20MCA245 MINI PROJECT

APPROVAL BY GUIDE

Name of the Student: ABDUL KHADAR.MS

Roll No: CHN24MCA2001

Project Title: CLOSED BOOK(Personal Vault)

Abstract

This is a web application designed to generate, manage, and secure passwords. These passwords are stored in an encrypted database and protected behind a master password.

The password storage app provides strong encryption, offering a robust defense against cyber criminals. By using this app, users can store all their passwords in one secure database, requiring them to remember only one master key to access all their stored credentials at any time.

Key Features:

Passwords are hashed or encrypted before being stored.

To retrieve a password, users simply copy and paste it, effectively avoiding key-logger attacks.

Besides passwords, the app also supports storage of various data file formats, including:

Video

Audio

Image

Text

Document files

All this data is kept in a secure, encrypted environment, accessible only through the master password. The files and passwords are encrypted using multiple random algorithms, ensuring maximum security.

This encrypted application can securely store any type of data and passwords, making it a comprehensive personal security vault.

—

Encryption Techniques Used:

1. Hash Algorithm:

A hashing algorithm is a mathematical function that scrambles data into an unreadable format.

It is a one-way function, meaning the original text cannot be reversed or decoded.

Commonly used for verifying password integrity and storing data securely.

2. AES Algorithm (Advanced Encryption Standard):

A symmetric block cipher algorithm that encrypts data in 128-bit blocks.

Supports key lengths of 128, 192, and 256 bits.

Recognized worldwide for its security and performance.

Used for encrypting stored data within the application.
3. RSA Algorithm (Rivest–Shamir–Adleman):
A public-key encryption algorithm widely used to secure data over the internet.
Forms the core of many cryptosystems providing confidentiality, integrity, and authenticity.
Often used for encrypting master keys or communication between clients and servers.
—

This multi-layered encryption approach ensures that only the master password holder can access the data, making the app a highly secure platform for storing both passwords and private files.

Signature of student:

Any remarks of guide:

Name and signature of guide with date: