Asymmetric Key Encryption

Reading

10m - 25m

Status | Incomplete

Introduction

Asymmetric cryptography is a framework that uses public and private keys instead of just the private keys used in the symmetric cryptography system. Key pairs provide public-key cryptography (PKC) with unique characteristics and capabilities that can be used to solve challenges inherent in other cryptographic techniques. This form of encryption has become an essential element of modern computer security and a critical component of the growing cryptocurrency ecosystem.

How Does Public Key Encryption Work?

In a PKC system, the public key is used by a sender to encrypt information, while the recipient uses the private key to decrypt that information. Since the two keys are different, the public key can be shared freely without compromising the security of the private key. Each asymmetric key pair is unique, ensuring that the person can only read a message encrypted using a public key with the corresponding private key.

Because asymmetric encryption algorithms generate key pairs that are mathematically linked, the length of these keys is much greater than that found in symmetric encryption. This longer length, typically between 1024 and 2048 bits, makes it extremely difficult to identify a private key using the public key as a basis.

One of the most common algorithms for asymmetric encryption in use today is known as the RSA algorithm which was first described in 1977 by Rivest, Shamir, and Adleman. Introduced by MIT colleagues Ron Rivest, Adi Shamir, and Leonard Adleman, RSA—its name derived from the initials of their surnames—is a specific type of PKC. Rivest, with Shamir and Adleman, developed cryptographic algorithms and techniques to practically enable secure encoding and decoding of messages between communicating parties. It has remained an essential component of PKC systems today.

> The RSA scheme generates keys using a module obtained by multiplying two numbers (usually two large prime numbers). In basic terms, the module generates two keys: a public one that can be shared and a private one that must be kept secret.

Asymmetric Key Encryption Tool

PKC solves one of the long-standing problems with symmetric algorithms, which is communicating the key used for both encryption and decryption at the same time. Sending this key over an insecure connection can expose it to third parties who can read any message encrypted with the shared key. Although cryptographic techniques exist to solve this problem, they are still vulnerable to attacks. In PKC, on the other hand, the key used for encryption can be shared securely over any connection. As a result, asymmetric algorithms offer a higher level of protection when compared to symmetric ones.

Use in Digital Signatures

Another application of asymmetric encryption algorithms is data authentication through digital signatures. A digital signature is a hash created using data from a message. When this message is sent, the recipient can verify the signature using the sender's public key to authenticate the message's origin and ensure that it has not been tampered with. In some cases, digital signatures and encryption are applied together, as the hash can be encrypted as part of the message. It should be noted, however, that not all digital signature schemes use encryption techniques.

Limitations

While it can enhance computer security and provide message integrity checking, PKC has some limitations. Due to the complex mathematical operations involved in encryption and decryption, asymmetric algorithms can be slow when forced to deal with large amounts of data. This type of encryption also relies heavily on the assumption that the private key will remain secret. If a private key is accidentally shared or exposed, the security of all encrypted messages with their corresponding public key will be compromised. It is also possible for users to accidentally lose their private keys, making it impossible to access the encrypted data.

Applications of PKC

Many modern computer systems use this type of encryption to secure sensitive information. E-mails can be encrypted using public key encryption techniques to keep contents confidential. The SSL protocol, which makes secure connections possible, also employs asymmetric cryptography. PKC systems have been explored to provide a safe electronic voting environment.

PKC also stands out in the world of blockchains and cryptocurrencies. A key pair is generated (public and private) when a new cryptocurrency wallet is set up. The public address is created using the public key and can be safely shared with others. On the other hand, the private key is used to create digital signatures and verify transactions, so it must be kept secret. Once a transaction is verified by confirming the hash contained in the digital signature, that transaction can be added to the blockchain ledger. This digital signature verification system ensures that only the person with the private key associated with the corresponding cryptocurrency wallet can release funds from it. Asymmetric ciphers used in cryptocurrency applications differ from those used for computer security purposes. Bitcoin and Ethereum, for example, use the Elliptic Curve Digital Signature Algorithm (ECDSA) to verify transactions.

PKC is essential in protecting modern digital systems, from securing computers to verifying cryptocurrency transactions. Using paired public and private keys, asymmetric cryptography algorithms solve the fundamental security problems presented by symmetric ciphers. While PKC has been around for many years, new uses and applications are regularly being developed, particularly in the blockchain and cryptocurrency space.

> Where two different keys are used for encryption and decryption. Each user has a pair of keys: a public key and a private key. The public key is freely available and can be shared with anyone, while the private key is kept secret and is only known to the owner.

Conclusion

Asymmetric cryptography provides a more secure method of encryption than symmetric cryptography because the private key is never shared or transmitted, making it difficult for attackers to decrypt the data even if they intercept the communication. However, asymmetric cryptography is typically slower and more computationally intensive than symmetric cryptography.

✓ Mark Completed

←
Previous
Symmetric 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 »