ĐỒ ÁN MÔN HỌC "LÝ THUYẾT MẬT MÃ"

Hình thức: Tiểu luận có thuyết trình trực tuyến

Hướng dẫn chung (yêu cầu với Colab)

- Mỗi nhóm tạo một notebook Google Colab chung (link public hoặc chia sẻ cho giảng viên).
- Ghi rõ hướng dẫn chạy trong cell đầu: môi trường, thư viện cần pip install.
- Tất cả file test (ví dụ ảnh BMP, csv, sample transactions) nộp kèm trong Google Drive hoặc upload vào Colab.
- Notebook phải có các phần: Mục tiêu, Yêu cầu, Cài đặt môi trường, Code, Kết quả thử nghiệm, Kết luận.

Mỗi nhóm chọn 1 trong các chủ đề:

1. Bảo mật giao dịch thương mại điện tử bằng AES

- **Mục tiêu**: Mã hóa dữ liệu đơn hàng và thông tin khách hàng.
- **Yêu cầu**: Thực hiện mã hóa AES-128 cho payload JSON của đơn hàng; minh họa mã hóa/giải mã trong Colab.
- **Thư viện**: pycryptodome.

2. Hệ thống thanh toán trực tuyến tích hợp RSA để bảo vệ thông tin thẻ

- **Mục tiêu**: Bảo mật số thẻ khi truyền từ client lên server.
- **Yêu cầu**: Triển khai sinh khóa RSA, mã hóa trường thẻ trước khi gửi (mô phỏng request) và giải mã ở server (Colab notebook mô phỏng client+server).
- **Thư viện**: pycryptodome.

3. Chữ ký số cho hợp đồng điện tử trong giao dịch B2B

- **Mục tiêu**: Xác thực tính toàn vẹn và nguồn gốc hợp đồng.
- **Yêu cầu**: Ký file PDF/TXT bằng RSA hoặc ECDSA; kiểm chứng chữ ký trong notebook.
- **Thư viện**: pycryptodome, ecdsa, PyPDF2 (nếu cần cho PDF).

4. Mô phỏng ví điện tử tích hợp ECC để bảo vệ khóa riêng

- **Mục tiêu**: Quản lý khóa và ký giao dịch bảo mật.
- **Yêu cầu**: Sinh cặp khóa ECC (secp256k1), tạo địa chỉ ví đơn giản và ký giao dịch mẫu.
- **Thư viện**: ecdsa, base58.

5. Tích hợp mã hóa lai (AES + RSA) trong nền tảng ví điện tử

- **Mục tiêu**: Bảo vệ dữ liệu giao dịch và lưu trữ khóa an toàn.
- **Yêu cầu**: Mã hóa payload bằng AES, mã hóa khóa AES bằng RSA; thực hiện luồng mã hóa/giải mã trong Colab.
- **Thư viện**: pycryptodome.

6. Ứng dụng OTP bảo vệ đăng nhập ngân hàng số (TOTP)

- **Mục tiêu**: Tăng cường bảo mật đăng nhập 2FA.
- **Yêu cầu**: Sinh secret, tạo QR để quét bằng Google Authenticator (hiển thị QR trong Colab), xác thực TOTP.
- **Thư viện**: pyotp, qrcode.

7. Hệ thống kiểm tra tính toàn vẹn báo cáo tài chính bằng SHA-256

- **Mục tiêu**: Bảo vệ báo cáo kế toán khỏi bị sửa đổi.
- **Yêu cầu**: Tạo hash file CSV/PDF, so sánh trước/sau; minh họa lưu trữ hash và xác thực.
- **Thư viện**: hashlib, pandas.

8. Mã hóa dữ liệu khách hàng trong CRM bằng AES-GCM

- **Mục tiêu**: Bảo đảm tính bảo mật và tính toàn vẹn dữ liệu khách hàng.
- **Yêu cầu**: Sử dụng AES-GCM để mã hóa các trường nhạy cảm trong dataset khách hàng (CSV) và minh họa giải mã an toàn.
- **Thư viện**: pycryptodome, pandas.

9. Triển khai API mã hóa cho dịch vụ ví điện tử (mô phỏng) bằng Flask trên Colab

- **Mục tiêu**: Cung cấp endpoint mã hóa/giải mã để tích hợp vào hệ thống tài chính.

- **Yêu cầu**: Dùng flask (mô phỏng server trong Colab bằng ngrok hoặc flask notebook run) cho các endpoint AES/RSA/hash; ghi rõ API spec.
- **Thư viện**: flask, pyngrok, pycryptodome.

10. Xây dựng mô phỏng kết nối an toàn SSL/TLS cho giao dịch chứng khoán

- **Mục tiêu**: Hiểu vai trò TLS trong bảo vệ kênh giao dịch.
- **Yêu cầu**: Mô phỏng client-server với HTTPS (Flask + tạo self-signed cert), kiểm tra mã hóa kênh khi truyền dữ liệu giao dịch.
- **Thư viện**: flask, ssl.

11. Blockchain cho quản lý hóa đơn điện tử (mô phỏng)

- **Mục tiêu**: Lưu trữ hóa đơn không thể chỉnh sửa.
- **Yêu cầu**: Tạo chuỗi khối đơn giản; dùng hash cho khối, chữ ký số cho issuer; minh họa truy vấn bằng Colab.
- **Thư viện**: hashlib, ecdsa, json.

12. Mã hóa dữ liệu trong mô hình phân tích hành vi khách hàng (privacy-preserving)

- **Mục tiêu**: Bảo vệ dữ liệu nhạy cảm khi phân tích kinh doanh.
- **Yêu cầu**: Mã hóa trường PII trước khi phân tích; so sánh kết quả phân tích trên dữ liệu gốc và dữ liệu mã hóa/giải mã.
- **Thư viện**: pycryptodome, pandas, scikit-learn (tùy chọn cho phân tích).

13. Xác thực giao dịch ví điện tử bằng chữ ký số ECDSA

- **Mục tiêu**: Ngăn chặn giao dịch giả mạo trong hệ thanh toán điện tử.
- **Yêu cầu**: Ký giao dịch bằng ECDSA; xây dựng flow xác thực trước khi chấp nhận giao dịch.
- **Thư viện**: ecdsa, json.

14. Hệ thống báo cáo kiểm toán bảo mật với blockchain

- **Mục tiêu**: Đảm bảo tính toàn vẹn và truy xuất nguồn gốc bản ghi kiểm toán.
- **Yêu cầu**: Lưu log kiểm toán vào block; cung cấp hàm verify cho auditor.
- **Thư viện**: hashlib, json.

15. Nền tảng gọi vốn cộng đồng (Crowdfunding) với bảo mật giao dịch

- **Mục tiêu**: Ứng dụng mã hóa trong mô hình kinh doanh gọi vốn.
- **Yêu cầu**: Mã hóa thông tin người ủng hộ, ký giao dịch đóng góp, mô phỏng luồng tiền (off-chain) trong Colab.
- **Thư viện**: pycryptodome, ecdsa, pandas.

Deliverables yêu cầu (áp dụng cho tất cả đề tài)

- Google Colab notebook hoàn chỉnh (code, hướng dẫn chạy, kết quả).
- File data mẫu (CSV, ảnh, transactions) kèm theo hoặc link Drive.
- Báo cáo ngắn (10–20 trang): Mục tiêu, thiết kế, test, kết luận.
- Video demo 5 phút (khuyến nghị).

Tiêu chí đánh giá chung

- Hoàn thành chức năng cơ bản (50%).
- Độ an toàn & lý giải bảo mật (20%).
- Chất lượng notebook & reproducibility (15%).
- Báo cáo và presentation (15%).