**Tên đề tài:** Cài Đặt Thuật Toán Mã Hóa AES Hàm Băm SHA-256 Và Ứng Dụng

**Mục tiêu:**

Tìm hiểu và nắm vững nguyên lý hoạt động của thuật toán mã hóa đối xứng **AES (Advanced Encryption Standard)** và hàm băm **SHA-256 (Secure Hash Algorithm 256-bit)**, đồng thời ứng dụng chúng trong bảo mật thông tin. Thông qua nghiên cứu này, người thực hiện sẽ hiểu rõ cách thức hoạt động của các thuật toán mã hóa và băm, bao gồm các bước xử lý dữ liệu, vòng lặp tính toán và nguyên tắc bảo mật. Đề tài hướng đến việc cài đặt thuật toán AES và SHA-256 từ đầu mà không sử dụng thư viện hỗ trợ sẵn có trong Java, giúp hiểu sâu hơn về cách chúng hoạt động ở mức thấp. Ngoài ra, một giao diện đồ họa trực quan cũng sẽ được xây dựng để hỗ trợ người dùng nhập dữ liệu, thực hiện mã hóa/băm, và hiển thị kết quả một cách dễ dàng. Việc thực hiện nghiên cứu này không chỉ giúp nâng cao kiến thức về mật mã học mà còn mở ra tiềm năng ứng dụng vào thực tế, đặc biệt trong các hệ thống bảo mật dữ liệu như quản lý mật khẩu, truyền thông an toàn và xác thực thông tin số.

**Nội dung chính của đề tài:**

**1. Tổng quan về đề tài**

* Giới thiệu về tầm quan trọng của bảo mật thông tin trong kỷ nguyên số.
* Tổng quan về thuật toán mã hóa AES và hàm băm SHA-256, cùng với vai trò của chúng trong bảo mật dữ liệu.
* Các ứng dụng thực tế của AES và SHA-256 trong hệ thống bảo mật, ngân hàng, thương mại điện tử và lưu trữ thông tin.
* Mục đích của đề tài và những đóng góp của nghiên cứu này trong việc hiểu sâu hơn về các thuật toán mã hóa và băm.

**2. Cơ sở lý thuyết**

* **Giới thiệu về mật mã học**: Tổng quan về mã hóa đối xứng và bất đối xứng, các thuật toán phổ biến và ứng dụng.
* **Thuật toán AES**:
  + Lịch sử và sự phát triển của AES.
  + Cấu trúc thuật toán, kích thước khóa (128-bit, 192-bit, 256-bit).
  + Các bước chính: **Thay thế byte (SubBytes), Dịch hàng (ShiftRows), Trộn cột (MixColumns), Cộng khóa vòng (AddRoundKey)**.
  + Quy trình tạo khóa con (Key Expansion) và cách hoạt động của các vòng lặp mã hóa.
* **Hàm băm SHA-256**:
  + Nguyên lý hoạt động của hàm băm và tính chất của SHA-256.
  + Các bước xử lý: **Nén dữ liệu, Padding, Chia khối, Vòng lặp xử lý với các phép toán logic (AND, OR, XOR, ROTATE RIGHT)**.
  + Cách SHA-256 đảm bảo tính toàn vẹn dữ liệu.

**3. Phân tích và cài đặt chương trình**

* **Thiết kế và cài đặt thuật toán AES**:
  + Cấu trúc chương trình và cách tổ chức mã nguồn.
  + Cách triển khai từng bước của thuật toán bằng Java mà không sử dụng thư viện hỗ trợ.
  + Kiểm tra và đánh giá kết quả so với tiêu chuẩn AES.
* **Thiết kế và cài đặt thuật toán SHA-256**:
  + Xây dựng chương trình băm dữ liệu với SHA-256 từ đầu.
  + Xử lý dữ liệu đầu vào và tạo giá trị băm đúng theo tiêu chuẩn.
  + So sánh kết quả với các công cụ băm SHA-256 phổ biến khác.
* **Xây dựng giao diện người dùng**:
  + Thiết kế một ứng dụng Java GUI đơn giản để nhập dữ liệu và hiển thị kết quả mã hóa/băm.
  + Hiển thị từng bước xử lý của thuật toán để giúp người dùng hiểu rõ hơn về cách hoạt động.
  + Hỗ trợ sao chép hoặc lưu trữ kết quả đầu ra.

**4. Kết luận và hướng phát triển**

* Tổng kết những điểm quan trọng đã đạt được trong quá trình nghiên cứu và triển khai.
* Đánh giá hiệu suất của thuật toán AES và SHA-256 so với các thư viện có sẵn trong Java.
* Các thách thức gặp phải khi cài đặt thuật toán từ đầu mà không sử dụng thư viện.
* Đề xuất hướng phát triển trong tương lai:
  + **Tối ưu hiệu suất** bằng cách sử dụng kỹ thuật lập trình song song.
  + **Ứng dụng thực tế** trong hệ thống bảo mật, ví dụ như bảo vệ mật khẩu người dùng hoặc mã hóa dữ liệu nhạy cảm.
  + **Nâng cấp thuật toán** bằng cách tích hợp với các phương pháp mã hóa bất đối xứng như RSA hoặc ECC.

**Tài liệu tham khảo:**

1. Phạm Văn Nam (2011, 2013), *Lập trình hướng đối tượng Java*. Thư viện Trường Đại học Nha Trang, Nha Trang.
2. Trần Minh Văn (2011), *Giáo trình An toàn và bảo mật thông tin*. Thư viện Trường Đại học Nha Trang, Nha Trang.
3. Trần Thị Kim Thủy (2012), *Nghiên Cứu Về Ứng Dụng Chuẩn Mật Mã Nâng Cao (AES) Trong Xây Dựng Hàm Băm*, Luận văn thạc sĩ, Học Viện Công Nghệ Bưu Chính Viễn Thông, Hà Nội.
4. <https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm> (simpliearn, 2024, Hướng dẫn dứt khoát để tìm hiểu SHA-256 (Thuật toán băm an toàn)).