Public Key Cryptography

Guide: ShaneHadden
Generated: 2026-11-02 10:48

What is public key cryptography

Public key cryptography is a method of securing communication using two keys: a public key, which anyone can access, and a private key, which is kept secret. The public key encrypts data, while the private key decrypts it. This allows secure data exchange without sharing the private key. It's widely used for secure online transactions, email encryption, and digital signatures, ensuring confidentiality and authenticity in communications.

What type of encryption is used in public key cryptography?

Public key cryptography uses asymmetric encryption. In this method, two keys are generated: a public key, which can be shared openly, and a private key, which is kept secret. Data encrypted with the public key can only be decrypted with the corresponding private key, ensuring secure communication.

How is asymmetric encryption different from symmetric encryption?

Asymmetric encryption uses two keys: a public key for encryption and a private key for decryption. This allows secure communication without sharing the private key. In contrast, symmetric encryption uses a single key for both encryption and decryption, requiring both parties to share this key securely. Asymmetric encryption is generally slower but offers better security for key exchange, while symmetric encryption is faster and more efficient for encrypting large amounts of data.

What is the problem with symmetric encryption? Why is asymmetric encryption needed?

The problem with symmetric encryption is that both parties must share the same secret key, which can be risky if the key is intercepted or if many users need access. Asymmetric encryption solves this by using two keys: a public key for encryption and a private key for decryption. This allows secure communication without needing to share a secret key, making it safer for online transactions and communications.

Who invented asymmetric encryption?

Asymmetric encryption, also known as public key cryptography, was invented by Whitfield Diffie and Martin Hellman in 1976. They introduced the concept in their groundbreaking paper, which outlined how two parties could communicate securely over an insecure channel using a pair of keys: a public key for encryption and a private key for decryption.

What is RSA?

RSA (Rivest-Shamir-Adleman) is a widely used public key cryptography algorithm. It relies on the mathematical properties of large prime numbers. RSA generates two keys: a public key for encryption and a private key for decryption. The security of RSA is based on the difficulty of factoring the product of two large prime numbers. RSA is commonly used for secure data transmission, digital signatures, and authentication in various applications.

How does bitcoin use public key cryptography?

Bitcoin uses public key cryptography to secure transactions and control the creation of new units. Each user has a pair of keys: a public key, which is shared and acts like an address, and a private key, which is kept secret. When a user wants to send bitcoin, they sign the transaction with their private key, proving ownership. The transaction is then broadcasted, and nodes verify it using the sender's public key. This ensures that only the rightful owner can spend their bitcoin, maintaining sec

How do internet browsers use public key cryptography?

Internet browsers use public key cryptography to secure communications between users and websites. When you connect to a secure site (HTTPS), the browser retrieves the site's public key from its SSL/TLS certificate. This key encrypts data sent to the server, ensuring that only the server, with its private key, can decrypt it. This process establishes a secure connection, protecting sensitive information like passwords and credit card numbers from eavesdroppers during transmission.

What is public key infrastructure (PKI)?

Public Key Infrastructure (PKI) is a framework that enables secure communication and authentication over networks. It uses a pair of keys: a public key, which can be shared widely, and a private key, which is kept secret. PKI includes components like digital certificates, Certificate Authorities (CAs), and registration authorities that verify identities. It ensures data integrity, confidentiality, and authenticity, allowing users to exchange information securely.

What is a Certificate Authority?

A Certificate Authority (CA) is an entity that issues digital certificates to verify the identity of organizations or individuals. These certificates contain a public key and information about the entity. The CA ensures that the public key belongs to the entity it claims to represent, enabling secure communication and trust in online transactions. Users can verify the authenticity of a certificate by checking its signature against the CA's public key.

Explain how public key encryption is used to create a digital signature.

Public key encryption creates a digital signature by using a private key to sign a message and a public key to verify it. The sender creates a hash of the message and encrypts it with their private key, producing the signature. This signature is sent along with the message. The recipient uses the sender's public key to decrypt the signature, revealing the hash. They then hash the received message and compare it to the decrypted hash. If they match, the signature is valid, confirming the message'

How do credit cards use public key encryption.

Credit cards use public key encryption to secure transactions. When you make a purchase, your card information is encrypted using the merchant's public key. This ensures that only the merchant can decrypt the information with their private key. This process protects your data from being intercepted by unauthorized parties during transmission. Additionally, public key infrastructure helps verify the identity of the merchant, ensuring that you are communicating with a legitimate entity.