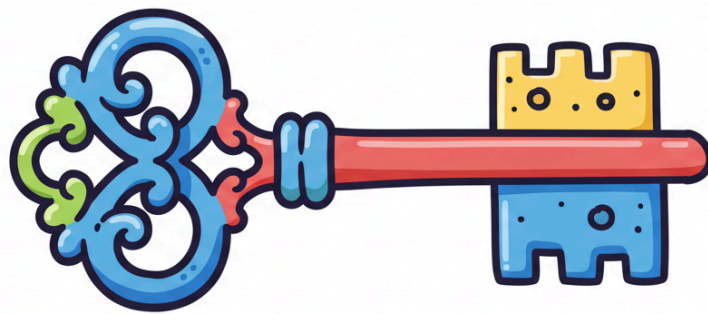


Cryptography: The Science of Secrecy

Textbook

Cryptography: The Science of Secrecy



Cryptography is the science of secure communication, making sure only authorized people can access information. It's about keeping digital data safe in our online world.

Let's look at its main ideas:

Confidentiality: Keeping Secrets

Confidentiality means only authorized people can read information. This involves **encryption**, which scrambles readable "plaintext" into unreadable "ciphertext." You need a special "key" to decrypt it back. Think of it like a locked box only your friend can open with their key.

Example: Your password is encrypted before being sent online, so no one can see it.

Integrity: Keeping Information Untouched

Integrity ensures information hasn't been changed. Cryptography uses **hash functions** to create a unique "fingerprint" of data. If the data changes even slightly, the fingerprint changes completely. If hashes match before and after, the data is untouched.

Example: Checking a downloaded file's "checksum" to ensure it's not corrupted.

Authentication: Proving Who You Are

Authentication verifies identity. **Digital signatures** use cryptographic techniques to prove a message came from a specific sender. It's like a secure electronic signature.

Example: Logging into online banking; the bank authenticates you with your username and password.

Non-Repudiation: No Denying It

Non-repudiation means a sender can't deny sending a message, and a receiver can't deny receiving it. Digital signatures provide strong, undeniable proof of involvement.

Example: Your digital signature on an online purchase proves you authorized the transaction.

Key Management: Handling the Keys

Key management is about securely generating, storing, distributing, using, and destroying cryptographic keys. If keys aren't handled well, even strong cryptography fails.

Example: Storing encryption keys securely in specialized software, not on sticky notes.

These five principles – Confidentiality, Integrity, Authentication, Non-Repudiation, and Key Management – are the foundation of digital security.

Choosing Encryption Methods

Choosing the right **encryption method** for a task is crucial for securing information.

For instance, if your goal is to ensure **confidentiality**—meaning only the intended recipient can read a message—you'd likely use encryption algorithms like AES or RSA. These methods scramble the data to make it unreadable without the correct key.

However, if the primary need is to confirm the **identity of the sender** and guarantee that the message hasn't been tampered with, then **digital signatures** are the appropriate method. A digital signature acts like a cryptographic seal, using a sender's private key to create a unique mark that can be verified with their public key. This provides both **authentication** (proving who sent it) and **data integrity** (proving it hasn't changed).

For example, secure online transactions often combine encryption for privacy with digital signatures for authenticity, ensuring both that the message is secret and that it truly came from the expected source.

Critical Thinking Questions

1. Imagine you want to send a sensitive document to a teacher. Which two cryptographic principles would be most important to ensure the document is seen only by them and hasn't been altered? Explain why.
2. Your school's online grading system suddenly crashes, and when it comes back online, some students claim their grades were changed. Which cryptographic principle, if properly implemented, could help determine if the grades were truly altered or if students are just mistaken? How?
3. Why is "Key Management" considered just as important as the other four principles, even though it's not directly about encrypting or signing messages? What could happen if key management is poor?

Questions (5)

1. You want to send a secret message to your friend so no one else can read it. Which cryptography idea are you mainly using?

MULTIPLE CHOICE

Choose the correct answer:

- A. Integrity
- B. Confidentiality
- C. Authentication
- D. Non-Repudiation

2. Imagine you download a game, and you want to make sure no one changed it to add a virus. Which cryptography idea helps you check if the file is untouched?

MULTIPLE CHOICE

Choose the correct answer:

- A. Confidentiality
- B. Authentication
- C. Integrity
- D. Key Management

3. When you log into an online game, and it asks for your username and password, what is the game trying to do?

MULTIPLE CHOICE

Choose the correct answer:

- A. Keep your password a secret from you.
- B. Make sure your account hasn't been changed.
- C. Prove that you are who you say you are.
- D. Make sure you can't deny playing the game.

4. You send an important email and want to make sure the person who gets it can't later say they never received it, or that you never sent it. Which cryptography idea provides this strong proof?

MULTIPLE CHOICE

Choose the correct answer:

- A. Confidentiality
- B. Integrity
- C. Authentication
- D. Non-Repudiation

5. You have a special code (a "key") to unlock your secret messages. If you lose this key or someone steals it, what happens to your secure communication, even if your encryption method is strong?

MULTIPLE CHOICE

Choose the correct answer:

- A. It becomes even more secure.
- B. Nothing, the messages are still safe.
- C. Your secure communication can fail because the key is compromised.
- D. The key will automatically be replaced.

Answer Keys & Solutions

Questions

1. You want to send a secret message to your friend so no one else can read it. Which cryptography idea are you mainly using?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--------------------|-------------|
| A. Integrity | ✗ Incorrect |
| B. Confidentiality | ✓ Correct |
| C. Authentication | ✗ Incorrect |
| D. Non-Repudiation | ✗ Incorrect |

Explanation:

Think about which principle is about keeping information private.

2. Imagine you download a game, and you want to make sure no one changed it to add a virus. Which cryptography idea helps you check if the file is untouched?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--------------------|-------------|
| A. Confidentiality | ✗ Incorrect |
| B. Authentication | ✗ Incorrect |
| C. Integrity | ✓ Correct |
| D. Key Management | ✗ Incorrect |

Explanation:

Consider the principle that ensures data hasn't been altered.

3. When you log into an online game, and it asks for your username and password, what is the game trying to do?

MULTIPLE CHOICE

Correct Answer:

- A. Keep your password a secret from you. ✗ Incorrect
- B. Make sure your account hasn't been changed. ✗ Incorrect
- C. Prove that you are who you say you are. ✓ Correct
- D. Make sure you can't deny playing the game. ✗ Incorrect

Explanation:

Think about the process of verifying identity.

4. You send an important email and want to make sure the person who gets it can't later say they never received it, or that you never sent it. Which cryptography idea provides this strong proof?

MULTIPLE CHOICE

Correct Answer:

- A. Confidentiality ✗ Incorrect
- B. Integrity ✗ Incorrect
- C. Authentication ✗ Incorrect
- D. Non-Repudiation ✓ Correct

Explanation:

Consider the principle that prevents someone from denying their involvement.

5. You have a special code (a "key") to unlock your secret messages. If you lose this key or someone steals it, what happens to your secure communication, even if your encryption method is strong?

MULTIPLE CHOICE

Correct Answer:

- A. It becomes even more secure. ✗ Incorrect
- B. Nothing, the messages are still safe. ✗ Incorrect

C. Your secure communication can fail because the key is compromised.

✓ Correct

D. The key will automatically be replaced.

✗ Incorrect

Explanation:

Think about the importance of "Key Management."