BỘ ĐỀ TÀI ĐỒ ÁN HỌC PHẦN MÃ HOÁ VÀ ỨNG DỤNG

Đề tài 1. Xây dựng trình mô phỏng thuật toán DES (Data Encryption Standard)

- **Mục tiêu:** Hiểu sâu về cấu trúc mạng Feistel, quá trình sinh khóa con (key scheduling), và vai trò của các thành phần S-boxes, P-boxes.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày chi tiết kiến trúc của DES, đặc biệt là cấu trúc Feistel và hàm F.
    2. **Hiện thực:** Xây dựng chương trình mô phỏng quá trình mã hóa/giải mã của DES qua 16 vòng. Cho phép người dùng nhập bản rõ và khóa, sau đó hiển thị kết quả sau mỗi vòng.
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo chi tiết về thuật toán, và demo chương trình mô phỏng.

Đề tài 2. Phân tích các Chế độ Hoạt động của Mật mã Khối (Block Cipher Modes)

- **Mục tiêu:** Trực quan hóa sự khác biệt về an ninh giữa các chế độ hoạt động, đặc biệt là điểm yếu của ECB.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Tìm hiểu về 5 chế độ: ECB, CBC, CFB, OFB, và CTR.
    2. **Hiện thực:** Viết chương trình sử dụng một thư viện mật mã có sẵn (ví dụ: OpenSSL, PyCryptodome) để mã hóa một file ảnh (định dạng BMP) bằng thuật toán AES với các chế độ ECB và CBC.
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo so sánh kết quả (hình ảnh sau khi mã hóa), phân tích ưu/nhược điểm của từng chế độ và giải thích tại sao ECB không an toàn.

Đề tài 3. So sánh hiệu năng và cấu trúc của AES và Triple DES (3DES)

- **Mục tiêu:** Đánh giá hiệu suất và độ phức tạp của chuẩn mã hóa hiện đại (AES) so với giải pháp kế thừa (3DES).

- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Phân tích sự khác biệt về cấu trúc (Feistel vs. SPN), kích thước khóa/khối, và lịch sử ra đời của 3DES và AES.
    2. **Hiện thực:** Viết một chương trình benchmark để đo tốc độ mã hóa của AES-128 và 3DES trên các file có kích thước khác nhau (ví dụ: 1MB, 10MB, 100MB).
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo phân tích kiến trúc, vẽ đồ thị so sánh hiệu năng và đưa ra kết luận.

Đề tài 4. **Xây dựng ứng dụng Chữ ký số sử dụng RSA**

- **Mục tiêu:** Áp dụng RSA và hàm băm để hiện thực hóa một hệ thống chữ ký số, đảm bảo tính toàn vẹn, xác thực và chống chối bỏ.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày quy trình tạo và xác thực chữ ký số (Hash-then-Sign).
    2. **Hiện thực:** Xây dựng cặp chương trình: một chương trình signer nhận đầu vào là một file và khóa bí mật, tạo ra file chữ ký; một chương trình verifier nhận đầu vào là file gốc, file chữ ký và khóa công khai để xác thực. Sử dụng hàm băm SHA-256.
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo phân tích và demo việc ký và xác thực thành công/thất bại.

Đề tài 5. **Mô phỏng Giao thức trao đổi khóa Diffie-Hellman**

- **Mục tiêu:** Hiểu cách hai bên có thể thiết lập một khóa bí mật chung trên một kênh truyền không an toàn.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày cơ sở toán học của Diffie-Hellman (bài toán Logarit rời rạc).
    2. **Hiện thực:** Xây dựng một chương trình mô phỏng cuộc trao đổi giữa hai bên (Alice và Bob). Chương trình cần hiển thị các giá trị công khai được trao đổi và khóa bí mật chung được tạo ra ở cả hai phía.
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo giải thích giao thức, và phân tích về tấn công Man-in-the-Middle đối với Diffie-Hellman cơ bản.

Đề tài 6. **Xây dựng hệ thống lưu trữ Mật khẩu An toàn sử dụng Salt và Hashing**

- **Mục tiêu:** Áp dụng đúng các kỹ thuật băm an toàn để bảo vệ thông tin nhạy cảm của người dùng.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Phân tích các rủi ro của việc lưu mật khẩu dạng bản rõ hoặc băm đơn thuần. Giải thích vai trò của **Salt** và **Stretching** (ví dụ: PBKDF2, Scrypt).
    2. **Hiện thực:** Xây dựng một ứng dụng web/dòng lệnh đơn giản có chức năng đăng ký và đăng nhập. Mật khẩu người dùng phải được lưu trong cơ sở dữ liệu dưới dạng băm có salt (sử dụng SHA-256 hoặc cao hơn).
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo giải thích kiến trúc, và demo hệ thống.

Đề tài 7. **Hiện thực hóa HMAC (Hash-based Message Authentication Code)**

- **Mục tiêu:** Hiểu sự khác biệt giữa đảm bảo tính toàn vẹn (hàm băm) và đảm bảo cả tính toàn vẹn lẫn xác thực (HMAC).
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày cấu trúc và quy trình tính toán của HMAC theo chuẩn RFC 2104.
    2. **Hiện thực:** Viết một hàm HMAC-SHA256 từ đầu (không dùng thư viện có sẵn). Viết chương trình cho phép người dùng nhập một thông điệp và một khóa bí mật để tạo ra mã HMAC.
    3. **Sản phẩm:** Nộp mã nguồn, báo cáo phân tích, và so sánh kết quả của hàm tự viết với một thư viện chuẩn để kiểm tra tính đúng đắn.

Đề tài 8. **Phân tích và Phá mã Vigenère bằng Phân tích Tần suất**

- **Mục tiêu:** Hiểu rõ cơ chế của mật mã đa bảng và chứng minh điểm yếu của nó khi độ dài khóa bị lộ thông qua phương pháp Kasiski và phân tích tần suất.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày về mật mã Vigenère, phương pháp Kasiski để ước tính độ dài khóa, và kỹ thuật phân tích tần suất trên từng bảng chữ cái.
    2. **Hiện thực:** Xây dựng một công cụ bằng Python/C++ có khả năng:
        - Mã hóa và giải mã văn bản bằng Vigenère.
        - Tự động phá mã một bản mã Vigenère đủ dài mà không cần biết khóa.
    3. **Sản phẩm:** Mã nguồn, báo cáo phân tích thuật toán, và demo phá mã thành công.

Đề tài 9. **Nghiên cứu Lý thuyết Số học và Ứng dụng trong Mật mã**

- **Mục tiêu:** Nắm vững các công cụ toán học nền tảng (số học modulo, định lý Euler, thuật toán Euclid mở rộng) là cơ sở cho mật mã khóa công khai.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Viết một báo cáo kỹ thuật tổng hợp về các khái niệm toán học quan trọng được trình bày trong sách.
    2. **Hiện thực:** Xây dựng một thư viện toán học nhỏ thực hiện các hàm:
        - Tính nghịch đảo modulo bằng thuật toán Euclid mở rộng.
        - Tính lũy thừa theo modulo (Modular Exponentiation) hiệu quả.
    3. **Sản phẩm:** Thư viện mã nguồn và báo cáo kỹ thuật.

Đề tài 10. **So sánh Trực quan các Chế độ Hoạt động của Mật mã Khối**

- **Mục tiêu:** Chứng minh bằng thực nghiệm tầm quan trọng của việc chọn đúng chế độ hoạt động và hiểm họa của việc sử dụng sai chế độ (đặc biệt là ECB).
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Phân tích ưu/nhược điểm của các chế độ ECB, CBC, CTR và GCM.
    2. **Hiện thực:** Viết chương trình sử dụng thư viện mật mã có sẵn (ví dụ: OpenSSL, PyCryptodome) để mã hóa một file ảnh BMP bằng thuật toán AES với 4 chế độ trên.

3. **Sản phẩm:** Báo cáo so sánh kết quả (hình ảnh sau mã hóa), phân tích sự khác biệt và giải thích tại sao GCM là lựa chọn tốt cho nhiều ứng dụng hiện đại.

Đề tài 11. **Đánh giá Hiệu năng giữa Mật mã Dòng và Mật mã Khối**

- **Mục tiêu:** So sánh tốc độ và đặc tính sử dụng của một thuật toán mật mã dòng (ví dụ: ChaCha20) và một thuật toán mật mã khối ở chế độ CTR.
- **Yêu cầu cụ thể:**
  1. **Nghiên cứu:** Tìm hiểu về cấu trúc của ChaCha20 và so sánh với cấu trúc của AES-CTR.
  2. **Hiện thực:** Viết chương trình benchmark để đo thông lượng (throughput) mã hóa/giải mã của ChaCha20 và AES-128-CTR trên các file có kích thước khác nhau.
  3. **Sản phẩm:** Mã nguồn, báo cáo phân tích, đồ thị so sánh hiệu năng và nhận xét.

Đề tài 12. **Hiện thực hóa Thuật toán RSA và các Thành phần Toán học**

- **Mục tiêu:** Nắm vững toàn bộ quy trình của RSA bằng cách xây dựng thuật toán từ các hàm toán học cơ bản.
- **Yêu cầu cụ thể:**
  1. **Nghiên cứu:** Trình bày nền tảng toán học của RSA.
  2. **Hiện thực:** Sử dụng thư viện số lớn (Big Integer), tự viết các hàm kiểm tra số nguyên tố (Miller-Rabin), sinh cặp khóa RSA, mã hóa và giải mã.
  3. **Sản phẩm:** Mã nguồn, báo cáo chi tiết các bước toán học và demo chương trình.

Đề tài 13. **Phân tích cấu trúc và An ninh của SHA-512**

- **Mục tiêu:** Hiểu sâu về cách một hàm băm hiện đại hoạt động ở mức bit.
- **Yêu cầu cụ thể:**
  1. **Nghiên cứu:** Trình bày chi tiết cấu trúc Merkle–Damgård và hàm nén (compression function) của SHA-512.
  2. **Hiện thực:** Viết chương trình mô phỏng quá trình tính toán mã băm SHA-512 cho một thông điệp ngắn, hiển thị các giá trị trung gian.
  3. **Sản phẩm:** Mã nguồn mô phỏng và báo cáo phân tích thuật toán.

Đề tài 14. **Xây dựng hệ thống Chữ ký số và Xác thực Tài liệu**

- **Mục tiêu:** Tạo ra một ứng dụng thực tế để đảm bảo tính toàn vẹn và chống chối bỏ cho tài liệu.
- **Yêu cầu cụ thể:**
  1. **Nghiên cứu:** Trình bày về chuẩn Digital Signature Standard (DSS) và thuật toán DSA/ECDSA.
  2. **Hiện thực:** Xây dựng một cặp công cụ dòng lệnh:
     - sign.exe: Nhận đầu vào là một file và khóa bí mật (private key), tạo ra một file chữ ký.
     - verify.exe: Nhận đầu vào là file gốc, file chữ ký và khóa công khai (public key), sau đó xác thực.
  3. **Sản phẩm:** Mã nguồn, báo cáo, và demo ký/xác thực thành công và thất bại.

Đề tài 15. **Phân tích và Hiện thực HMAC**

- **Mục tiêu:** Hiểu rõ sự cần thiết của MAC và cách HMAC xây dựng một cơ chế MAC an toàn từ bất kỳ hàm băm nào.
- **Yêu cầu cụ thể:**
    1. **Nghiên cứu:** Trình bày lý do tại sao các cấu trúc MAC đơn giản như Hash(Key || Message) không an toàn và cách HMAC giải quyết vấn đề đó.
    2. **Hiện thực:** Tự viết lại hàm HMAC-SHA256 theo chuẩn RFC 2104.
    3. **Sản phẩm:** Mã nguồn, báo cáo phân tích, và so sánh kết quả với một thư viện chuẩn để kiểm tra.

Đề tài 16. **Xây dựng trình mô phỏng thuật toán DES (Data Encryption Standard)**

- **Mục tiêu:** Hiểu sâu về cấu trúc mạng Feistel, quá trình sinh khóa con (key scheduling), và vai trò của các thành phần S-boxes, P-boxes.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày chi tiết kiến trúc của DES, đặc biệt là cấu trúc Feistel và hàm F.
    2. Hiện thực: Xây dựng chương trình mô phỏng quá trình mã hóa/giải mã của DES qua 16 vòng. Cho phép người dùng nhập bản rõ và khóa, sau đó hiển thị kết quả sau mỗi vòng.
    3. Sản phẩm: Nộp mã nguồn, báo cáo chi tiết về thuật toán, và demo chương trình mô phỏng.

Đề tài 17. **Ứng dụng DES để mã hóa ảnh xám và phân tích kết quả**

- **Mục tiêu:** Thực hành áp dụng thuật toán DES vào dữ liệu ảnh và đánh giá tính bảo mật trên dữ liệu đa phương tiện.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày cơ chế sinh khóa trong DES.
    2. Hiện thực: Xây dựng chương trình mã hóa ảnh xám 256x256 bằng DES.
    3. Thực nghiệm: So sánh ảnh gốc và ảnh mã hóa, phân tích độ nhiễu.
    4. Sản phẩm: Nộp mã nguồn, báo cáo kết quả thực nghiệm, ảnh minh họa.

Đề tài 18. **Ứng dụng AES để bảo mật tập tin văn bản**

- **Mục tiêu:** Áp dụng thuật toán AES vào mã hóa dữ liệu văn bản, phân tích hiệu suất theo độ dài khóa.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày cấu trúc các vòng lặp của thuật toán AES.
    2. Hiện thực: Viết chương trình mã hóa/giải mã tập tin văn bản bằng AES.
    3. Thực nghiệm: So sánh kết quả mã hóa với các độ dài khóa 128/192/256 bit.
    4. Sản phẩm: Nộp mã nguồn, báo cáo kết quả phân tích hiệu suất.

Đề tài 19. **So sánh hiệu năng và độ an toàn của AES với các độ dài khóa khác nhau**

- **Mục tiêu:** Đánh giá sự ảnh hưởng của độ dài khóa tới hiệu suất và mức độ bảo mật của AES.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày sự khác biệt giữa các khóa 128, 192, 256 bit trong AES.
    2. Hiện thực: Cài đặt chương trình AES và đo thời gian mã hóa/giải mã.
    3. Thực nghiệm: Phân tích tốc độ và mức độ bảo mật tương ứng.
    4. Sản phẩm: Nộp mã nguồn, biểu đồ so sánh, báo cáo đánh giá.

Đề tài 20. **Ứng dụng AES để bảo mật cơ sở dữ liệu SQLite**

- **Mục tiêu:** Nghiên cứu tích hợp mã hóa AES vào cơ sở dữ liệu để bảo mật thông tin lưu trữ.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Mô tả cơ chế lưu trữ dữ liệu trong SQLite.
    2. Hiện thực: Viết chương trình AES để mã hóa dữ liệu trước khi lưu vào DB.
    3. Thực nghiệm: Thực hiện giải mã dữ liệu khi truy vấn từ DB.
    4. Sản phẩm: Nộp mã nguồn, báo cáo đánh giá ưu/nhược điểm.

Đề tài 21. **So sánh thuật toán DES và AES về cấu trúc và hiệu năng**

- **Mục tiêu:** Phân tích sâu sự khác biệt giữa DES và AES nhằm hiểu rõ lý do AES thay thế DES.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày chi tiết cấu trúc DES và AES.
    2. Hiện thực: Cài đặt cả hai thuật toán và đo thời gian mã hóa trên cùng dữ liệu.
    3. Thực nghiệm: So sánh kết quả bảo mật và tốc độ.
    4. Sản phẩm: Bảng so sánh, mã nguồn, báo cáo phân tích.

Đề tài 22. **Xây dựng ứng dụng mini chat có mã hóa AES thời gian thực**

- **Mục tiêu:** Thực hành áp dụng AES để bảo mật truyền thông thời gian thực.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày cơ chế mã hóa đối xứng trong truyền thông.
    2. Hiện thực: Xây dựng ứng dụng chat đơn giản sử dụng AES cho mỗi tin nhắn.
    3. Thực nghiệm: Đo độ trễ và tốc độ truyền khi bật/tắt mã hóa.
    4. Sản phẩm: Mã nguồn, demo ứng dụng, báo cáo kỹ thuật.

Đề tài 23. **Mô phỏng quá trình sinh khóa động trong AES (Key Expansion)**

- **Mục tiêu:** Hiểu rõ cơ chế sinh khóa động trong AES và trực quan hóa từng bước.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày thuật toán Key Expansion trong AES.
    2. Hiện thực: Viết chương trình mô phỏng quá trình sinh toàn bộ khóa vòng.
    3. Thực nghiệm: So sánh khóa sinh ra khi thay đổi khóa chính đầu vào.
    4. Sản phẩm: Mã nguồn, hình ảnh minh họa, báo cáo phân tích.

Đề tài 24. Ứng dụng RSA để mã hóa/giải mã thông điệp văn bản

- **Mục tiêu:** Nắm vững nguyên lý RSA và áp dụng vào truyền thông bảo mật.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày nguyên lý hoạt động của RSA.
    2. Hiện thực: Cài đặt chương trình tạo khóa RSA và mã hóa/giải mã thông điệp.
    3. Thực nghiệm: Kiểm thử với các độ dài khóa khác nhau.
    4. Sản phẩm: Nộp mã nguồn, báo cáo phân tích.

Đề tài 25. Ứng dụng RSA để ký số và xác thực chữ ký số cho tập tin

- **Mục tiêu:** Hiểu và áp dụng quy trình ký số sử dụng RSA.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày quy trình ký số và xác thực chữ ký số bằng RSA.
    2. Hiện thực: Viết chương trình tạo chữ ký số cho tập tin văn bản.
    3. Thực nghiệm: Viết chương trình kiểm tra chữ ký số vừa tạo.
    4. Sản phẩm: Mã nguồn, báo cáo đánh giá tính pháp lý, ứng dụng thực tế.

Đề tài 26. Mô phỏng quy trình sinh khóa RSA và ứng dụng trao đổi khóa phiên

- **Mục tiêu:** Nắm rõ quá trình sinh khóa và ứng dụng RSA trong trao đổi khóa phiên.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày chi tiết quá trình sinh khóa trong RSA.
    2. Hiện thực: Mô phỏng tạo và lưu trữ cặp khóa.
    3. Thực nghiệm: Sử dụng khóa để mã hóa khóa phiên.
    4. Sản phẩm: Nộp mã nguồn, báo cáo.

Đề tài 27. So sánh hiệu suất RSA và ECC (Elliptic Curve Cryptography)

- **Mục tiêu:** Phân tích điểm mạnh yếu của RSA và ECC về tốc độ, độ dài khóa và bảo mật.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày tổng quan RSA và ECC.
    2. Hiện thực: Cài đặt chương trình đo thời gian tạo khóa và mã hóa bằng RSA và ECC.
    3. Thực nghiệm: So sánh kích thước khóa và tốc độ xử lý.
    4. Sản phẩm: Mã nguồn, bảng so sánh, báo cáo phân tích.

Đề tài 28. Xây dựng hệ thống chia sẻ khóa công khai (Public Key Infrastructure - PKI) đơn giản

- **Mục tiêu:** Hiểu mô hình PKI và thực hành triển khai mô hình nhỏ sử dụng RSA.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày kiến trúc PKI, vai trò CA, RA.
    2. Hiện thực: Viết chương trình tạo, phát hành và thu hồi chứng chỉ RSA.
    3. Thực nghiệm: Tích hợp vào ứng dụng trao đổi khóa.
    4. Sản phẩm: Mã nguồn, báo cáo mô hình PKI.

Đề tài 29. Ứng dụng RSA để bảo mật kênh truyền TCP Socket

- **Mục tiêu:** Áp dụng RSA để thiết lập kênh truyền bảo mật giữa client-server.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày quá trình bắt tay khóa công khai.
    2. Hiện thực: Viết chương trình client-server sử dụng RSA để mã hóa dữ liệu truyền.
    3. Thực nghiệm: Đo tốc độ truyền khi bật/tắt mã hóa.
    4. Sản phẩm: Mã nguồn, demo truyền dữ liệu, báo cáo kết quả.

Đề tài 30. Mô phỏng tấn công phân tích thừa số trên RSA

- **Mục tiêu:** Nhận diện điểm yếu tiềm ẩn của RSA và minh họa cách tấn công phân tích thừa số.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày nguyên lý an toàn của RSA dựa trên bài toán phân tích thừa số.
    2. Hiện thực: Viết chương trình thử phân tích n (p×q) với khóa nhỏ.
    3. Thực nghiệm: So sánh thời gian bẻ khóa theo độ dài n.
    4. Sản phẩm: Mã nguồn, báo cáo kết quả thử nghiệm.

Đề tài 31. Ứng dụng kết hợp RSA và AES (Hybrid Encryption)

- **Mục tiêu:** Tìm hiểu và áp dụng mô hình kết hợp RSA-AES trong bảo mật.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày mô hình mã hóa lai (Hybrid Encryption).
    2. Hiện thực: Viết chương trình sử dụng RSA để trao đổi khóa AES, sau đó mã hóa dữ liệu bằng AES.
    3. Thực nghiệm: So sánh tốc độ và bảo mật với RSA/AES đơn lẻ.
    4. Sản phẩm: Mã nguồn, báo cáo phân tích.

Đề tài 32. Ứng dụng SHA-256 để kiểm tra tính toàn vẹn của file tải về

- **Mục tiêu:** Thực hành sử dụng hàm băm để phát hiện thay đổi dữ liệu.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày nguyên lý hoạt động của SHA-256.
    2. Hiện thực: Viết chương trình sinh mã băm SHA-256 cho tập tin.
    3. Thực nghiệm: So sánh mã băm với checksum do server cung cấp.
    4. Sản phẩm: Mã nguồn, báo cáo thử nghiệm.

Đề tài 33. So sánh khả năng chống va chạm của MD5, SHA-1 và SHA-256

- **Mục tiêu:** Phân tích khả năng chống va chạm của các hàm băm phổ biến.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày sự khác nhau giữa MD5, SHA-1, SHA-256.
    2. Hiện thực: Viết chương trình sinh mã băm cho cùng một tập tin bằng cả 3 hàm.
    3. Thực nghiệm: Thay đổi 1 byte và phân tích sự khác biệt của mã băm.

4. Sản phẩm: Mã nguồn, báo cáo phân tích.

Đề tài 34. **Xây dựng công cụ tạo và xác minh chữ ký số dùng SHA-256 + RSA**

- **Mục tiêu:** Hiểu và áp dụng kết hợp hàm băm với mã hóa bất đối xứng trong chữ ký số.
- **Yêu cầu cụ thể:**
  1. Nghiên cứu: Trình bày cơ chế kết hợp SHA-256 và RSA để ký số.
  2. Hiện thực: Viết chương trình ký số và xác minh chữ ký số.
  3. Thực nghiệm: Kiểm thử với các file khác nhau.
  4. Sản phẩm: Mã nguồn, báo cáo kết quả.

Đề tài 35. **Mô phỏng tấn công sinh va chạm trên MD5**

- **Mục tiêu:** Minh họa điểm yếu của MD5 thông qua thử nghiệm tạo va chạm.
- **Yêu cầu cụ thể:**
  1. Nghiên cứu: Trình bày lý thuyết va chạm và điểm yếu MD5.
  2. Hiện thực: Viết chương trình thử tìm 2 file có cùng mã băm MD5.
  3. Thực nghiệm: So sánh thời gian sinh va chạm với kích thước file khác nhau.
  4. Sản phẩm: Mã nguồn, báo cáo phân tích.

Đề tài 36. **Ứng dụng SHA-3 để kiểm tra tính toàn vẹn dữ liệu trong mạng**

- **Mục tiêu:** Thử nghiệm SHA-3 trong môi trường mạng để đánh giá tính toàn vẹn dữ liệu.
- **Yêu cầu cụ thể:**
  1. Nghiên cứu: Trình bày cấu trúc và ưu điểm của SHA-3.
  2. Hiện thực: Viết chương trình gửi/nhận dữ liệu có kèm mã băm SHA-3.
  3. Thực nghiệm: Mô phỏng lỗi đường truyền và kiểm tra khả năng phát hiện lỗi.
  4. Sản phẩm: Mã nguồn, báo cáo thử nghiệm.

Đề tài 37. **So sánh tốc độ và độ dài đầu ra của các hàm băm phổ biến**

- **Mục tiêu:** Đánh giá hiệu suất và đặc điểm đầu ra của các hàm băm.
- **Yêu cầu cụ thể:**
  1. Nghiên cứu: Tổng quan về MD5, SHA-1, SHA-256, SHA-3.
  2. Hiện thực: Viết chương trình đo thời gian băm và độ dài kết quả đầu ra.
  3. Thực nghiệm: Thử nghiệm với file kích thước tăng dần.
  4. Sản phẩm: Bảng kết quả, mã nguồn, báo cáo phân tích.

Đề tài 38. **Xây dựng hệ thống kiểm tra tính toàn vẹn file log máy chủ**

- **Mục tiêu:** Áp dụng hàm băm để bảo vệ log hệ thống khỏi chỉnh sửa trái phép.
- **Yêu cầu cụ thể:**
  1. Nghiên cứu: Trình bày cơ chế băm chuỗi log và phát hiện thay đổi.
  2. Hiện thực: Viết chương trình sinh mã băm cho log định kỳ và lưu trữ.
  3. Thực nghiệm: Giả lập chỉnh sửa log và phát hiện.
  4. Sản phẩm: Mã nguồn, báo cáo đánh giá.

Đề tài 39. Kết hợp HMAC và SHA-256 để xác thực thông điệp

- **Mục tiêu:** Hiểu cơ chế tạo mã xác thực thông điệp (MAC) bằng HMAC-SHA256.
- **Yêu cầu cụ thể:**
    1. Nghiên cứu: Trình bày cấu trúc và nguyên lý HMAC.
    2. Hiện thực: Viết chương trình tạo và kiểm tra HMAC-SHA256 cho thông điệp.
    3. Thực nghiệm: Thử chỉnh sửa thông điệp và kiểm tra khả năng phát hiện.
    4. Sản phẩm: Mã nguồn, báo cáo kết quả.