Assignment – Practice of Information Security – Đề 2

Ngôn ngữ lập trình sử dụng trong bài tập lớn: **Python**

1. Sinh viên xây dựng công cụ minh họa mã hóa và giải mã tài liệu bằng các phương pháp sau;
   - AES (Advanced Encryption Standard)
   - DES (Data Encryption Standard)
   - Triple DES
   - RSA

   Yêu cầu: thuật toán phải được viết chi tiết và không được dùng thư viện bên thứ ba. Chọn file (file nguồn chứa plain text và file đích chứa cipher text). Gợi ý như *hình 1*

Hình 1

   a. Danh sách lựa chọn các giải thuật mã hoá. Gợi ý như hình 2

Hình 2

   b. Các Button xác nhận hành động mã hoá và giải mã. Gợi ý theo hình 3

Hình 3

    c. Riêng với mã hoá bất đối xứng RSA, sinh viên có thể tự thiết kế các màn hình con để lấy thêm các thông tin từ người dùng.
2. Sử dụng thư việnPython-RSA, sinh viên viết chương trình (Console hoặc Winform) để triển khai mã hóa RSA theo các yêu cầu sau:
    a. Hàm tạo cặp khóa công khai – bí mật cho Alice và cặp khóa công khai – bí mật cho Bob.
    b. Xây dựng chức năng mã hóa văn bản gốc (plain text) mà Alice muốn chỉ có Bob mới đọc được
    c. Xây dựng chức năng xác nhận bản quyền cho văn bản gốc (plain text) cho Alice. Bất cứ ai cũng có thể xác nhận văn bản đó là của duy nhất Alice
3. Sinh viên mô tả và giải thích rõ ràng, từng bước (kèm ví dụ minh hoạ) về giao thức xác thực OAuth2.
4. Sinh viên lập trình minh hoạ từng bước trong giao thức xác thực OAuth2.