History of Cryptography

Reading

40m

Status | Incomplete

Introduction

Cryptography is a combination of techniques used to secure information and communicate them based on mathematical concepts and algorithms. Its main purpose is to transform messages that are difficult to decipher.

It is its own field of study, which involves many techniques and technologies, including algorithms, mathematics, information theories, transmission, and encryption.

> Cryptography is used as a fundamental practice of protecting information whenever it is sent over the web, where anyone can access or intercept it.

Reading and Videos

> Review the [11 Cryptographic Methods That Marked History: From the Caesar Cipher to Enigma Code and Beyond] reading and make notes on the following seven cryptographic methods listed below.

For each method, take note of their origin, how they were used, and how difficult it was to break them.

1. The Caesar Shift Cipher
2. Scytale
3. Steganography
4. The Pigpen Cipher
5. The Playfair Cipher
6. The Polyalphabetic Cipher
7. The Data Encryption Standard

> Make sure that you have watched the following videos highlighted in the reading:

- [Secret Hidden in Images (Steganography)]

- The Enigma Machine Explained
- Polyalphabetic cipher

Which was the easiest to break?

Your Answer

Type in your answer here and Compass will let you reveal our answer below. Compass will auto-save your answer as you type. Once you click Toggle Answer below, your answer cannot be changed.

Toggle Answer

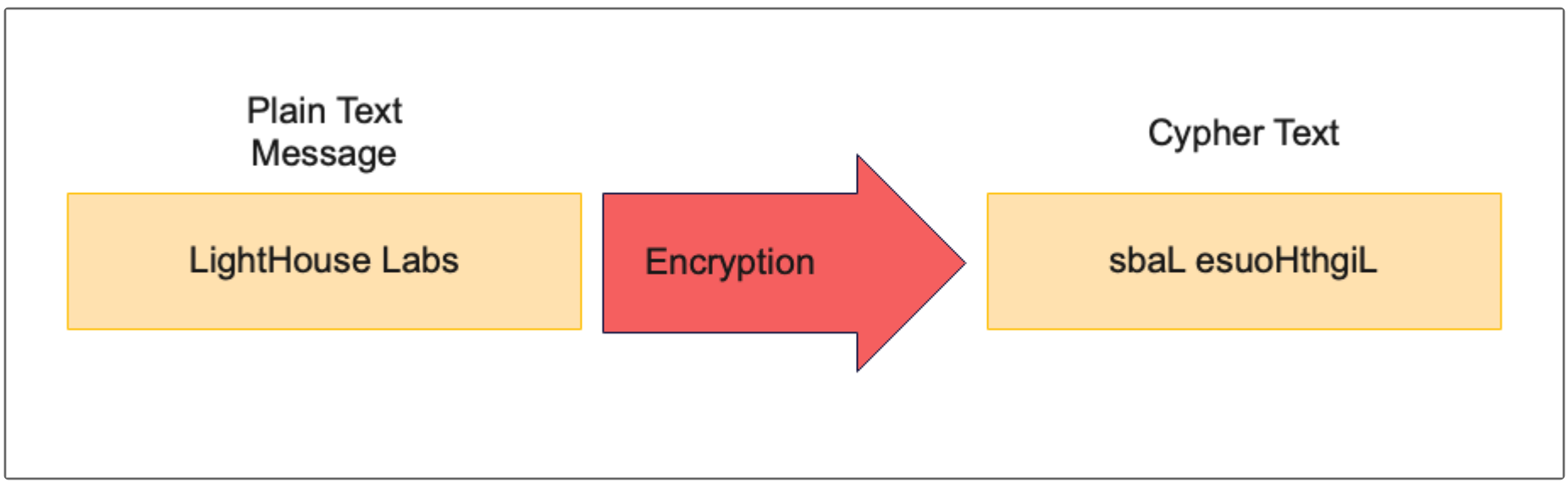
Reflection Question: Which was the start of modern day encryption?

Difference Between Cryptography and Encryption

Cryptography is the science of concealing messages with a secret code; studying methods to keep a message secret between two parties. Encryption, however, is about the processes used to encrypt and decrypt data. Encryption is generally used to conceal messages using algorithms.

You can think of encryption as a subset of cryptography with its own specific terms and processes.

The actual application of encryption uses an algorithm to encode a message. It is considered one of the most effective and popular data security techniques, as seen in the example in the image below.

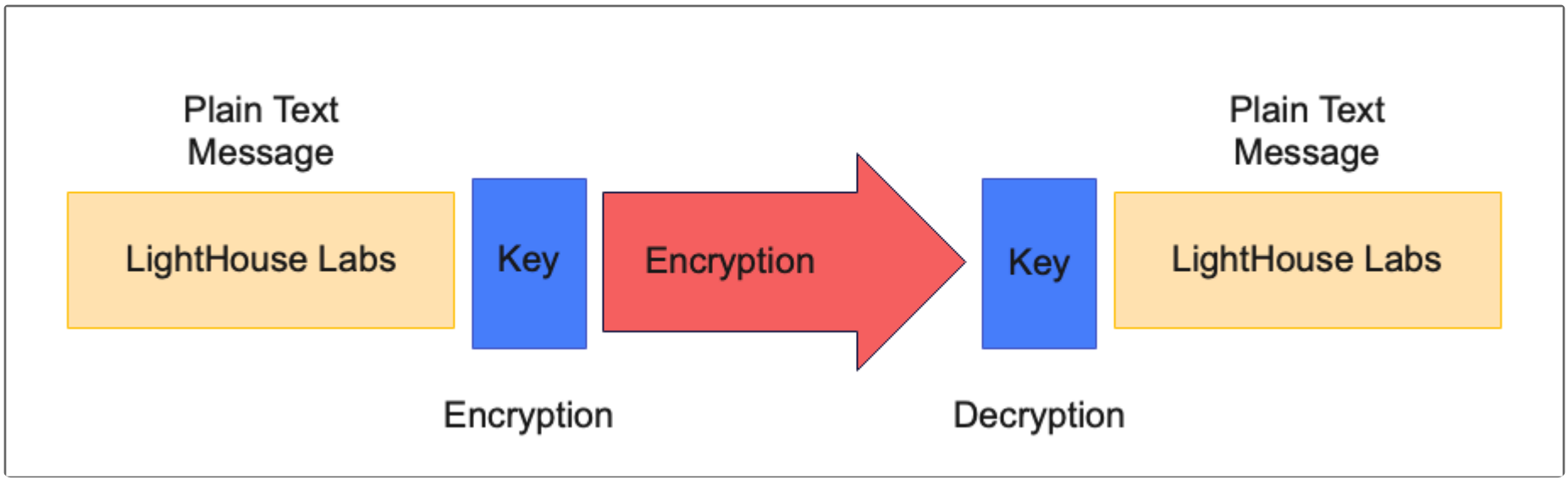


Encryption generally helps protect private information and sensitive data and enhances communication security among client apps and servers.

Cryptography's main objective on the other hand, is to provide various methods to secure and protect information and communications using encryption and other related techniques. Cryptographic techniques encompass authentication, integrity, and confidentiality.

While encryption can provide confidentiality, it does not meet the requirements of authentication and integrity that the field of cryptography covers.

As seen in the example in the image below, a key is used to encrypt and decrypt a message.



Features of Cryptography

Some of the key features of cryptography include:

- **Authentication:** the sender and receiver can confirm each other's identity and the origin/destination of the information.
- **Integrity:** the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- **Non-repudiation:** the creator/sender of the information cannot deny at a later stage their intentions in the creation or transmission of the information.
- **Confidentiality:** ensuring data is only accessible to authorized personnel and kept private from unauthorized entities.
- **Authorization:** allowing authorized persons access to specific data.
- **Key management:** cryptographic keys are securely stored, distributed, and managed.

Source: TechTarget What is Cryptography - Kathleen Richards former features editor of Information Security magazine.

Applications of Cryptography

To simplify the concept further, you can think of how cryptography might apply to everyday interactions you may have online:

- Email encryption services transform a plain text email message into a scrambled ciphertext format. This works through public-key infrastructure, which ensures that even if a cyber criminal manages to intercept a sent message, they will not be able to read it.
- Digital signatures

Further Reading

Read the article History of Cryptography to get a deeper understanding of the concepts covered in this reading. Note the historical methods used and compare them to modern techniques you will learn about in the rest of this course.

Conclusion

Understanding Cryptography will help you secure information and communicate them based on mathematical concepts and algorithms. Its main purpose is to transform messages that are difficult to decipher. Next, you'll have a introduction to the history of Encryption.

✓ Mark Completed

Previous

Next

Overview - Encryption

History of Encryption

How well did this activity help you to understand the content?

Let us know how we're doing

W06D4

Thu Aug 1

W06D4 Schedule »