KHOA CÔNG NGHỆ THÔNG TIN
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
227 Nguyễn Văn Cừ, Phường 4, Quận 5, TP.HCM
Điện Thoại: (08) 38.354.266 - Fax:(08) 38.350.096

Đồ án thực hành (lập trình) cuối kỳ

☐ Bài tập cá nhân ☑ Bài tập nhóm (nhóm tối đa 02 sinh viên)

☐ Bài tập tự luyện tập ☑ Bài tập cần nộp (Đồ án cuối kỳ)

Quy định về việc nộp bài:

- **Thời hạn nộp bài**: theo thông báo của Giảng viên
- **Cách nộp**: nộp bài trên Website môn học vào mục **Đồ án thực hành cuối kỳ.**
- **Nội dung đồ án cuối kỳ gồm:**
  - Thư mục **Document**: chứa tập tin báo cáo về chương trình mà nhóm đã xây dựng.
    - **Trong file báo cáo cần ghi rõ thông tin của nhóm, bao gồm: họ tên, mã số sinh viên, điện thoại, email liên hệ**
    - Cần ghi rõ tất cả chức năng đã làm (kèm giao diện tương ứng)
    - Trình bày những vấn đề, giải pháp (về lý thuyết hay kỹ thuật) mà nhóm đã tìm hiểu và xây dựng trong đề tài.
    - **Nhóm sinh viên cần điền đầy đủ thông tin vào bảng tổng hợp chức năng của đề tài (theo mẫu ở trang 6, 7, 8)**
  - Thư mục **Source**: chứa đầy đủ các tập tin mã nguồn chương trình (cùng với các tập tin dữ liệu, hình ảnh, tài nguyên, thư viện liên kết động cần dùng...). Cần đảm bảo GV có thể build lại thành công toàn bộ ứng dụng từ mã nguồn của đồ án.
  - Thư mục **Release**: chứa đầy đủ các tập tin cần thiết để thực thi chương trình (kèm dữ liệu, hình ảnh, tài nguyên, thư viện liên kết động...)
  - Thư mục **Misc**: chứa các tập tin khác cần dùng (nếu có).
- **Quy tắc đặt tên khi nộp bài:**
  - Mỗi nhóm sinh viên có thể nộp tối đa **20 file**, mỗi file có **kích thước tối đa 12MB**. Nếu sinh viên chia file nén (ZIP/RAR) thành nhiều file nhỏ, cần kiểm tra kỹ nộp đầy đủ tất cả các file này.
  - Tên file được đặt là MSSV1-MSSV2.* nếu làm theo nhóm (với quy ước MSSV1 < MSSV2) hoặc MSSV.* nếu làm cá nhân.
- **Lưu ý:**
  - Sinh viên nên chủ động đề xuất các ý tưởng, giải pháp cho bài làm của nhóm mình.
  - Những bài giống nhau hoặc giống bài làm của khóa trước, tùy theo mức độ vi phạm, sẽ bị 0 điểm hoặc bị trừ điểm.

1. Nội dung đồ án (Phần cơ bản) :

Ứng dụng gồm các chức năng chính sau:

- **Đăng ký tài khoản và phát sinh cặp khóa (bất đối xứng):**
  - **Bước 1 – Nhập thông tin về người sở hữu cặp khóa**: Mỗi tài khoản tương ứng với ***1 địa chỉ email riêng*** (địa chỉ email là định danh của tài khoản). Mỗi tài khoản kèm theo các thông tin cá nhân của người sử dụng, bao gồm: họ tên, ngày sinh, điện thoại, địa chỉ.
  - **Bước 2 - Phát sinh cặp khóa**: Sử dụng thuật toán RSA với kích thước khóa do NSD quyết định (từ 512 bit đến 1024 bit, độ dài khóa là bội số của 64). NSD phải nhập passphrase dùng để kiểm tra khi giải mã private key
    - Passphrase phải được lưu trữ dạng Hash có **kết hợp với salt**. Gợi ý: thay vì lưu trữ trực tiếp passphrase, cần lưu trữ giá trị hash (Passphrase kết hợp với salt) và giá trị salt.
    - Thuật toán hash và thuật toán dùng để mã hóa nội dung private key do chương trình **tự quy định**, người sử dụng không cần chọn.
    - ***Vấn đề mở***: Nhóm sinh viên tự quyết định nên sử dụng passphrase để mã hóa private key hay chỉ dùng passphrase để kiểm tra xem NSD có phải là người chủ của cặp khóa hay không. Nếu được, nên có giải thích lý do phương án mình chọn trong báo cáo.
  - **Bước 3 – Lưu trữ:** Thông tin tài khoản của người sử dụng và cặp khóa được lưu trữ trong file (cấu trúc tự định nghĩa, hoặc XML), hoặc CSDL Access.
- **Cập nhật thông tin tài khoản và passphrase:**
  - Cho phép NSD cập nhật thông tin tài khoản và cập nhật passphrase nếu NSD nhập chính xác passphrase hiện tại.
    - NSD có thể cập nhật thông tin cá nhân (họ tên, ngày sinh, điện thoại, địa chỉ, passphrase)
    - Những thông tin mới được lưu trữ lại.
- **Export và Import thông tin về cặp khóa:**
  - Cho phép export thông tin về cặp khóa ra file (có cấu trúc tự định nghĩa, hoặc XML). Thông tin cần export gồm: public key, private key, họ tên, ngày sinh, điện thoại, địa chỉ của người chủ cặp khóa, hash (passphrase kết hợp salt), salt.
  - Cho phép import thông tin về cặp khóa từ file.

- **Mã hóa và giải mã tập tin:**
  - **Mã hóa tập tin**: Cho phép NSD chọn tập tin cần mã hóa, thuật toán mã hóa đối xứng và người nhận.
    - Hệ thống **tự phát sinh** ra 1 khóa bí mật (secret key K_s) có độ dài phù hợp với thuật toán mã hóa được chọn
    - Hệ thống **mã hóa** toàn bộ nội dung tập tin bằng phương pháp mã hóa đối xứng được chọn sử dụng khóa bí mật K_s
    - Hệ thống sử dụng public key của người nhận để mã hóa khóa K_s
    - Khóa K_s sau khi được mã hóa được bổ sung vào trong tập tin đã mã hóa (sinh viên tự quyết định sẽ đưa thông tin này vào vị trí nào trong tập tin đã mã hóa).
  - **Giải mã tập tin**: Cho phép NSD chọn tập tin cần giải mã, sử dụng private key của chính mình để giải mã. Trước khi sử dụng private key, NSD phải nhập chính xác passphrase.
    - Hệ thống yêu cầu NSD nhập passphrase trước khi giải mã private key.
    - Sử dụng private key này, hệ thống giải mã khóa bí mật K_s trong tập tin đã mã hóa
    - Sử dụng khóa bí mật K_s, hệ thống giải mã tập tin đã mã hóa
  - ***Một số vấn đề mở*** : Nhóm sinh viên tự quyết định giải pháp cho các vấn đề sau:
    - Chọn padding scheme và mode of operation: Chương trình cho phép NSD chọn padding scheme và mode of operation, hay quy định sẵn (cố định) 1 padding scheme và 1 mode of operation? Nếu cho phép NSD chọn thì làm cách nào để khi giải mã, hệ thống tự động xác định được tập tin đã được mã hóa với padding scheme và mode of operation nào?
    - Khóa bí mật (K_s) sau khi được mã hóa bằng public key của người nhận, nên được đưa vào phần nào trong tập tin dữ liệu mã hóa? Làm sao để hệ thống tự động lấy ra được thông tin này khi giải mã?
- **Ký và xác nhận chữ ký cho tập tin**
  - **Ký trên tập tin**: Cho phép NSD chọn tập tin cần ký, sử dụng private key của chính mình để tạo chữ ký.
    - Sử dụng thuật toán hash trước khi ký (nhóm sinh viên tự chọn cố định 1 thuật toán hash phù hợp)
    - Trước khi sử dụng private key, NSD phải nhập chính xác passphrase
    - Chữ ký được lưu trữ riêng trong 1 file .sig (ví dụ: chữ ký đi kèm với file **ABC.doc** được lưu trữ trong file **ABC.doc.sig**)
  - **Xác nhận chữ ký trên tập tin**:
    - Cho phép NSD chọn 2 tập tin, bao gồm tập tin cần xác nhận chữ ký (ví dụ **ABC.doc**) và tập tin chứa chữ ký (ví dụ: **ABC.doc.sig**)
    - Hệ thống duyệt lần lượt qua tất cả public key có trong danh sách lưu trữ sẵn và tiến hành kiểm tra chữ ký điện tử tương ứng. Nếu kiểm tra thành công chữ ký với một public key có sẵn thì thông báo chữ ký hợp lệ và do ai đã ký. Ngược lại, thông báo việc xác nhận chữ ký thất bại.

2. Nội dung đồ án (Phần nâng cao) :

Các tính năng dưới đây chỉ là các gợi ý. Sinh viên được khuyến khích bổ sung các tính năng nâng cao theo sở trường của mình.

- Xây dựng giao diện quản lý hệ thống tập tin, thư mục (có các tính năng copy, delete, rename … đối với tập tin và thư mục). Gợi ý: giao diện tương tự Window Explorer hoặc WinZIP/WinRAR.
- Bổ sung tính năng plug-in chức năng (mã hoá và giải mã) + (ký và xác nhận chữ ký) trên nội dung. thông tin vào môi trường MS Word 2003 và MS Outlook 2003 (khuyến khích plug-in vào Office 2007).
- Cho phép NSD chọn có nén tập tin trước khi mã hóa hay không. Cho phép giải nén tập tin khi giải mã (chương trình tự xác định có cần giải nén tập tin hay không khi giải mã). Được phép sử dụng các thư viện nén có sẵn (cần ghi rõ trong báo cáo)
- Cho phép chọn nhiều tập tin hay thư mục để mã hóa thành duy nhất 1 tập tin mã hóa. Cho phép giải mã các tập tin và thư mục này từ tập tin mã hóa. Có thể tích hợp thêm tính năng nén và giải nén.
- …

BẢNG TỔNG HỢP CHỨC NĂNG ĐÃ THỰC HIỆN

STT	Chức năng	Thực hiện	Ghi chú
1. Đăng ký tài khoản và phát sinh cặp khóa (bất đối xứng):			
1.1	Nhập đầy đủ thông tin về người sở hữu khóa	☐	
1.2	Cho NSD chọn độ dài cặp khóa (từ 512 đến 1024 bit)	☐	
1.3	Phát sinh cặp khóa với độ dài được chọn	☐	
1.4	Passphrase được lưu dưới dạng Hash (Passphrase kết hợp với Salt) và Salt	☐	
1.5	Lưu trữ thông tin về người sở hữu và thông tin cặp khóa vào file hay CSDL	☐	
1.6	Mã hóa nội dung private key	☐	
2. Cập nhật thông tin tài khoản và passphrase			
2.1	Có kiểm tra passphrase trước khi cập nhật hay không?	☐	
2.2	Cho phép cập nhật thông tin cá nhân	☐	
2.3	Cho phép phát sinh passphrase	☐	
2.4	Lưu lại thông tin cập nhật	☐	
3. Export và Import thông tin về cặp khóa			
3.1	Export cặp khóa và thông tin liên quan	☐	
3.2	Import cặp khóa và thông tin liên quan	☐	
4. Mã hóa tập tin			
4.1	Cho NSD chọn tập tin cần mã hóa	☐	
4.2	Cho NSD chọn thuật toán mã hóa đối xứng	☐	
4.3	Cho NSD chọn người nhận	☐	
4.4	Hệ thống phát sinh khóa bí mật (K_s)	☐	
4.5	Mã hóa nội dung tập tin (mã hóa đối xứng)	☐	
4.6	Mã hóa khóa bí mật K_s bằng public key của người nhận	☐	
4.7	Đưa thông tin khóa bí mật đã được mã hóa vào tập tin	☐	

STT	Chức năng	Thực hiện	Ghi chú
4.8	*Cho NSD chọn padding mode*	☐	Không bắt buộc
4.9	*Cho NSD chọn mode of operation*	☐	Không bắt buộc
4.10	*Nén tập tin trước khi mã hóa*	☐	Không bắt buộc
4.11	*Cho phép chọn nhiều tập tin để xử lý cùng lúc*	☐	Không bắt buộc
5. Giải mã tập tin			
5.1	Kiểm tra passphrase trước khi giải mã tập tin	☐	
5.2	Giải mã khóa bí mật K_s bằng private key của người nhận	☐	
5.3	Giải mã nội dung tập tin	☐	
5.4	*Giải nén tập tin (nếu đã nén khi mã hóa)*	☐	Không bắt buộc
6. Ký trên tập tin			
6.1	Kiểm tra passphrase trước khi ký	☐	
6.2	Hash tập tin cần ký	☐	
6.3	Tạo tập tin chữ ký	☐	
7. Xác nhận chữ ký cho tập tin			
7.1	Hệ thống tự động duyệt qua từng public key có trong dữ liệu	☐	Sinh viên có thể làm ở mức độ đơn giản hơn là cho NSD chọn muốn kiểm tra bằng public key của ai.
7.2	Kiểm tra chữ ký hợp lệ	☐	

8. Các chức năng khác

Nhóm sinh viên có thể bổ sung các chức năng đặc biệt khác chưa được liệt kê trong phần dưới đây

	Giao diện quản lý hệ thống tập tin, thư mục	☐	
	Plug-in vào Microsoft Word	☐	
	Plug-in vào Microsoft Outlook	☐	
	Tự cài đặt thêm thuật toán mã hóa mới	☐	
	Sử dụng thêm thư viện các thuật toán mã hóa mới	☐	
	Xử lý digital certificate	☐	
	Có demo	☐	
	Hướng dẫn sử dụng	☐	
	…	☐	