AN NINH MÁY TÍNH

ĐỒ ÁN 1

QUI ĐỊNH

- Đồ án nhóm 2 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.zip/rar là bài nộp của nhóm lên link nộp bài ở website môn học.

YÊU CẦU

A. Xây dựng một module gồm các chức năng chính sau:

1. Cho phép phát sinh một khoá bí mật Ks của thuật toán AES
2. Mã hoá tập tin sử dụng thuật toán AES với khoá Ks
3. Giải mã tập tin sử dụng thuật toán AES với khoá Ks
4. Phát sinh một cặp khoá Kprivate và Kpublic của thuật toán RSA
5. Mã hoá một chuỗi sử dụng thuật toán RSA sử dụng khoá Kpublic
6. Giải mã một chuỗi sử dụng thuật toán RSA sử dụng khoá Kprivate
7. Tính giá trị hash của một chuỗi sử dụng thuật toán SHA-1, SHA-256

B. Xây dựng một ứng dụng để sử dụng các chức năng của module ở mục A, gồm các chức năng chính sau:

1. Cho phép người dùng mã hoá một tập tin theo các bước:
    a. Người dùng chọn tập tin cần mã hoá (tập tin P)

b. Hệ thống phát sinh khoá bí mật Ks và mã hoá tập tin P thành tập tin C bằng thuật toán AES
c. Hệ thống phát sinh cặp khoá Kprivate và Kpublic của thuật toán RSA và mã hoá khoá Ks bằng khoá Kpublic, output là chuỗi Kx.
d. Hệ thống lưu lại chuỗi Kx kèm theo giá trị hash SHA-1 của Kprivate (gọi là HKprivate). Có thể xuất thành file C.metadata, với C là tên của tập tin C ở trên, cấu trúc tập tin là tuỳ chọn (XML, JSON, Plain text…).
e. Hệ thống kết xuất khoá Kprivate cho người dùng (có thể xuất ra file).

2. Cho phép người dùng giải mã một tập tin theo các bước:
   a. Người dùng chọn tập tin cần giải mã (tập tin C)
   b. Người dùng nhập khoá Kprivate (có thể chọn từ file)
   c. Hệ thống kiểm tra giá trị hash SHA-1 của Kprivate có trùng với HKprivate không? Nếu không trùng thì giải mã thất bại, nếu trùng thì tiếp tục các bước sau:
   d. Giải mã chuỗi Kx để có được Ks dùng Kprivate.
   e. Dùng Ks giải mã tập tin C thành tập tin P.