Introduction

The purpose of the project is to develop and implement a secure file transfer application designed to ensure the confidentiality, integrity, and authenticity of digital files during transmission. The project leverages a combination of modern and classical cryptographic techniques: the International Data Encryption Algorithm (IDEA) in Cipher Block Chaining (CBC) mode, the Merkle-Hellman Knapsack (MHK) cryptosystem for secure private session key exchange, and Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures.

Project Components

This project integrates three primary cryptographic components:

IDEA + CBC: IDEA is a block cipher that operates on 64-bit blocks with a 128-bit key. It is used in Cipher Block Chaining (CBC) mode to encrypt and decrypt the file content, ensuring confidentiality. CBC mode enhances security by linking each ciphertext block to the previous one, hiding patterns in the plaintext

Merkle-Hellman Key Management: Merkle-Hellman Key Management is employed for the secure delivery of the ephemeral IDEA private session key. It is a public-key cryptosystem that allows a sender to encrypt the private session key using the receiver's public key, which can then be unwrapped by the receiver using their private key.

Elliptic Curve Digital Signature Algorithm: provides authenticity and integrity for the transferred files. It enables the sender to create a unique signature for the encrypted file, which the receiver can verify using the sender's public key to ensure the file has not been tampered with and originated from the legitimate sender.

Project Flow

We started with an in-depth study of the given cryptographic algorithms: IDEA and CBC for encryption, Merkle-Hellman for key exchange, and ECDSA for authentication. After thoroughly understanding their theoretical foundations and operational mechanisms, basic simulations were developed to test their functionalities and ensure correct implementation. These algorithms were then integrated into a system, followed by error correction.

Implementation Process

IDEA + CBC

Encryption: The sender encrypts the plaintext file using a randomly generated 128-bit IDEA private session key in CBC mode.

Decryption: The receiver decrypts the ciphertext back to plaintext using the same IDEA private session key

Merkle-Hellman Key Exchange

Key Generation: The receiver generates a Merkle-Hellman private key and corresponding public key.

Key Wrapping: The sender securely wraps the IDEA private session key using the receiver's Merkle-Hellman public key

Key Unwrapping: The receiver recovers the IDEA private session key using their Merkle-Hellman private key.

Elliptic Curve Digital Signature Algorithm

Key Generation: The sender generates an ECDSA public-private key pair derived from their passphrase.

Signing: The sender signs the encrypted file using their ECDSA private key.

Verification: The receiver verifies the signature using the sender's ECDSA public key to ensure message authenticity and integrity.

Obtained Results

The system successfully demonstrated secure file communication by:

- Encrypting and decrypting files with IDEA-CBC: Confidentiality was successfully maintained, preventing unauthorized access to file contents.
- Exchanging encryption keys securely using Merkle-Hellman: The private session key for IDEA encryption was securely transmitted, ensuring that only the intended recipient could recover it.
- Authenticating file messages with ECDSA signatures: File integrity and sender authenticity were verified, protecting against tampering and ensuring the origin of the message.

Conclusions

This project achieved its goal of building a secure file exchange system by integrating IDEA + CBC mode, Merkle-Hellman, and ECDSA. By implementing these cryptographic algorithms, we gained valuable insights into their operational mechanisms and the importance of each step in ensuring secure communication.