# 3-1 Threats and Countermeasures in Information Security [1]

## Point!

### 1 Information Security

(1) ([1]**Information security**) : The act of properly managing information and keeping it safe.

(2) The three essential elements of information security

[1] ([2]**Confidentiality**) : A state in which only authorized individuals can access the information.

[2] ([3]**Integrity**) : A state in which the information is not destroyed, tampered with, or erased.

[3] ([4]**Availability**) : A state in which information can be accessed at any time when needed.

### 2 Various threats to information security

(1) ([5]**Unauthorized access**) : When someone without permission gains access to a computer system.

(2) ([6]**Cracking**) : The act of unlawfully accessing a system to tamper with, erase, or steal data. A person who commits such acts is called a ([7]**cracker** ).

(3) ([8]**Malware**) : A general term for malicious programs designed to harm computers. Infection can occur through websites, email attachments, USB drives, or networks.

[1] ([9]**Computer virus**) : A program designed to intentionally cause harm, such as destroying data or programs.

[2] ([10]**Trojan horse**) : A program disguised as a legitimate one that infiltrates a system and quietly initiates attacks.

[3] ([11]**Worm**) : A program that replicates itself and spreads across the internet like a worm, expanding the infection.

[4] ([12]**Spyware**) : A program that collects personal information without the user's knowledge and sends it to third parties.

- ([13]**Keylogger**) : Software that monitors and records keystrokes.
- ([14]**Adware**) : A program that displays unwanted advertisements without the user's consent.

[5] ([15]**Ransomware**) : A program that renders data inaccessible and demands a ransom to restore access.

(4) ([16]**Cybercrime**) : Criminal acts committed over computer networks.

[1] ([17]**Violation of the Unauthorized Computer Access Law**) : Illegally accessing a computer using someone else's user ID or password.

[2] Crimes involving computer or electronic records : Crimes involving tampering with stored data or unauthorized manipulation of devices.

[3] Network-based crimes : Crimes committed using networks, such as fraud, defamation, or copyright infringement.

## Warm Up

Answer the following questions.

(1) Choose the one in which availability is compromised in terms of information security from the options **A** to **C** below.

**A** A cyberattack caused a website to go down.

**B** Incorrect data was entered due to a keyboard typing error.

**C** Personal information was leaked due to a malware infection on the computer.

(2) Choose all actions that constitute a violation of the Unauthorized Computer Access Law from the options **A** to **D** below.

**A** Illegally used another person's user ID and password to access a computer.

**B** Stored a password that was obtained illegally on a computer.

**C** Shared a friend's user ID and password with someone else without the friend's permission.

**D** Published a website selling quasi-legal drugs or containing unlawful and inappropriate content.

### Explanation

(1) Information security consists of three elements: integrity, confidentiality, and availability.

**A** When information becomes unavailable, availability is compromised.

**B** When information is no longer accurate, integrity is compromised.

**C** When unauthorized individuals can view the information, confidentiality is compromised.

Therefore, the correct answer is **A**.

(2) **A** Using a computer without having access rights constitutes unauthorized access and is prohibited under the Unauthorized Computer Access Law.

**B** Storing a password obtained illegally for the purpose of unauthorized access is prohibited under the Unauthorized Computer Access Law.

**C** Sharing someone else's password with a third party without valid reason or permission promotes unauthorized access and is also prohibited by law.

**D** Publishing illegal content may fall under network-related crimes.

Therefore, the correct answers are **A**, **B**, and **C**.

## Try

**1** There are three elements of information security: Integrity, Confidentiality, and Availability. For each of these elements, choose the one most appropriate measure from the following options **A** to **E**.

(1) Integrity (2) Confidentiality (3) Availability

**A** Report your arrival at work to the network administrator.

**B** Handle special data such as personal ID numbers in a room where only authorized personnel are allowed to enter.

**C** Keep logs of data access and modifications to enable traceability.

**D** Install backup power supplies for all devices related to critical information systems in preparation for power outages.

**E** Run malware in order to always have access to important information.

**2** Choose the terms that best fit into the blanks [1] to [5] from the options **A** to **H** below, and answer using the letters.

> When a third party without network access rights uses someone else's ID and password to illegally enter a computer system, it is called ( [1] ). Incidents have occurred in which individuals known as hackers or ( [2] ) have destroyed systems.
>
> Programs that destroy internal computer data or cause abnormal operations are called ( [3] ). Among these are ( [4] ), which disguise themselves as legitimate programs and silently infiltrate systems to carry out attacks, and ( [5] ), which replicate themselves and spread across the internet like worms to increase infections.

| | | |
|---|---|---|
| **A** Worm | **B** Cracker | **C** Unauthorized access |
| **D** Trojan horse | **E** Computer virus | **F** Adware |
| **G** Keylogger | **H** Impersonation | |

**3** Answer the following questions.

(1) Choose all items from **A** to **D** that present a risk of computer virus infection.

**A** An email attachment sent from a computer infected with a virus.

**B** Connecting to a network infected with a virus.

**C** A USB memory stick that was used on a computer infected with a virus.

**D** A movie DVD played on a computer infected with a virus.

(2) Choose one act from **A** to **D** that constitutes a violation of the Unauthorized Computer Access Law.

**A** Provided personal information to a third party without the individual's consent.

**B** Took a photo of a magazine page with a smartphone and uploaded it to social media.

**C** Acquired a computer virus capable of automatically infiltrating networks.

**D** Used another person's user ID and password without permission to purchase products through online shopping.

## Exercise

**1** Cover the **Point!** section on page 23 with a red sheet and test yourself by writing the items in order in your notebook.

**2** For each of the three elements of information security, select:

- The most appropriate description from Group A (**A**–**C**), one per element
- All applicable potential damages from Group B (a–f) that may occur if that element is not ensured

(1) Confidentiality (2) Integrity (3) Availability

<Group A>

**A** Ensuring uninterrupted access to information when needed.

**B** Ensuring that only authorized individuals can access the information.

**C** Ensuring that information has not been destroyed, tampered with, or deleted.

<Group B>

a Eavesdropping on the network

b Service interruptions such as system downtime

c Password leakage

d Tampering with or destruction of information

e Information leakage

f Unauthorized use of computers or networks

**3** Answer the following questions.

(1) Choose the most suitable option for the blank from the options **A** to **G** below, and answer using the letters.

[1] A virus that displays advertisements the user did not intend to see is called ( ).

[2] The act of illegally infiltrating a computer to tamper with, erase, or steal data is called ( ).

[3] Software that leaks data stored on a computer to the outside is called ( ).

[4] Malicious software including computer viruses and Trojan horses is collectively referred to as ( ).

**A** Malware **B** Keylogger **C** Adware **D** Cracking

**E** Hacking **F** Phishing **G** Spyware

(2) Choose the one correct statement from **A** to **D** regarding computer virus infection.

**A** As long as the computer is connected to a network, there is always a risk of infection by a computer virus.

**B** If you do not connect to a computer or network and only transfer data using a USB memory stick, infection will not occur.

**C** If you avoid accessing harmful or illegal websites, you will not get infected.

**D** As long as you do not open emails, you are safe from infection, so being cautious with emails is sufficient.

# 3-2 Threats and Countermeasures in Information Security [2]

## Point!

### 1 Passwords and Authentication

(1) Password: A string of characters used to verify that the user of a given user ID is the legitimate account holder.

(2) Guidelines for creating passwords:
- Use a string that is as ([1]**long**) as possible.
- ([2]**Combine**) uppercase letters, lowercase letters, numbers, and symbols.
- Do not use personal information such as your birthday, email address, or user ID.
- Do not reuse passwords used for other services.

(3) ([3]**One-time-password**) : A password that changes at regular intervals and can only be used once.

(4) ([4]**Authentification**) : The process of verifying the identity of a user on a computer or network.

(5) Types of authentication:

| Name | Method | Examples |
|---|---|---|
| [1] ([5]Knowledge-based authentication) | Authentication using information known only to the individual. | User ID and password, PIN code |
| [2] ([6]Biometric authentication (Biometrics)) | Authentication using physical or behavioral characteristics of the individual. | Fingerprint, Iris, Vein pattern, Handwriting |
| [3] ([7]Possession-based authentication) | Authentication using an item that the individual possesses. | IC card, One-time password, SMS-based verification |

[4] ([8]**Two-factor authentication**) : A method that combines two different types of factors from "knowledge," "biometrics," and "possession" to perform authentication.

[5] ([9]**Two-step authentication**) : A method that performs authentication in two steps using two pieces of information from the same type of factor.

### 2 Information Security Measures

(1) ([10]**Access control**) : A method of limiting access to computer systems or data so that only specific users, verified through authentication, are allowed to use them.

(2) ([11]**Firewall**) : A system installed at network entry points to prevent ([12]**unauthorized access**) from outside and to stop ([13]**data leaks**) from within.

(3) Countermeasures against computer viruses
- Install ([14]**antivirus software**) to remove or isolate viruses, and keep the virus definitions within the software up to date.
- Always keep the operating system (OS) and application software ([15]**updated**) to prevent ([16]**security holes**) (vulnerabilities) in the software.
- Regularly create ([17]**backups**) of your data.

## Warm Up

Answer the following questions.

(1) Choose the one incorrect statement regarding password best practices from the options **A** to **D** below, and answer using the letter.

**A** Do not reuse the same password across multiple services.
**B** It is best to keep using the default password that was initially assigned.
**C** Combine letters, numbers, and symbols when creating a password.
**D** Avoid using easily guessable information such as your name or birthday.

(2) Choose all correct statements about one-time passwords from the options **A** to **D** below, and answer using the letters.

**A** If a one-time password is leaked, it can easily lead to unauthorized access.
**B** Using a one-time password strengthens overall security.
**C** A one-time password has a limited usage time and becomes invalid after expiration.
**D** It can prevent unauthorized access using leaked passwords.

(3) Choose the one correct example of biometric authentication from the options **A** to **D** below, and answer using the letter.

**A** Authentication using a user ID and password assigned to each individual
**B** Authentication using an SMS sent to a smartphone
**C** Authentication by scanning a fingerprint on a sensor
**D** Authentication using a one-time password

(4) If a password can use the digits 0 to 9 and lowercase letters a to z, how many different combinations are there for a 3-character password? Give your answer in the form of $a^n$.

### Explanation

(1) If an initial password is assigned via email or memo, there is a possibility that the password has been leaked to a third party. Therefore, the initial password must be changed. The correct answer is **B**.

(2) A one-time password is a password that changes at fixed intervals and can only be used once. This strengthens security. The correct answers are **B, C,** and **D**.

(3) Biometric authentication refers to the use of an individual's physical or behavioral characteristics for verification. Examples include fingerprint, iris, vein, or handwriting-based authentication. The correct answer is **C**.
Note: A is knowledge-based authentication, B is possession-based authentication, and D is also possession-based authentication.

(4) There are 10 digits (0–9) and 26 letters (a–z), making 36 possible characters. Since each character in the password can be any of the 36, the total number of combinations for a 3-character password is 36 × 36 × 36 = **$36^3$ combinations**.

## Try

Answer the following questions.

(1) Choose the one incorrect statement regarding password best practices from the options **A** to **D** below, and answer using the letter.

**A** Do not use information such as phone numbers, birthdays, email addresses, or user IDs.
**B** It is best to continue using the initial password without changing it.
**C** Do not reuse the same password across different services.
**D** Use a mix of uppercase and lowercase letters, numbers, and symbols.

(2) Choose the one thing that can be prevented by using a one-time password from the options **A** to **D** below, and answer using the letter.

**A** Password theft during transmission over a network
**B** Tampering with confidential files after unauthorized access
**C** Infection by a virus through malicious software
**D** Unauthorized access using a leaked password

(3) Choose the one correct example of biometric authentication from the options **A** to **D** below, and answer using the letter.

**A** Authentication using the shape of a fingerprint or vein pattern
**B** Authentication using a digital certificate
**C** Authentication based on whether the user can correctly read distorted text in an image
**D** Authentication using a one-time password

(4) Choose the terms that best fit into the blanks [1] to [4] from the options **A** to **F** below, and answer using the letters.

To protect computers and networks from threats such as unauthorized access and computer viruses, it is necessary to implement various security measures. For example, determining whether a person is authorized to access a computer or network is called ( [1] ). As countermeasures against computer viruses, there are the introduction of ( [2] ) and the ( [3] ) of hardware and operating systems. Furthermore, a system that hides internal LAN computers from external networks and prevents unauthorized access is called a ( [4] ).

**A** Firewall **B** Antivirus software **C** Encryption
**D** Authentication **E** Update **F** Security hole

(5) What is the term for restricting access so that only specific users can operate a computer system or network?

♪ (6) If a password uses 26 characters (A to Z), how many times greater is the maximum number of brute-force attempts required to crack the password when increasing the length from 4 characters to 6 characters?

## Exercise

**1** Cover the **Point!** section on page 27 with a red sheet and test yourself by writing the items in order in your notebook.

**2** Answer the following questions.

(1) Choose the one incorrect statement regarding password creation from the options **A** to **D** below, and answer using the letter.

**A** Use the shortest possible string to make it easy to remember.
**B** Do not reuse passwords used for other services.
**C** Do not write passwords down in a notebook or on sticky notes.
**D** Combine uppercase and lowercase letters, numbers, and symbols.

(2) Choose the one threat that can be prevented by using a one-time password from the options **A** to **D** below, and answer using the letters.

**A** Theft of user ID through social engineering
**B** Unauthorized access through brute-force attacks
**C** Unauthorized access using a leaked password
**D** Virus infection through a security hole

(3) Choose the one correct example of biometric authentication from the options **A** to **D** below, and answer using the letter.

**A** Authentication using a personal ID or password
**B** Authentication using physical characteristics such as fingerprints or irises
**C** Authentication based on an individual's problem-solving ability
**D** Authentication using physical performance such as grip strength or flexibility

(4) Choose the terms that best fit into the blanks [1] to [5] from the options **A** to **F** below, and answer using the letters.

> System administrators must implement measures such as installing a ( [1] ) to prevent unauthorized access from outside the system and to minimize data tampering or leakage as much as possible. In order to deal with the constant emergence of new ( [2] ), it is essential to introduce ( [3] ) and patch ( [4] ).
> To prevent unauthorized access, ( [5] ) is useful for restricting system or network usage to specific users only.

**A** Firewall **B** Antivirus software **C** Security
**D** Access control **E** Computer virus **F** Security hole

(5) What is the name of the authentication method that combines two different elements from "knowledge," "biometric," and "possession"?

♪ (6) If a password can use the digits 0–9 and lowercase letters a–z, how many possible combinations are there for a 4-character password? Give your answer in the form of $a^n$.

# 3-3 Threats and Countermeasures in Information Security [3]

## Point!

### 1 Fraudulent Billing

([1]**Fraudulent billing**): A scam in which a person is billed for a fictitious service they have never used, with the intent to fraudulently extract money.

([2]**One-click fraud**): A scam where clicking a URL in a website or email automatically triggers a message pretending a contract has been concluded, followed by an exorbitant payment demand.

### 2 Unauthorized Acquisition of Information

(1) ([3]**Phishing**) : A scam that uses fake websites disguised as financial institutions or public agencies to steal personal information such as PINs or account details.

(2) ([4]**Social engineering**) : A method of fraudulently obtaining information by exploiting human psychology, carelessness, or lack of awareness.

[1] ([5]**Impersonation**) : The act of pretending to be someone else—such as making a phone call in their name—to obtain information.

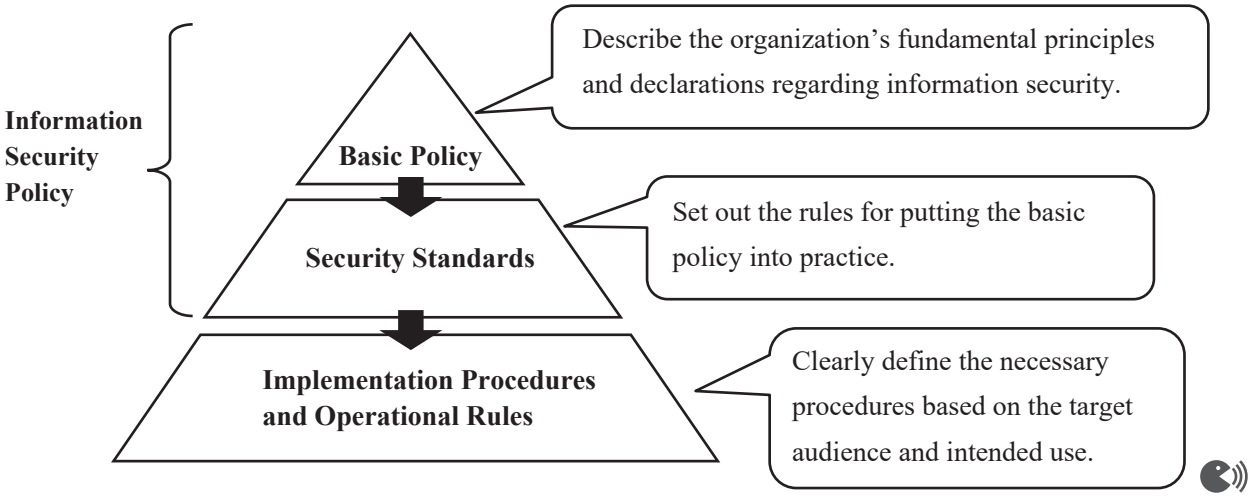
[2] ([6]**Shoulder surfing**) : The act of peeking over someone's shoulder to steal passwords or PIN codes.

[3] ([7]**Dumpster diving**) : The act of rummaging through trash to obtain discarded confidential information.

(3) ([8]**Skimming**) : The act of illegally extracting data from someone's credit or debit card and using it to create a counterfeit card.

### 3 Information security policy

([9]**Information Security Policy**) : A set of fundamental rules and guidelines established by a company or organization to maintain and protect information security.



## Warm Up

Answer the following questions.

(1) Choose the one that correctly describes phishing from the options **A** to **D** below, and answer using the letter.

**A** A program that unknowingly steals personal information from inside a computer and sends it to a third party.

**B** Pretending to be an email from a financial institution to lure someone to a fake website and illegally obtain their PIN or credit card number.

**C** Clicking a URL once in a website or email triggers a false declaration of contract and a demand for a large payment.

**D** Being billed for a service you don't recognize and being defrauded of money.

(2) Choose *all* that correspond to social engineering from the options **A** to **D** below, and answer using the letters.

**A** Disabling access to data on a computer and demanding a ransom for its recovery.

**B** Creating a fake website posing as a bank to steal the PIN of a bank account.

**C**. Eavesdropping on conversations with other users.

**D** Rummaging through trash to obtain discarded confidential information.

### Explanation

(1) A is spyware, C is one-click fraud, and D is fraudulent billing. Answer: **B**

(2) A is ransomware, B is phishing. Answers: **C, D**

## Try

Read the following passage and answer the questions that follow.

As more people use the internet, cases of fraud involving the misuse of computers and smartphones are also increasing. For example, there are scams where simply clicking a URL on a website is treated as agreeing to a service contract, and a large fee is demanded ( [1] ), or emails pretending to be from financial institutions lead users to fake websites in order to steal PINs or credit card numbers ( [2] ). Various deceptive methods exist. In addition, (A)exploiting gaps in human psychology or carelessness can also lead to the unauthorized acquisition of information.

(1) Write the terms that best fit in blanks [1] and [2].
(2) What is the term used to describe the kind of activity mentioned in the underlined part A?
(3) Choose *all* that are related to the answer in (2) from the options **A** to **D** below, and answer using the letters.
- **A** Individuals can communicate with each other over the internet.
- **B** Data on a computer is made inaccessible, and a ransom is demanded for its recovery.
- **C** Eavesdropping on conversations with other users.
- **D** Peeking while someone is entering their user ID or password.

## Exercise

**1** Cover the **Point!** section on page 31 with a red sheet and test yourself by writing the items in order in your notebook.

**2** Answer the question to the following.

(1) For each of the following sentences, choose the most closely related option from the options **A** to **E** below, and answer using the letters.
- [1] Being charged a usage fee simply by clicking a link, as if you had joined or signed a contract.
- [2] Pretending to be a financial institution to trick users into entering their user ID and password, which are then misused.
- [3] A basic policy established by a company or organization to maintain information security.
- [4] Illegally extracting information from someone else's credit card or bank card.

**A** Phishing **B** One-click fraud **C** Skimming
**D** Information security policy **E** Social engineering

(2) Choose *all* that fall under social engineering from the options **A** to **D** below, and answer using the letters.
- **A** Calling from outside while pretending to be an employee, in order to extract confidential internal information.
- **B** Being billed for a fictitious service you don't recognize and being defrauded of money.
- **C** Rummaging through trash to obtain discarded confidential information.
- **D** Running a program that causes malicious software to be downloaded without the user's knowledge.

# 3-4 Information Technology for Safety [1]

## Point!

### 1 Encryption

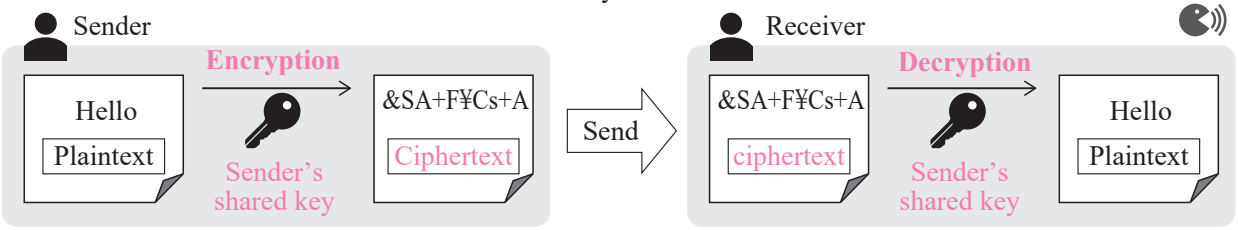
(1) ([1]**Encryption** ) : A method used when sending information to prevent it from being intercepted by anyone other than the intended recipient. The encrypted text is called ([2]**ciphertext**), and the original, unencrypted text is called ([3]**plaintext**).

(2) ([4]**Decryption**) : The process of converting ciphertext back into its original plaintext form.

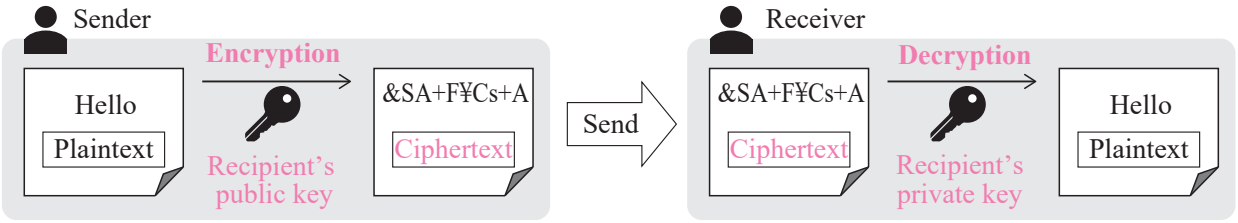
(3) ([5]**Key**) : The specific procedure or data used for encryption and decryption.

### 2 Types of encryption

(1) ([6]**Symmetric key encryption**) : An encryption method where the same ([7]**shared key**) is used for both encryption and decryption.
The message is encrypted using the ([8]**sender's shared key**) and decrypted using the ([9]**sender's shared key**) that was sent in advance by the sender.




(2) ([10]**Public key encryption**) : An encryption method that uses a publicly shared encryption key ([11]**public key**) and a private encryption key ([12]**private key**). The message is encrypted using the ([13]**recipient's public key**), which was sent in advance, and decrypted using the ([14]**recipient's private key**), which only the recipient possesses.




(3) Characteristics of Symmetric Key Encryption and Public Key Encryption

| | Symmetric Key Encryption | Public Key Encryption |
|---|---|---|
| Merit | Compared to public-key encryption, encryption and decryption processing speed is ([15]**faster**). | Since data can be decrypted by anyone with the key, a different shared key is needed for each sender. |
| Demerit | Because the public key can be shared freely, key management is easier. | Compared to symmetric-key encryption, encryption and decryption processing speed is ([16]**slower**). |

(4) ([17]**Session key method**) : An encryption method that combines symmetric key encryption and public key encryption.

## Warm Up

Answer the following questions.

(1) Complete the following sentences by filling in the blanks [1] to [4] with the appropriate terms.

> When sending information, the technology used to prevent it from being leaked or tampered with by anyone other than the intended recipient is called ( [1] ). The original data before encryption is called ( [2] ), and the act of converting the ciphertext back into plaintext is called ( [3] ). Also, during both ([1]) and ([3]), something called a ( [4] ) is used.

(2) For each of the following items **A** to **D**, write "S" if the statement refers to symmetric key encryption, or "P" if it refers to public key encryption.

**A** The encryption key is made public, and encryption is done using the public key while decryption is done with the private key.

**B** Encryption uses separate keys held by the recipient — one for encryption and one for decryption.

**C** Compared to the other method, the encryption and decryption processing speed is faster.

**D** Compared to the other method, exchanging the key is more difficult.

(3) What is the name of the hybrid encryption method that combines symmetric key encryption and public key encryption?

### Explanation

(1) [1] encryption [2] plaintext [3] decryption [4] key

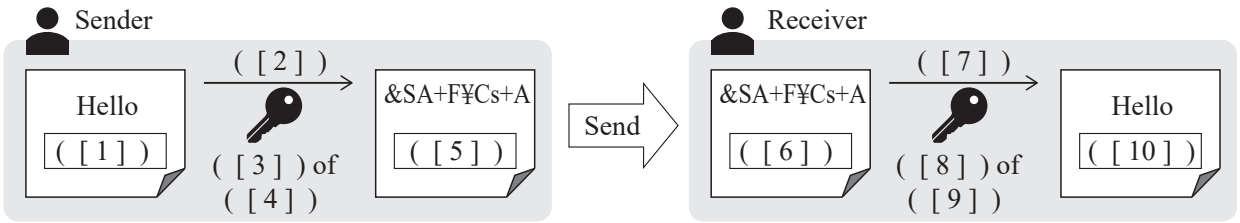
(2) **A** and **B**: The method in which encryption is performed with the recipient's public key and decryption with the recipient's private key is public key encryption.
**C** and **D**: Symmetric key encryption is faster than public key encryption, but since it uses the same key for both encryption and decryption, there is the issue of how to securely share the key with the recipient.
Therefore, A: **P**, B: **P**, C: **S**, D: **S**

(3) Session key method

## Try

**1** Answer the following question.

(1) The diagram illustrates the process flow of public key encryption. For blanks [1] to [10], choose the appropriate terms from options **A** to **J** below. Note that the same option may be used more than once.




**A** Plaintext **B** Ciphertext **C** Decryption **D** Encryption **E** Encoding
**F** Shared key **G** Public key **H** Private key **I** Sender **J** Recipient

(2) For each of the following items **A** to **D**, write "S" if the statement refers to symmetric key encryption, or "P" if it refers to public key encryption.

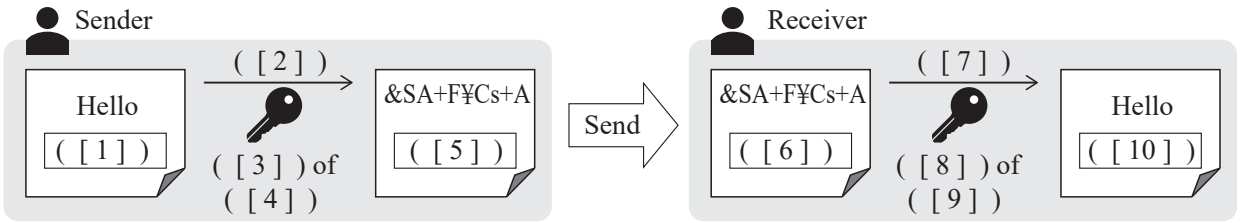
**A** A separate key must be prepared for each sender.
**B** The same key is used by the sender for both encryption and decryption.
**C** Encryption and decryption are slower compared to the other method.
**D** Exchanging the key is easier compared to the other method.

## Exercise

**1** Cover the **Point!** section on page 34 with a red sheet and test yourself by writing the items in order in your notebook.

**2** Answer the following question.

(1) The diagram shows the process flow of symmetric key encryption. For blanks [1] to [10], choose the appropriate terms from the options **A** to **J** below. The same option may be used more than once.




**A** Plaintext **B** Ciphertext **C** Decryption **D** Encryption **E** Encoding
**F** Shared key **G** Public key **H** Private key **I** Sender **J** Recipient

(2) Among the options **A** to **D** below, choose the one that best describes a characteristic of symmetric key encryption when compared to public key encryption. Answer using the corresponding letter.

**A** Uses different keys for encryption and decryption.
**B** Allows fast encryption and decryption.
**C** Enables safer distribution of keys.
**D** Makes key management easier even when communicating with many different parties.

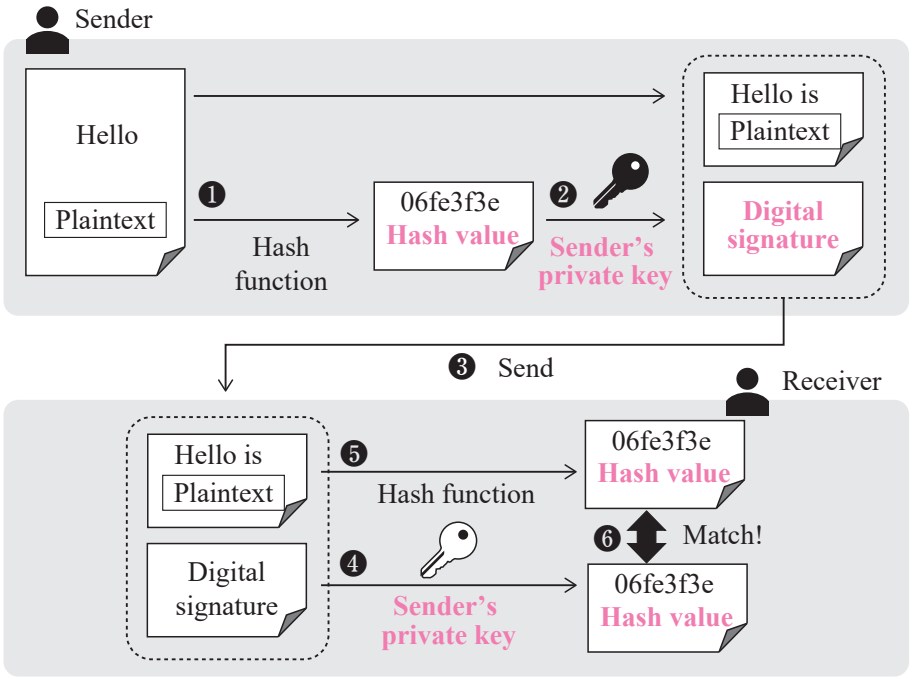
# 3-5 Information Technology for Safety [2]

## Point!

### 1 Digital Signature

(1) ([1]**Hash function**) : A function that calculates a unique value based on the input data.The value generated by the hash function is called a ([2]**hash value**). It is not possible to restore the original data from the hash value.

(2) ([3]**Digital signature (Electronic signature)**) : A technology that uses public key encryption and hash values to prove that the transmitted data is from the sender and has not been tampered with.




【Sender's Procedure】

1. Use a hash function to generate a ([4]**hash value**) from the plaintext to be sent.
2. Encrypt the hash value using the ([5]**sender's private key**). This encrypted hash is called a ([6]**digital signature**).
3. Send both the plaintext and the digital signature to the recipient.

【Recipient's Procedure】

4. Use the ([7]**sender's public key**) to decrypt the received digital signature and retrieve the original hash value.
5. Use the same hash function used in step 1 to generate a new ([8]**hash value**) from the received plaintext.
6. Compare the two ([9]**hash values**) from steps 4 and 5. If they match, it proves that the message is from the sender and has not been tampered with.

(3) ([10]**Certification authority (CA)**) : A trusted third-party organization that verifies whether a public key truly belongs to its claimed owner.
It issues ([11]**digital certificates**) that include the public key and identifying information of the key owner.

## 2 SSL / TLS

([12]**SSL/TLS**) : A technology used to encrypt communication between a web server and a web browser. The ([13]**session key method**) is used in this encryption. The URL of an encrypted web page begins with "([14]**https**):// …".

*TLS (Transport Layer Security) was introduced as a more secure version of the originally used SSL (Secure Sockets Layer). However, since the term "SSL" became widely recognized, the combined term SSL/TLS is often used.

## Warm Up

Answer the following questions.

(1) For the following statements **A** to **D** about hash values, mark "○" if the statement is correct, or "×" if it is incorrect.

**A** If one character in the original data is changed, only one character in the resulting hash value will change.

**B** A digital signature is created by encrypting the hash value of the document to be sent with a private key.

**C** It is difficult to restore the original message from its hash value.

**D** Even if the documents being sent are different, the hash values obtained from the same hash function will always be the same.

(2) The following sentences describe the steps of creating a digital signature. Fill in the blanks [1] to [4] with the appropriate terms.

> The sender generates a ( [1] ) based on the data they want to send and encrypts it using their ( [2] ). This is called a ( [3] ), and the sender sends both the data and the digital signature to the recipient. The recipient decrypts the received ([3]) using the sender's ( [4] ) to recover the original ([1]). The recipient also generates a ([1]) from the received data using the same hash function. If the two ([1]) values match, it proves that the data is from the sender and has not been tampered with.

(3) What is the name of the technology used to encrypt communication between a web server and a web browser?

## Explanation

(1) **A**. If even a single character in the original message is different, the resulting hash value becomes completely different. Therefore: ×

**B** ○

**C** ○

**D** If the message being sent is different, the resulting hash value will also be completely different even when using the same hash function. Therefore: ×

(2) [1] hash value [2] private key [3] digital signature (electronic signature) [4] public key

(3) SSL/TLS

## Try

Answer the following question.

(1) Choose the terms that best fit into the blanks [1] to [6] from the options **A** to **J** below, and answer using the letters.

> To allow the recipient to verify that the data was created by the actual sender and was not tampered with during transmission, there is a technology called ( [1] ). A ([1]) is created by generating a ( [2] ) from the plaintext to be sent using a program, and then encrypting it with the ( [3] ). This is attached to the plaintext and sent to the recipient. The recipient decrypts the ([1]) using the ( [4] ). If the resulting ([2]) matches the ([2]) generated from the received plaintext, it proves that the data was created by the sender and has not been altered. However, this alone cannot prevent impersonation. Therefore, a third-party organization called a ( [5] ) issues a ( [6] ) to guarantee that the public key truly belongs to the sender.

**A** Sender's private key **B** Sender's public key **C** Sender's shared key
**D** Recipient's private key **E** Recipient's public key **F** Recipient's shared key
**G** Digital certificate **H** Digital signature **I** Hash value
**J** Certification Authority (CA)

(2) Choose the terms that best fit into the blanks [1] to [2] from the options **A** to **D** below, and answer using the letters.

> Regarding the hash function used in digital signatures: The same data is always converted into the same ( [1] ) hash value, and it is ( [2] ) impossible to restore the original data from the converted hash value.

**A** Different **B** Same **C** Possible **D** Impossible

(3) Choose the terms that best fit into the blanks [1] to [6] from the options **A** to **G** below, and answer using the letters.

> When the beginning of a web page URL is "https://", it means that encryption using ( [1] ) is being performed. In ([1]), encryption is carried out using a ( [4] ) that combines ( [2] ) and ( [3] ). In addition, ([1]) also helps prevent phishing to direct towards a fake website by attaching a ( [6] ) issued by a ( [5] ).

**A** Public key encryption **B** Symmetric key encryption **C** Session key method
**D** Digital certificate **E** Digital signature **F** SSL/TLS
**G** Certification Authority (CA)

(4) Among the following options **A** to **D**, choose the one that correctly describes a function of SSL/TLS. Answer using the corresponding letter.

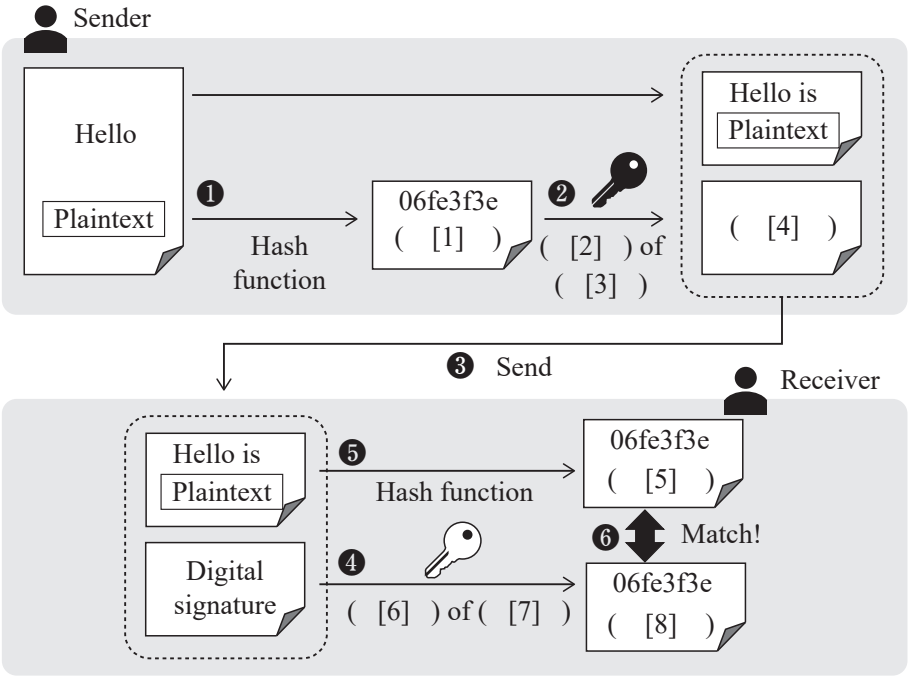
**A** Generates one-time passwords for user authentication on websites.
**B** Encrypts communication between the web browser and the web server.
**C** Filters communication to unauthorized websites.
**D** Detects viruses that spread through networks.

# Exercise

**1** Cover the **Point!** section on pages 37 and 38 with a red sheet and test yourself by writing the items in order in your notebook.

**2** Answer the following question.

(1) The diagram below illustrates the mechanism of a digital signature. For blanks [1] to [8], choose the appropriate terms from the options **A** to **H** below and answer using the corresponding letters. The same letter may be used more than once.




【Word Bank】 **A** Sender **B** Recipient **C** Shared key **D** Private key
**E** Public key **F** Hash value **G** Digital signature **H** Electronic authentication

(2) Among the options **A** to **D** below, choose the one that appropriately describes something related to an email with a digital signature. Answer using the corresponding letter.

**A** Garbled text is more likely to occur during transmission of the email.
**B** It allows you to confirm whether the email was sent from the correct sender.
**C** It prevents the contents of the email from being intercepted during transmission.
**D** It prevents the contents of the email from being lost.

(3) Among the options **A** to **D** below, choose *all* that correctly describe functions of SSL/TLS. Answer using the corresponding letters.

**A** SSL is the predecessor of TLS, and currently, TLS is the mainstream standard in use.
**B** It is a function that restricts access to harmful or illegal websites based on certain conditions.
**C** URLs that begin with "http://..." are encrypted using SSL/TLS.
**D** SSL/TLS encrypts communication using a session key method that combines symmetric and public key encryption methods.