**TOPIC: AES-256 APPLICATION IN PASSWORD MANAGER**

|  |  |
| --- | --- |
| **Sinh viên thực hiện:** Nguyễn Đức Hiếu | **MSSV:** 22070072 |
| **Lecturer:** TS. Diêm Công Hoàng |  |
|  |  |

Table of Contents

[**Part I : Tính cấp thiết của đề tài** 2](#_Toc194741006)

[**Part II: Project objectives** 3](#_Toc194741007)

[I. Mục tiêu chung 3](#_Toc194741008)

[II. Mục tiêu cụ thể 3](#_Toc194741009)

[**Part III: Nội dung nghiên cứu** 4](#_Toc194741010)

[I. Introduction 4](#_Toc194741011)

[II. Theoretical basis 4](#_Toc194741012)

[III. Solution Theory 5](#_Toc194741013)

[**Part IV: Implementation** 6](#_Toc194741014)

[**REFERENCE** 7](#_Toc194741015)

## **Part I : Tính cấp thiết của đề tài**

* Introduction to password managers and their critical role in cybersecurity
* Overview of encryption in password management systems
* Significance of AES-256 as an industry standard for password vaults
* Current landscape of threats to password security
* The need for robust encryption in modern password management
* Introduction to the proposed password manager solution

## **Part II: Project objectives**

### Mục tiêu chung

* Analyze the implementation of AES-256 encryption in password manager applications
* Evaluate the security benefits provided by AES-256 in protecting sensitive credentials
* Develop a secure password management system utilizing AES-256 encryption

### Mục tiêu cụ thể

* Design and implement a phrase-based password generation system
* Create a password strength analysis tool with visual feedback
* Develop a secure password retrieval mechanism
* Implement master password management with strong key derivation
* Design an AES-256 encrypted vault for secure credential storage

## **Part III: Nội dung nghiên cứu**

### Introduction

### Theoretical basis

1. Foundational cryptographic principles
   1. Symmetric vs. asymmetric encryption
   2. Block ciphers and their characteristics
   3. Encryption modes of operation (GCM)
2. AES-256 algorithm detailed analysis
   1. Historical development and NIST selection
   2. Mathematical foundations (Galois fields, substitution-permutation network)
   3. Key expansion algorithm
   4. Encryption rounds (SubBytes, ShiftRows, MixColumns, AddRoundKey)
   5. Decryption process and inverse operations
3. Password strength fundamentals
   1. Entropy calculation methods
   2. Brute force resistance metrics
   3. Common password vulnerabilities
4. Key derivation functions
   1. PBKDF2 Scrypt theoretical foundations
   2. Security parameters and iteration counts
   3. Salt generation and management

### Solution Theory

1. Password manager cryptographic architecture

* End-to-end encryption models
* Zero-knowledge design principles
* Master password transformation into encryption keys

1. Implementation of AES-256 in password vault context

* Database encryption strategies
* Memory security considerations
* Secure password generation algorithms

1. Password strength analysis methodologies

* Scoring systems and metrics
* Visual feedback mechanisms
* Improvement recommendations

1. Secure retrieval mechanisms

* Copy functionality with security considerations
* Temporary memory handling
* Browser integration security

## **Part IV: Implementation**

1. Function:

* Password generation: nhập một hoặc một số cụm từ quen thuộc 🡪 tạo một mật khẩu dựa theo cụm từ đó mà đảm bảo secure strong password requirement | nhập một mật khẩu mới 10-digit
* Password strength analysis: nhập một mật khẩu bất kỳ, đối chiếu các thành phần mật khẩu với các tiêu chí để chấm điểm (nếu đáp ứng thì tích v xanh; không đáp ứng thì tích x đỏ)
* Password Retrieval: xem hoặc copy khi cần thiết (button)
* Master Password Management: một mã 6 số được sinh liên tục trong 30s
* Secure Storage (Encrypted Vault): store in a encrypted database

## **REFERENCE**

[1]. Cryptography and Network Security: Principles and Practice

[2]. NIST Special Publication 800-38D

[3]. Understanding Cryptography

[4]. NIST Special Publication 197

[5]. NIST SP 800-132, "Recommendation for Password-Based Key Derivation"

[6]. NIST SP 800-63B