AN NINH MÁY TÍNH

ĐỒ ÁN 1

QUI ĐỊNH

- Đồ án nhóm 3 sinh viên.
- Nhóm sinh viên thực hiện đồ án theo yêu cầu bên dưới, phân công đều để tất cả các thành viên trong nhóm đều tham gia thực hiện đồ án.
- Ngôn ngữ lập trình: tuỳ chọn (khuyến khích sử dụng Java, Python, C#). Giao diện chương trình: Console hoặc GUI, sao cho tiện dụng.
- Viết báo cáo trình bày rõ các nội dung sau:
    - Thông tin các thành viên trong nhóm (họ tên, mssv, email), phân công thực hiện
    - Ghi rõ các chức năng đã thực hiện kèm giao diện tương ứng
    - Giải thích ngắn gọn, súc tích các vấn đề, giải pháp đã tìm hiểu và thực hiện theo các chức năng mà đề bài yêu cầu.
- 1 sinh viên đại diện nhóm nộp file MSSV1_MSSV2_MSSV3.zip/rar là bài nộp của nhóm lên link nộp bài ở website môn học.
- Vấn đáp khi kết thúc đồ án.

YÊU CẦU

Xây dựng ứng dụng gồm các chức năng chính sau:

1. **Đăng ký tài khoản người dùng**

1.1 Ứng dụng cho phép người dùng đăng ký 1 tài khoản với các thông tin: email (dùng làm định danh tài khoản), họ tên, ngày sinh, điện thoại, địa chỉ, mật khẩu (passphase).

1.2 Mật khẩu cần được lưu trữ dưới dạng Hash có kết hợp với Salt. Thuật toán Hash là SHA-256.

1.3 Ứng dụng có thể sử dụng CSDL SQL hoặc file XML, JSON để lưu trữ thông tin về người dùng.

1.4 Người dùng phải đăng nhập ứng dụng bằng email và passphase trước khi sử dụng các tính sau tiếp theo sau đây.

2. **Phát sinh cặp khoá bất đối xứng**

2.1 Ứng dụng cho phép phát sinh một cặp khoá (Kpublic, Kprivate) có độ dài là 2048 bit cho thuật toán RSA tương ứng với mỗi người dùng.

2.2 Khoá riêng Kprivate cần được mã hoá bằng thuật toán AES. Passphase của người dùng được sử dụng để phát sinh khoá bí mật Ksecret trong thuật toán AES. Khoá riêng Kprivate sau khi được mã hoá và khoá công cộng Kpublic được lưu trữ tương ứng với thông tin người dùng.

2.3 Cặp khoá này chỉ cần phát sinh 1 lần.

3. Cập nhật thông tin tài khoản

3.1 Ứng dụng cho phép cập nhật thông tin tài khoản (họ tên, ngày sinh, điện thoại, địa chỉ, passphase).

3.2 Trường hợp đổi passphase cần đảm bảo cặp khoá Kprivate, Kpublic không bị thay đổi. Tức là khoá Kprivate được mã hoá ở bước 2.2 với passphase cũ, cần được mã hoá lại với passphase mới.

4. Mã hoá tập tin (người gửi mã khoá tập tin và gửi cho người nhận)

4.1 Ứng dụng cho phép người dùng chọn tập tin cần mã hoá và chọn người nhận (giả sử người nhận là 1 người dùng khác của ứng dụng).

4.2 Ứng dụng tự phát sinh một khoá bí mật Ksession (khoá phiên) cho thuật toán AES để mã hoá toàn bộ tập tin.

4.3 Ứng dụng sử dụng public key (Kpublic) của người nhận để mã hoá khoá Ksession bằng thuật toán RSA. Khoá Ksession sau khi được mã hoá thì sẽ được bổ sung vào tập tin đã mã hoá (sinh viên tự đề nghị cấu trúc tập tin này).

5. Giải mã tập tin (người nhận nhận tập tin và giải mã)

5.1 Ứng dụng cho phép người dùng chọn tập tin cần giải mã.

5.2 Ứng dụng dùng passphase của người dùng (đã đăng nhập thành công) để giải mã thông tin private key (Kprivate) của mình đã được mã hoá bằng thuật toán AES ở bước 2.2.

5.3 Ứng dụng dùng private key (Kprivate) của mình để giải mã nội dung trong tập tin để có được khoá Ksession (giải mã cho bước 4.3).

5.4 Ứng dụng dùng khoá Ksession để giải mã tập tin (giải mã cho bước 4.2)

6. Ký trên tập tin

6.1 Ứng dụng cho phép chọn tập tin cần ký

6.2 Hash nội dung tập tin cần ký (dùng thuật toán SHA-256)

6.3 Ký trên nội dung Hash sử dụng private key (Kprivate) của người dùng

6.4 Chữ ký lưu riêng thành 1 file .sig (ví dụ: chữ ký đi kèm với file sample.doc là file sample.doc.sig)

7. Xác nhận chữ ký trên tập tin

7.1 Ứng dụng cho phép chọn 2 tập tin, gồm 1 tập tin cần xác nhận chữ ký, 1 tập tin chữ ký (ví dụ: sample.doc và sample.doc.sig ở bước 6.4)

7.2 Ứng dụng sử dụng danh sách các public key (Kpublic) của tất cả các người dùng để kiểm tra chữ ký điện tử tương ứng. Nếu kiểm tra thành công với một public key có trong danh sách trên thì thông báo chữ ký hợp lệ và do ai đã ký. Ngược lại, thông báo lỗi không xác nhận được chữ ký.