

Encryption

Textbook

Encryption



During times of conflict, many countries have used secret codes to conceal messages in case they fall into the wrong hands. That way, people who don't know the code wouldn't be able to read it. Changing a message into a secret code is called [encryption](#).

Computers also use encryption to help secure important files and programs. [Encryption](#) is the process of encoding data to prevent unauthorized access. [Decryption](#) is the process of decoding the data.

Computers process information so quickly that they are very good at encrypting information with complex codes that are very difficult to crack. If you had a program that you didn't want somebody to mess with, you could encrypt it so that it would be unreadable if someone got into your system.

So how does encryption work? Let's explore a few methods.

Symmetric Key Encryption

[Symmetric key encryption](#) involves one key for both encryption and decryption. Both the sender and the receiver know the secret key and can therefore understand the message being sent.

Some examples of where symmetric cryptography is used are:

- Payment applications, such as card transactions where PII needs to be protected to prevent identity

theft or fraudulent charges

- Validations to confirm that the sender of a message is who he claims to be

A writer named Panayotic Vryonis came up with an analogy that helps to explain this concept.

Phil has a box with a lock. As usual, the lock has a key that can lock and unlock the box. So, if Phil wants to protect something, he puts it in the box and locks it. Obviously, only he or someone else with a copy of his key can open the box.

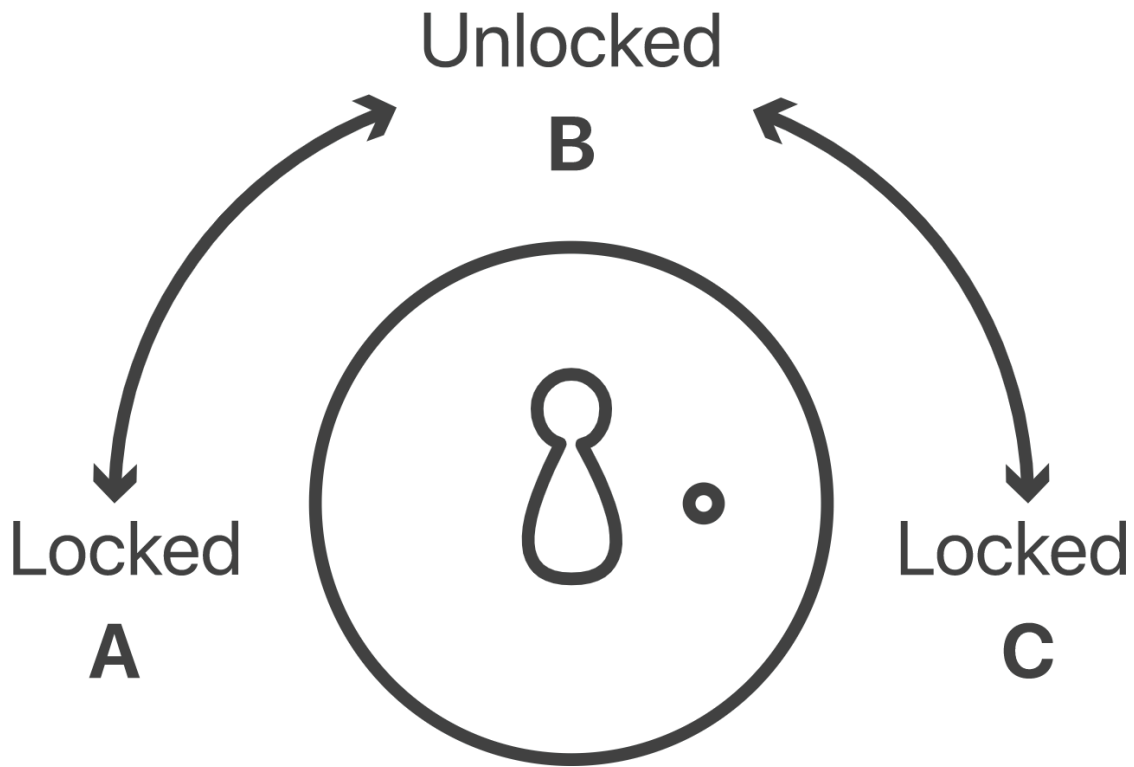
That's symmetric cryptography: you have one key, and you use it to encrypt ("lock") and decrypt ("unlock") your data.

Public Key Encryption or Asymmetric Encryption



Public key encryption is also known as [asymmetric encryption](#). Public key encryption pairs a public key for encryption and a private key for decryption. The sender does not need the receiver's private key to encrypt a message, but the receiver's private key is required to decrypt the message.

Let's use the analogy again.



Let's say Phil has a box with a special kind of lock. This lock has three positions: left, up, and right. The left and right positions mean "locked" and the up position means "unlocked."

This special kind of lock also has TWO keys that work:

Key 1 only turns to the right.

Key 2 only turns to the left.

Sam picks Key 1 and keeps it to herself. We will call this key, her "private" key -because only Sam has it.

We will call Key 2, the "public" key. Sam makes hundreds of copies of it and gives it away freely. Anyone who wants one of these keys is welcome to have it.

So only Sam can turn to the right and everyone can turn to the left.

Why is this kind of box helpful?

First of all, imagine you want to send Sam a very personal message. You put the message in the box and use a copy of her public key (Key 2) to lock it. Remember, Sam's public key only turns left, so you turn it to position A. Now the box is locked. The only key that can turn to the left is Sam's private key, the one she's kept for herself. So the only person who can access the message is Sam.

That's it! This is what we call public key encryption: Everyone who has Key 2 (which has been broadly distributed) can put information into the box, lock it, and know that the only person who can unlock it is Sam.

Assure the Correct Sender



Another cool thing this box can do, is people can know a message is sent from Sam herself. Imagine if Sam put a message in the box and locked it by turning to position C? People would know that the only person who could have locked it in that way was Sam herself, so it assures that the sender truly is Sam herself.

It's important to make sure the ownership of encryption keys is correct, so that your programs and information can be protected. Certificate authorities issue digital certificates that validate the ownership of encryption keys used in secure communications and are based on a trust model.

Learn more about this box analogy [here](#).

Cryptographer

[Cryptography](#) is the practice of writing (or cracking) encryption code which keeps data private.

[Cryptographers](#) are the individuals who do the writing and cracking of these ciphers. Cryptographers have made the internet a safer place to conduct tasks such as online shopping and sending private emails.

Cryptographers are in high demand and have high earning potential.

Discussion Question: Would you be interested in becoming a cryptographer? Why or why not? What might you enjoy about being a cryptographer? What might you not enjoy?

Summary

[Encryption](#) is a method of encoding programs or files so that they can't be easily read. We have different methods of encryption including symmetric and asymmetric encryption. [Symmetric encryption](#) involves one key to both encrypt and decrypt the messages. [Asymmetric encryption](#) involves different keys which determine who can encrypt and decrypt the messages. A [cryptographer](#) is a person who works on encrypting programs.

AP Standards

IOC-2.B.5

IOC-2.B.6

CSTA Standards

3A-NI-06

3A-NI-07

3A-NI-08

3B-NI-04

3B-AP-18

Questions (8)

1. Which type of encryption involves one key to encrypt and decrypt messages?

MULTIPLE CHOICE

Choose the correct answer:

- A. Symmetric encryption
- B. Asymmetric encryption
- C. Specific encryption
- D. General encryption

2. What is the process of decoding information?

MULTIPLE CHOICE

Choose the correct answer:

- A. Encryption
- B. Decryption
- C. Cryptography
- D. Asymmetric

3. Public key encryption is also known as what?

MULTIPLE CHOICE

Choose the correct answer:

- A. Symmetric Encryption
- B. Asymmetric Encryption
- C. Cryptography
- D. Specific Encryption

4. Which kind of encryption uses multiple keys?

MULTIPLE CHOICE

Choose the correct answer:

- A. Symmetric Encryption
- B. Asymmetric Encryption
- C. Cryptography
- D. Specific Encryption

5. True or False: Certificate authorities issue digital certificates that validate the ownership of encryption keys.

MULTIPLE CHOICE

Choose the correct answer:

- A. True
- B. False

6. What is the name of a person who works on encryptions and decryptions?

MULTIPLE CHOICE

Choose the correct answer:

- A. Cryptographer
- B. Symmetric Encryption
- C. Asymmetric Encryption
- D. Public Encryption

7. True or False: Public key encryption is also known as symmetric encryption.

MULTIPLE CHOICE

Choose the correct answer:

- A. True
- B. False

8. True or False: Cryptographers are in high demand and have high earning potential.

MULTIPLE CHOICE

Choose the correct answer:

- A. True
- B. False

Answer Keys & Solutions

Questions

1. Which type of encryption involves one key to encrypt and decrypt messages?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--------------------------|-------------|
| A. Symmetric encryption | ✓ Correct |
| B. Asymmetric encryption | ✗ Incorrect |
| C. Specific encryption | ✗ Incorrect |
| D. General encryption | ✗ Incorrect |

Explanation:

This key needs to be known by both the sender and the receiver.

2. What is the process of decoding information?

MULTIPLE CHOICE

Correct Answer:

- | | |
|-----------------|-------------|
| A. Encryption | ✗ Incorrect |
| B. Decryption | ✓ Correct |
| C. Cryptography | ✗ Incorrect |
| D. Asymmetric | ✗ Incorrect |

Explanation:

Encryption is the process of encoding a message.

3. Public key encryption is also known as what?

MULTIPLE CHOICE

Correct Answer:

A. Symmetric Encryption

✗ Incorrect

B. Asymmetric Encryption

✓ Correct

C. Cryptography

✗ Incorrect

D. Specific Encryption

✗ Incorrect

Explanation:

This is the kind of encryption that uses multiple keys.

4. Which kind of encryption uses multiple keys?

MULTIPLE CHOICE

Correct Answer:

A. Symmetric Encryption

✗ Incorrect

B. Asymmetric Encryption

✓ Correct

C. Cryptography

✗ Incorrect

D. Specific Encryption

✗ Incorrect

Explanation:

Symmetric encryption is the kind that uses one key.

5. True or False: Certificate authorities issue digital certificates that validate the ownership of encryption keys.

MULTIPLE CHOICE

Correct Answer:

A. True

✓ Correct

B. False

✗ Incorrect

Explanation:

Someone needs to make sure that the owner of encryption keys is correct.

6. What is the name of a person who works on encryptions and decryptions?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--------------------------|-------------|
| A. Cryptographer | ✓ Correct |
| B. Symmetric Encryption | ✗ Incorrect |
| C. Asymmetric Encryption | ✗ Incorrect |
| D. Public Encryption | ✗ Incorrect |

Explanation:

They work with both symmetric and asymmetric encryptions.

7. True or False: Public key encryption is also known as symmetric encryption.

MULTIPLE CHOICE

Correct Answer:

- | | |
|----------|-------------|
| A. True | ✗ Incorrect |
| B. False | ✓ Correct |

Explanation:

Public key encryption is also known as asymmetric encryption.

8. True or False: Cryptographers are in high demand and have high earning potential.

MULTIPLE CHOICE

Correct Answer:

- | | |
|----------|-------------|
| A. True | ✓ Correct |
| B. False | ✗ Incorrect |

Explanation:

Cryptographers are highly paid.

