Bài tập tuần

December 4, 2021

I Lý thuyết

Tìm hiểu, phân tích và cài đặt thuật toán kiểm tra số nguyên tố Miller-Rabin.

II Thực hành

Viết chương trình thực hiện ba nhiệm vụ sau:

1. Sinh cặp khóa ElGamal (gồm 1 khóa công khai, 1 khóa bí mật tương ứng) và yêu cầu người dùng nhập tên thư mục muốn lưu trữ khóa. Sau đó lưu khóa công khai vào file `el_pub.txt` và lưu khóa bí mật vào file `el.txt` tại thư mục đó.

2. Mã hóa đoạn văn bản: Người dùng nhập vào tên file có định dạng `.txt`, sau đó yêu cầu người dùng nhập tên file **khóa công khai**, tiến hành mã hóa nội dung file `.txt` của người dùng bằng khóa vừa nhận được. Nội dung mã hóa lưu vào file `encrypted.txt` ngay tại thư mục chứa file của người dùng.

3. Giải mã đoạn văn bản: Người dùng nhập vào tên file có định dạng `.txt`, sau đó yêu cầu người dùng nhập tên file **khóa bí mật**, tiến hành giải mã nội dung file `.txt` của người dùng bằng khóa vừa nhận được. Nội dung giải mã lưu vào file `decrypted.txt` ngay tại thư mục chứa file của người dùng.

III Các quy định nộp bài

III.1 Các quy định chung

1. Bài tập làm nhóm 2 người.

2. Phần nộp bài sẽ gồm có 2 phần là mã nguồn (lưu trong thư mục Source) và báo cáo (lưu trong thư mục Report), được nén thành 1 file bằng định dạng ZIP có tên dạng như sau: MSSV1_MSSV2.zip

III.2 Mã nguồn

1. Mã nguồn không thể biên dịch (báo lỗi biên dịch như sai cú pháp) hoặc không thể chạy được (báo các lỗi như lỗi runtime, sai logic chương trình): 0 điểm.

2. Các hành vi gian lận liên quan đến mã nguồn (sao chép mã nguồn giữa các nhóm, sao chép mã nguồn trên Internet, ...): 0 điểm.

III.3 Báo cáo

Phần báo cáo cần đảm bảo tối thiểu có các phần sau:

1. Trình bày cách biên dịch và chạy mã nguồn. Giải thích cụ thể thuật toán và trình bày mã giả thuật toán. Trường hợp mã giả không khớp với mã nguồn: 0 điểm.