Secure File Encryption Using AES with Password Protection

TEAM MEMBERS:

Praveen P Hebbal (1RV22CS149)
Prajwal M Biradar (1RV22CS141)
PavanKumar R (1RV22CS136)
Gopinath Ramaje (1RV23CS404)

CONTENTS

01.

Introduction to AES Encryption

02.

AES Encryption Mechanism

03.

Implementing AES File Encryption

04.

Security Considerations

01

Introduction to AES Encryption

Overview of AES

What is AES?

AES, or Advanced Encryption Standard, is a symmetric encryption algorithm widely used across the globe to secure data through a series of fixed block sizes and key lengths.

History and Development

AES was established in 2001 by the National Institute of Standards and Technology (NIST) as a replacement for the older DES algorithm, following a rigorous evaluation process of several candidate algorithms.

Importance of File Encryption

Data Privacy

File encryption, particularly using AES, plays a crucial role in ensuring sensitive data remains confidential and accessible only to authorized users, protecting against unauthorized access.

Cybersecurity Threats

With the rise of cyberattacks, encryption like AES is essential in combating threats such as data breaches and ransomware, providing a defense mechanism to safeguard sensitive information.

02

AES Encryption Mechanism

How AES Works

Key Sizes

AES supports key sizes of 128, 192, and 256 bits, with increased key lengths providing enhanced security against brute- force attacks and ensuring data confidentiality.

Encryption Process

The AES encryption process involves multiple rounds of substitution, permutation, and mixing of the plaintext with a secret key, transforming it into ciphertext through a series of well- defined steps.

Modes of AES Operation

ECB Mode

Electronic Codebook (ECB) mode encrypts each block of plaintext independently, making it fast and simple but vulnerable to pattern attacks, compromising data security in certain conditions.

CBC Mode

Cipher Block Chaining (CBC) mode enhances security by linking blocks through an Initialization Vector (IV), ensuring that identical plaintext blocks yield different ciphertext, thereby preventing pattern recognition.

GCM Mode

Galois/Counter Mode (GCM) combines the advantages of counter mode encryption with authentication, providing both data confidentiality and integrity, making it ideal for modern secure communications.

03

Implementing AES File Encryption

Required Tools and Libraries

Programming Languages

Various programming languages can be used for implementing AES encryption, including Python, Java, and C++. Each has its own syntax and libraries suited for cryptographic operations.

Cryptography Libraries

Popular cryptography libraries such as PyCryptodome for Python and Bouncy Castle for Java provide built- in functions for AES encryption, making implementation easier and more secure.

Step-by-Step File Encryption

Generating a Password

A strong password should be generated using a combination of letters, numbers, and symbols. This password will serve as the key for the AES encryption process.

Saving the Encrypted File

After encryption, the transformed file should be saved to a secure location, ensuring that it is protected against unauthorized access or data breaches.

Encrypting the File

The actual encryption process takes the selected file and the generated password, using the AES algorithm to convert the file's contents into an unreadable format.

04

Security Considerations

Choosing a Strong Password

Password Length and Complexity

A strong password should be at least 12 characters long, incorporating a mix of uppercase letters, lowercase letters, numbers, and special symbols to enhance security.

Password Management Tools

Utilizing password management tools allows users to generate, store, and manage complex passwords securely, reducing the risk of password reuse and facilitating effortless login processes.

Best Practices for File Encryption

Regular Key Rotation

Regularly changing encryption keys helps to minimize the risk of unauthorized access, ensuring that even if a key is compromised, its effectiveness is limited over time.

Backup of Encrypted Files

Maintaining backups of encrypted files ensures data recovery in case of loss, while protecting sensitive information from unauthorized access through robust encryption methods.

Thanks