Elliptic Curve Cryptography Suite

Griffin Ryan

December 8th, 2023

Introduction

In the digital age, data security and privacy have become paramount concerns. Cryptography plays a crucial role in safeguarding sensitive information, enabling secure communication, and protecting digital assets. To address these concerns, we have developed a versatile and secure cryptographic utility that empowers users to perform various cryptographic operations, such as hashing, message authentication, encryption, and decryption.

Overview of Elliptic Curve Cryptography Suite

This document presents an overview of an advanced cryptographic suite that leverages elliptic curve cryptography (ECC), specifically utilizing the Ed448 curve. The suite provides robust security features, including hashing, key pair generation, encryption, decryption, digital signing, and signature verification. Its implementation is based on SHA-3 derived functions and Schnorr signatures, offering high security and efficiency.

Key Features

Elliptic Curve Cryptography (ECC) with Ed448:

Utilizes the Ed448 elliptic curve, known for its strong security properties and resistance to common cryptographic attacks.

Capable of generating public and private key pairs on the Ed448 curve.

SHA-3 Derived Hashing (KMACXOF256)

Implements the KMACXOF256 function, a variant of the SHA-3 family's Keccak hash function, for key derivation and data integrity checks.

Elliptic Curve Diffie-Hellman Integrated Encryption Scheme (EC-DHIES)

Provides a secure method for encrypting and decrypting data using elliptic curve cryptography. Employs a combination of ECC for key exchange and symmetric encryption (like AES) for encrypting the actual data.

Schnorr Signature Scheme

Implements the Schnorr signature algorithm for signing and verifying data, which is known for its simplicity and efficiency.

The signing process involves creating a hash of the data, followed by elliptic curve operations using the private key. Verification involves confirming the signature's validity with the corresponding public key.

Functionalities

Hashing

Generates cryptographic hashes of data using the cSHAKE256 function.
Provides a secure way to verify data integrity.

Key Pair Generation

Generates elliptic curve key pairs, allowing users to securely create public and private keys for encryption, decryption, and signing.
Encryption & Decryption:

Encrypts data using the recipient's public key and decrypts using the corresponding private key.
Supports both file-based and direct text input/output for encryption and decryption processes.
Digital Signing & Verification:

Generates digital signatures for data files or direct text input using the private key.
Verifies the authenticity and integrity of signed data using the corresponding public key.

Ed448Point Represents points on the Ed448 curve.

EllipticCurveEncryptor Manages key pair generation, encryption, decryption, signing, and verification.

Implements SHA-256 and cSHAKE256 hash functions.

Usage

Getting Started

To begin using the cryptographic suite, users must first have a Java environment set up, as the suite is developed in Java. After ensuring Java is installed, the suite can be run from the command line or integrated into other Java applications.

Encrypting Data

Users can choose to encrypt either a file or direct text input. The encryption process requires the recipient's public key. The encrypted data is saved to a file, ensuring secure storage or transmission.

Decrypting Data

For decryption, users provide the path to the encrypted file and enter the passphrase for their private key. The suite decrypts the data and can output it either as a file or directly display the decrypted text.

Digital Signing and Verification

Signing Data

The suite allows signing of either file-based data or direct text input.
Users need to provide their private key passphrase for signing. The generated signature is saved to a file, which can be used later for verification.

Verifying Signatures

To verify a signature, users must have the original data, the signature file, and the signer's public key. The suite checks the signature's validity and confirms whether it matches the provided data and public key.

To generate an elliptic curve key pair, users can select the 'generate key pair' option from the main menu. The suite prompts for a passphrase, which is then used to derive the private key securely. The corresponding public key is computed on the Ed448 curve.
Both keys are stored in separate files, with the private key being encrypted for security.

Security Considerations

Emphasizes the use of secure random number generation for key pair creation and signing.
Ensures that cryptographic operations conform to the standards of the ECC and SHA-3.

This cryptographic suite is suitable for applications requiring high levels of data security, including secure communications systems, data integrity verification systems, cryptographic authentication processes, secure data storage and transmission, and more.

This ECC cryptographic suite offers a comprehensive set of tools for modern security needs, combining the strength of elliptic curve cryptography with advanced hashing and signature algorithms, which considers robust cryptography practice.