Symmetric Key Encryption

Reading

10m - 25m

Status | Incomplete

Introduction

Symmetric key encryption is a type of encryption in which the same key (private key) is used to encrypt and decrypt messages. This method of encoding information has been widely used in recent decades to allow for secret communication between governments and military agencies. Symmetric key algorithms are commonly applied in various computer systems to improve data security.

How Does Symmetric Encryption Work?

A symmetric encryption scheme relies on a single key shared between two or more users. The same key is used to encrypt and decrypt the plain text (which represents the message or part of the data being encoded). The encryption process consists of executing a plain text (input) through an encryption algorithm called a cipher, which generates a ciphertext (output).

If the encryption scheme is strong enough, the only way for a person to read or access the information in the encoded text is to use the corresponding key to decrypt it. The decryption process converts the encoded text back to plain text format.

> ℹ Symmetric encryption is based on the difficulty of guessing, randomly, the corresponding key of the system. A 128-bit key, for example, would take billions of years to get the key. The longer the encryption key, the more difficult it is to decrypt. Keys with a length of 256 bits are considered highly secure and resistant to quantum computer-enforced attacks.

There are two types of symmetric encryption schemes which are based on **block** ciphers and **stream** ciphers.

- Block ciphers group data of a predetermined size into blocks and each block is encrypted using the corresponding key and encryption algorithm (for example, 128-bit plain text is incremented into 128-bit ciphertext).
- Stream ciphers do not encrypt data in blocks but in 1-bit (1 bit of plain text is encrypted in 1 bit of ciphertext).

The Use of Symmetric Encryption in Modern Systems

Symmetric encryption algorithms are employed in many modern computer systems to improve data security and user privacy. Advanced Encryption Standard (AES) is widely used in secure messaging applications and cloud storage, and is a prominent example of symmetric encryption.

In addition to software implementations, AES can also be implemented directly in computer hardware. Hardware-based symmetric encryption schemes generally use **AES 256**, a specific variant of AES that has a key size of 256 bits.

The Bitcoin blockchain does not use encryption, as many tend to believe. Instead, a specific Digital Signature Algorithm (DSA), known as the Elliptic Curve Digital Signature Algorithm (ECDSA), is used, which generates digital signatures without using encryption.

> ℹ One point that often needs clarification is that ECDSA is based on elliptic-curve cryptography (ECC), which can be applied to multiple tasks, including encryption, digital signatures, and pseudo-random generators. However, ECDSA itself cannot be used for encryption.

Advantages and Disadvantages

Symmetric algorithms provide a high level of security while allowing messages to be encrypted and decrypted quickly. The simplicity of symmetric systems is also an advantage, by requiring less computing power than asymmetric systems. Furthermore, the security provided by symmetric encryption can be increased by increasing the key lengths. For each bit added to the size of a symmetric key, the difficulty of decrypting the encryption via brute-force increases exponentially.

Although symmetric encryption offers a wide range of benefits, it has a major associated disadvantage: the inherent problem of transmitting the keys used to encrypt and decrypt data. When these keys are shared over an unsecured connection, they are vulnerable to being intercepted by third parties or malicious users.

Suppose an unauthorized user gains access to a symmetric key. In that case, the security of any data encrypted using that key will be compromised. In response to this situation, many web protocols use symmetric and asymmetric encryption to establish secure connections. Among the most prominent examples of such a hybrid system is the Transport Layer Security (TLS) encryption protocol used to secure large portions of the modern Internet.

> ℹ It is also worth mentioning that all types of computer encryption are subject to vulnerabilities due to improper implementation. While a long enough key can make a hard-hitting attack mathematically impossible, implementation mistakes made by programmers often create weaknesses that pave the way for cyberattacks.

Conclusion

Symmetric key encryption is a type of encryption where the same key is used for both encrypting and decrypting the data. In this encryption method, the data is transformed using a mathematical algorithm and a secret key, and the same key is used to transform the data back to its original form.

Next, you'll learn about Asymmetric cryptography and how it is different from Symmetric key encryption.

✓ Mark Completed

← Previous
Encryption Exercise

Next
Asymmetric Key Encryption →

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

Let us know how we're doing

☆ ☆ ☆ ☆ ☆

W06D4

Thu Aug 1

Outline & Notes (1)

Lectures (1)

Work (8)

6 hrs

- Project: IR Plan, Playbook and Policy
- Course Reflection
- Overview - Encryption
- History of Cryptography
- History of Encryption
- Encryption Exercise
- Symmetric Key Encryption
- Asymmetric Key Encryption

Other (1)

W06D4 Schedule »