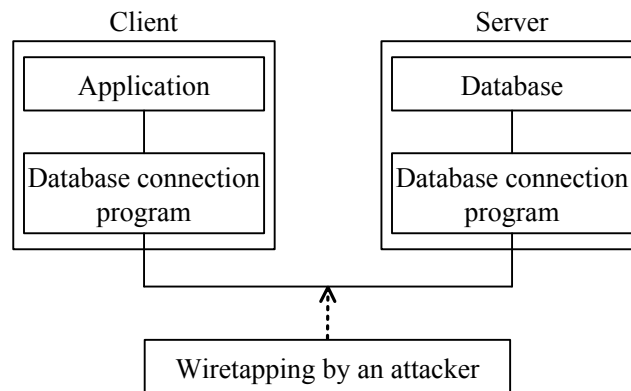
Q44. Which of the following can be achieved by receiving mail text and its hash value from the sender and comparing the hash value with the one calculated from the mail text by the receiver? Here, the hash value from the sender is protected.

- a) Confirmation of e-mail delivery
- b) Detection of presence or absence of falsification
- c) Prevention of spoofing
- d) Prevention of tapping

Q45. When the judgment threshold is changed in a biometric authentication system, which of the following shows the relationship between FRR (False Rejection Rate) and FAR (False Acceptance Rate)?

- a) As FRR decreases, FAR decreases.
- b) As FRR decreases, FAR increases.
- c) As FRR increases, FAR increases.
- d) FRR and FAR are independent.

Q46. As shown in the figure, an application on a client has access to the database on a server via a pair of database connection programs. Which of the following is the appropriate measure for preventing the data transmitted and received between the database connection programs from being wiretapped on a communication line?



- a) Changing the default port number provided by the database management system to another number, which is used for communication by the database connection programs
- b) Encrypting the communication between the database connection programs on the client and server sides
- c) Restricting the IP addresses of the clients that have access to the database connection program on the server side to only those required
- d) Setting a password that is required to start and stop the database connection program on the server side

Q47. Which of the following sends a program incorporating fraudulent functions, such as destruction and falsification of data, for installation and execution?

- a) Buffer overflow attack
- b) Dictionary attack
- c) DoS attack
- d) Trojan horse

Q48. A Web server was invaded from the outside, and its contents were falsified. Which of the following is the appropriate sequence of subsequent activities?

(1)	Analyze each log on the server, IDS (Intrusion Detection System), and the firewall to identify the method used to gain unauthorized access, the extent of the impact, and the path of the invasion.
(2)	Reconstruct the system, and apply the latest patches and security setting information.
(3)	Disconnect the server from the network.
(4)	Monitor for a while after connecting the server to the network.

a) (1) → (2) → (3) → (4)

b) (1) → (3) → (2) → (4)

c) (2) → (3) → (1) → (4)

d) (3) → (1) → (2) → (4)

Q66. When secret documents are sent and received using public key cryptography, which of the following is an appropriate description of the key management?

- a) The decryption key must be kept private, but the encryption key is public.
- b) The encryption and decryption keys may be public, but the encryption algorithm must be kept private.
- c) The encryption key may be public, but the encryption algorithm must be kept private.
- d) The encryption key must be kept private, but the decryption key is public.

Q67. In the context of message authentication code, which of the following is the purpose of using message digests?

- a) To check a summary of the message
- b) To check the message encryption method
- c) To confirm that no message has been tampered with
- d) To ensure message confidentiality

Q68. Which of the following is an appropriate explanation of Web beacons?

- a) Images embedded in Web pages to gather information such as user access trends
- b) Latent errors in application programs used on Web sites
- c) Unauthorized techniques to inflict damage on both PCs and Web servers themselves, through malicious script
- d) Viruses downloaded from Web sites that delete image files on a PC

- Q69.** Which of the following is an appropriate description concerning security measures for network systems?
- a) By using a circuit-switched network with closed-area connection functions, limiting connections to particular user groups is an effective way to prevent unauthorized external access.
 - b) In ISDN and packet-switched lines, it is possible to confirm the other party based on the subscriber number which is received in notification at the time of connection. This is referred to as callback.
 - c) Installing a line encryption device between DTEs (such as communication control units and terminal equipment) and DCEs (such as modems and DSUs) as an encryption method for each transmission segment requires modification of some existing hardware and software.
 - d) Using a wireless LAN is an effective way to prevent interception of transmissions because there is no cable in between.

Q70. There are two types of attacks which an information system might face: active attack and passive attack. Which of the following is categorized as an active attack?

- a) Analysis of data traffic
- b) DoS (Denial of Service)
- c) Falsification of data
- d) Replay of messages

Q71. Which of the following shows the appropriate sequence of items 1 through 3 that are required for establishing ISMS according to ISO/IEC27001:2005?

[Items]

1. Prepare a Statement of Applicability
2. Select control objectives and controls for the treatment of risks
3. Analyze and evaluate the risks

a) $1 \rightarrow 2 \rightarrow 3$

b) $1 \rightarrow 3 \rightarrow 2$

c) $2 \rightarrow 3 \rightarrow 1$

d) $3 \rightarrow 2 \rightarrow 1$

Q66. In public key cryptography, which of the following key can be used for decrypting the data that is encrypted by using the server's public key?

- a) Client's private key
- b) Client's public key
- c) Server's private key
- d) Server's public key

Q67. Which of the following is an appropriate description of phishing?

- a) It is a technique for fooling users into visiting a hostile or untrusted website through spam messages and divulging personal data such as accounting numbers, passwords, and other confidential information.
- b) It is an attempt to prevent legitimate users from accessing network services, by sending repetitive data packets to a targeted system from a number of systems called botnets.
- c) It goes through every possible combination of numbers, letters, and symbols in order to login to the system by defeating password security.
- d) It has the capability to capture and analyze data from information packets that travel over a network. That data may include user names, passwords, and proprietary information in plain text.

Q68. In an electronic transaction that employs public key cryptography, which of the following is created by the certification authority (CA), a third party independent of the parties involved in the transaction?

- a) The digital signatures of the parties involved in the transaction
- b) The electronic certificates for the private keys of the parties involved in the transaction
- c) The electronic certificates for the public keys of the parties involved in the transaction
- d) The passwords of the parties involved in the transaction

Q69. Which of the following is an appropriate description concerning Internet VPN security?

- a) A virtual network is configured, so there is no way to prevent a third party that is not qualified to participate in the network from wiretapping or falsification.
- b) The virtual tunnel of Internet VPN is a dedicated channel between specified LANs, so there is no function for protecting data that passes along this route from wiretapping.
- c) There is no capability for identifying individual people who are qualified to participate in the network.
- d) There is no risk of abusing the IP address for unauthorized access or intrusion, so there is no need to encrypt the entire packet including the IP address.

Q70. Which of the following is an appropriate description concerning risk analysis?

- a) It takes too much time and cost to handle all potential risks, so the damage costs and occurrence probabilities should be estimated in advance and priority should be given in accordance with the magnitude of risks.
- b) Risk analysis should not be repeated until all measures against the previously analyzed and evaluated risks are implemented.
- c) The objective of risk analysis is to estimate the amount of damage associated with the occurrence of risks, so the cost of implementing countermeasures should be determined in proportion to the amount of damage.
- d) The objective of risk analysis is to prevent future losses, so data accumulated from past similar projects should not be used as reference.

Q71. Which of the following is a meta-language that includes self-defining markup symbols called tags to describe the content of a Web page or file and supports bi-directional hyperlinks with high affinity to the Internet?

- a) HTML b) SGML c) UML d) XML

Q66. Which of the following authentications can be realized with the information exchange between two communication actors X and Y according to the procedure below?

[Procedure]

- (1) Y transmits a character string (challenge) including optional information to X .
 - (2) X generates a new character string (response) from the received character string based on predetermined rules between X and Y , and sends back this character string (response) to Y .
 - (3) Y confirms that the returned character string (response) is correct.
-
- a) X authenticates Y .
 - b) X authenticates Y , with the result that Y authenticates X .
 - c) Y authenticates X .
 - d) Y authenticates X , with the result that X authenticates Y .

Q67. Which of the following is an advantageous effect of encrypting e-mails?

- a) It is possible to prevent denial-of-service attacks against e-mails.
- b) It is possible to prevent encryption keys from being lost.
- c) It is possible to prevent the contents of e-mails from leaking out.
- d) It is possible to protect transmission records on mail servers from being falsified.

Q68. Which of the following is an appropriate action to be taken when a computer virus is found?

- a) First, the computer is powered off, because the virus program may be resident in memory.
- b) First, the infected computer is disconnected from the relevant network, because other computers may be infected via the network.
- c) If a worm that infects a wide area in a short period of time is found while an on-line business system is running, the virus countermeasure is taken without stopping the system.
- d) The reproducibility of virus activities is confirmed for the purpose of identifying the virus name by special characteristics activated at the time of infection.

Q69. Which of the following is an appropriate operations management method for user IDs and passwords?

- a) A list of user IDs and passwords is prepared for the purpose of expediting troubleshooting, and the administrator in charge keeps the list.
- b) For the purpose of preventing passwords from being abused by other people, it is so arranged that users become free to change their passwords at any time.
- c) User IDs and passwords that are not currently used are reused for the purpose of simplifying management work.
- d) With the aim of improving convenience, user IDs and temporary passwords for newcomers are registered, prior to the arrival of user registration applications, by referring to the advance announcements of personnel changes.

Q70. When LAN analyzers are used for finding out the causes of network failures, which of the following is a point to keep in mind?

- a) As a provision against the occurrence of failures, it is necessary to inform all network users of the storage places and directions for use of LAN analyzers.
- b) LAN cables must be temporarily disconnected during measurement. Therefore, it is necessary to inform users of the measurement dates in advance.
- c) Packets originally intended to be transmitted to their destinations are destroyed during measurement. Therefore, it is necessary to limit the use of computers other than those to be measured.
- d) Some analyzers are capable of displaying packets that pass through networks. Therefore, it is necessary to be careful not to use them in different ways such as wiretapping.

Q67. A store intends to use public key cryptography so that it may receive orders from customers through a network without exposing the contents of the orders to third parties. Which of the following is the appropriate combination of keys used by both the store and customer?

	Store	Customer
a	Private key	Private key
b	Private key	Public key
c	Public key	Private key
d	Public key	Public key

Q68. What is the purpose of attaching a digital signature to software disclosed on the Internet?

- a) To guarantee that the software contents have not been tampered with
- b) To limit the use of the software to certain specified users
- c) To make it clear that the copyright of the software belongs to the person whose signature appears there
- d) To notify that the software's author is the person in charge of maintenance

Q69. Which of the following can be realized by using the packet filtering function of a firewall?

- a) To allow only the packets with specific TCP port numbers to pass from the Internet through to the internal network
- b) To change a packet with a dynamically assigned TCP port number to a TCP port number that is fixed at the receiving side and allow it to pass through to the internal network
- c) To check for tampering in the header and/or data of a packet received on the Internet and remove the packet if tampering has been found
- d) To repair a packet received on the Internet if it has been tampered with, or to record the packet in a log and prevent the packet from passing through to the internal network if the tampering cannot be repaired

Q70. Which of the following is the salami technique used in computer crime?

- a) Illegally intercepting audio and/or data being transmitted or received on a network
- b) Secretly gaining access to a part of the line to steal someone's password and/or ID and to steal data
- c) Secretly searching for information left inside or around a computer after a program is executed, for the purpose of obtaining necessary information
- d) Stealing from multiple assets little by little, to a degree that the illegal action does not come to the surface and become noticeable

Q71. Which of the following is a method of phishing?

- a) A virus-infected computer is controlled from the outside via a network such as the Internet.
- b) Personal information such as the IP address and Web browsing history of computer users is secretly collected and sent to the outside.
- c) Someone sends e-mails to entice the recipients and to have them access fake Web sites that appear to be sites of actually existing companies etc. and steals personal information.
- d) When there is a part that directly displays what has been entered on a Web page, a malicious script is embedded within the page, causing damage to the user and the server.

Q70. Which of the following is the major impact of a Denial of Service (DoS) attack?

- a) An increased volume of spam e-mails
- b) Degradation of service due to network traffic congestion
- c) Falsification of database and/or website
- d) Leakage of user ID and password

- Q71.** Which of the following is the appropriate method that supports both private key cryptography and public key cryptography, enables users to securely exchange e-mail messages, and to secure files, disk volumes, and network connections with both privacy and strong authentication?
- a) DES (Data Encryption Standard)
 - b) DSA(Digital Signature Algorithm)
 - c) PGP (Pretty Good Privacy)
 - d) RSA (Rivest, Shamir, and Adleman)

Q72. Port scanning is the process of sending packets to check every port on each target system to see which ports are open and which ports are locked. Which of the following information can be identified by port scanning?

- a) Computer viruses in activity
- b) Hardware configuration and compatibility
- c) Network and application services currently available
- d) Operating system in execution

Q70. There is an OS that can set access privileges to read, update, and create subordinate files in a directory. These three types of access privileges can be set to “enabled” or “disabled” using 1 bit. If these three bits are set by an octal (base-8) number expressed by numerals 0 to 7, which of the following is an appropriate description, taking into account the trial results below?

[Trial results]

- (1) When 0 was set, all accesses were disabled.
 - (2) When 3 was set, read and update were enabled, but create was disabled.
 - (3) When 7 was set, all accesses were enabled.
-
- a) When 2 is set, read and create are enabled.
 - b) When 4 is set, only create is enabled.
 - c) When 5 is set, only update is enabled.
 - d) When 6 is set, read and update are enabled.

Q71. Which of the following is an appropriate description of the virus pattern file that is used in virus protection measures for computers?

- a) It is a file included in virus protection software and is used to repair files that have been infected by viruses.
- b) It is a file that records the program code of known viruses and is used to re-enact viruses to monitor their activities.
- c) It is a file that records the signature code of known viruses and is used to detect viruses by the virus protection software.
- d) It is a restoration file and is used when a data file is damaged by a virus.

Q72. Against what kind of attacks does SSL (Secure Socket Layer) protect users on the Internet?

- a) Bruce force attack
- b) DoS (Denial of Service) attack
- c) IP Spoofing
- d) Tapping and exploitation of data

Q73. Which of the following is an appropriate statement regarding elements of information security defined in ISO/IEC 17799:2005?

- a) Availability is ensuring that information is accessible only to those authorized to have access.
- b) Confidentiality is ensuring that authorized users have access to information and associated assets when required.
- c) Information security is characterized as the preservation of confidentiality and integrity of information assets, but not its availability.
- d) Integrity is safe-guarding the accuracy and completeness of information and processing methods.