**BÁO CÁO ĐỒ ÁN NHÓM**

Sinh viên viết báo cáo đồ án nhóm mô tả chi tiết nội dung công việc nhóm đã thực hiện được

**-----**

**BẢNG PHÂN CÔNG CÔNG VIỆC**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Các thành viên trong nhóm** | **Công việc được giao** | **Tỷ lệ hoàn thành** |
| 1. | Lê Ngọc Kiều Anh | Lập trình PlayFair, design GUI | 100% |
| 2. | Phùng Việt Bắc | Điều chỉnh source code, lập trình thêm tính năng cho cả 2 giải thuật | 100% |
| 3. | Trần Phước Đại | Lập trình RSA, design GUI | 100% |

**I. NỘI DUNG 1: VIẾT ỨNG DỤNG**

**Các nội dung ghi vào báo cáo:**

1. **Tên ứng dụng**

* Giải thuật PlayFair-RSA.

1. **Ngôn ngữ sử dụng:**

* Sử dụng ngôn ngữ C#
* Mã nguồn là do nhóm tự code và sử dụng các thư viện do Winform cung cấp như:
  + **using System.Text;**
  + **using System.Numerics;**
  + **using System.Data;**
  + **…**
* Ứng với giải thuật PlayFair mã nguồn sử dụng chủ yếu phân tích triển khai ma trận khóa và phiên dịch từ ma trận để mã hóa / giải mã nội dung (Input).
* Về giải thuật RSA, mã nguồn được tích hợp các thuật toán như Euclidean và Miller Rabin để kiểm tra số nguyên tố và thực hiện chức năng sinh giá trị.

1. **Giao diện chính**
2. Giao diện Menu lựa chọn:

* Menu chính là trang chủ gồm tên các giải thuật : PlayFair, RSA.
* Tên các giải thuật được đặt trên các button ẩn để người dùng có thể truy cập vào và chuyển tiếp tới trang chủ chính của các giải thuật.
* Chủ đề trang trí được sử dụng là “Mùa Xuân Nho Nhỏ”.

Ảnh có chứa hoa, văn bản, màu hồng, màu tím

Mô tả được tạo tự động

*Giao diện Menu*

1. Giao diện chính của ứng dụng PlayFair:

* Giao diện của kỹ thuật mã hóa / giải mã với Giải thuật PlayFair bao gồm các thành phần:
* 1 Textbox Text dùng để nhập dữ liệu người dùng cần mã hóa/ giải mã (Input).
* 1 Textbox PlayFair Key dùng để nhập khóa mà người dùng muốn.
* 1 Textbox Result dùng để hiển thị kết quả sau khi chạy chương trình.
* Đồng thời sử dụng các button để thực hiện các chức năng chính như:
  + - Encrypt
    - Decrypt
    - Import
    - Export
    - Clear

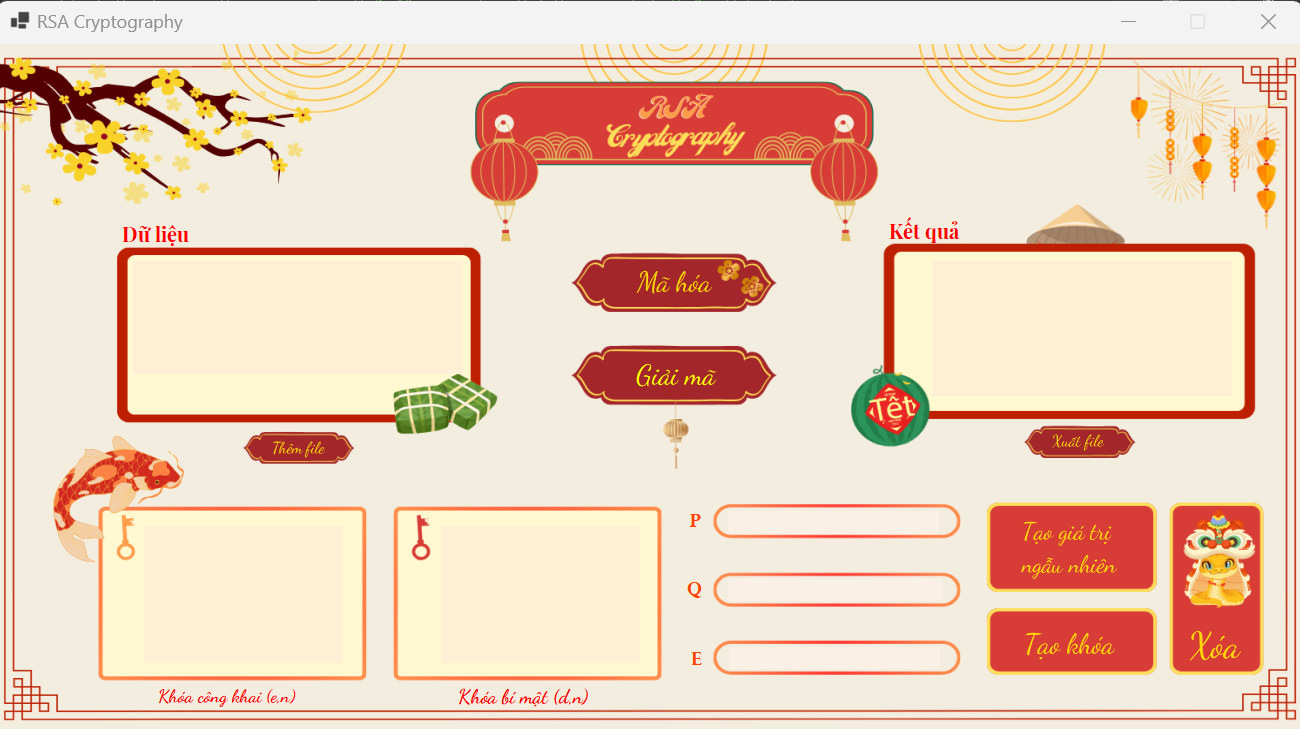
Ảnh có chứa văn bản, ảnh chụp màn hình, hoa, màu hồng

Mô tả được tạo tự động

*Giao diện ứng dụng PlayFair*

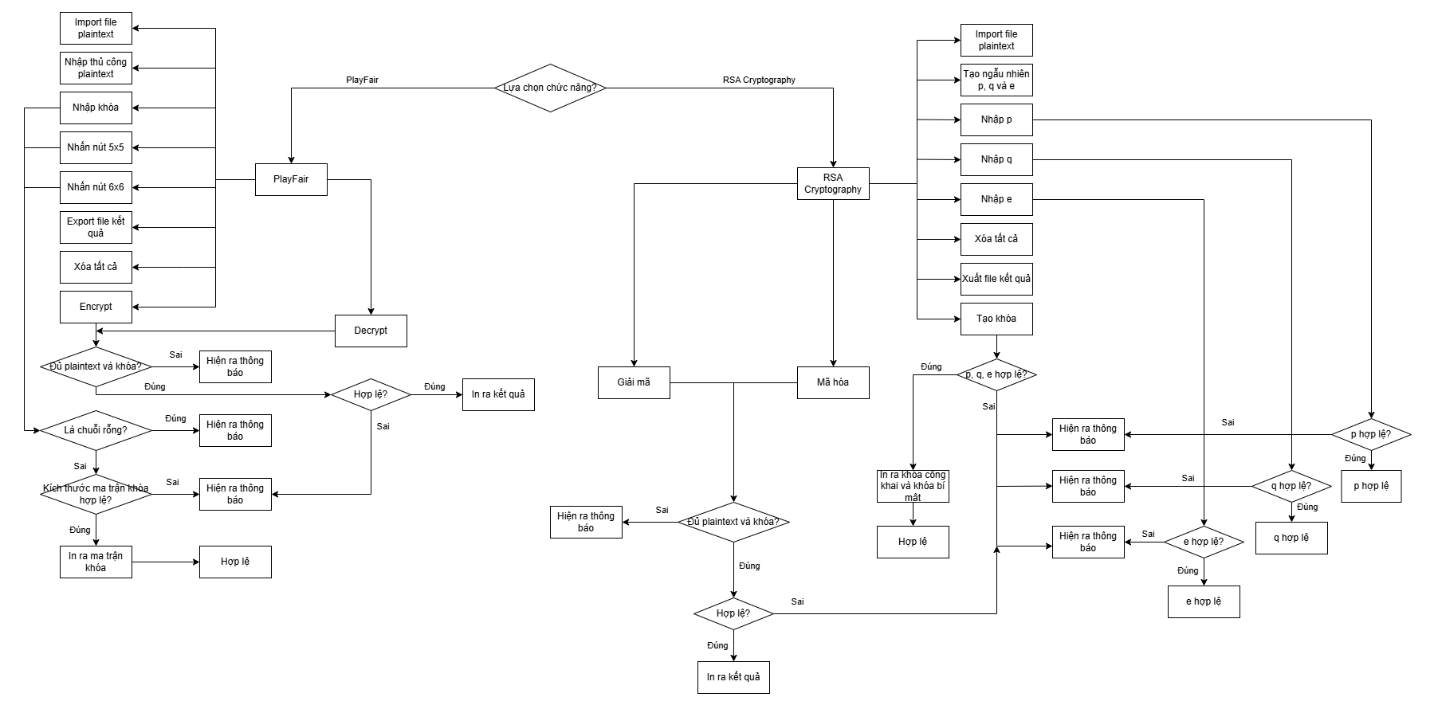
1. Giao diện chính của ứng dụng RSA Cryptography:

* Giao diện của kỹ thuật mã hóa / giải mã với Giải thuật RSA bao gồm các thành phần:
  + 2 Textbox bao gồm 1 Textbox dùng để hiển thị Dữ liệu (Input) do người dùng nhập vào để giải mã hoặc mã hóa và 1 Textbox với chức năng hiển thị Kết quả (Output) sau khi đã mã hóa / giải mã dữ liệu
  + Ngoài ra sử dụng 2 Rich Textbox khác để hiển thị các nội dung về khóa công khai, khóa bí mật được trích xuất thông qua việc tính toán dữ liệu p,q và e bởi người dùng nhập vào.
  + Đồng thời sử dụng các button để thực hiện các chức năng chính như:
    - Mã hóa
    - Giải mã
    - Thêm file (Input)
    - Xuất file (Output)
    - Tạo giá trị ngẫu nhiên
    - Tạo khóa (từ giá trị nhập vào)
    - Xóa



*Giao diện chương trình RSA Cryptography*

1. **Lưu đồ hoạt động**

****

Link ảnh: <https://drive.google.com/file/d/1YLrJdZFoOd5gh2b4fHzxZGev1ocbQWLx/view?usp=drive_link>

**5. Một số màn hình chạy ví dụ của chương trình**

a. Chạy chương trình ứng dụng PlayFair

* Mã hóa (Encrypt)

A screenshot of a computer

Description automatically generated

*Mã hóa với khóa chỉ bao gồm chữ (5x5)*

A screenshot of a computer

Description automatically generated

*Mã hóa với khóa bao gồm cả số và chữ (6x6)*

* Giải mã (Decrypt)

A screenshot of a computer

Description automatically generated

*Giải mã thông điệp vừa tạo ở trên*

* Thêm file / Xuất file:

*Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động*

*Thêm file (Input)*

*Ảnh có chứa văn bản, ảnh chụp màn hình, phần mềm, Phần mềm đa phương tiện

Mô tả được tạo tự động*

*Xuất file (Output)*

1. Chạy chương trình RSA Cryptography

* Mã hóa (Encrypt)

Ảnh có chứa văn bản, ảnh chụp màn hình, Hình chữ nhật, thiết kế

Mô tả được tạo tự động

*Mã hóa thông điệp với khóa thủ công*

Ảnh có chứa văn bản, ảnh chụp màn hình

Mô tả được tạo tự động

*Mã hóa thông điệp với giá trị khóa ngẫu nhiên (512 bit)*

* Giải mã (Decrypt)

Ảnh có chứa văn bản, ảnh chụp màn hình, biểu đồ, Hình chữ nhật

Mô tả được tạo tự động

*Giải mã thông điệp với khóa thủ công vừa tạo*

*Ảnh có chứa văn bản, ảnh chụp màn hình, thiết kế

Mô tả được tạo tự động*

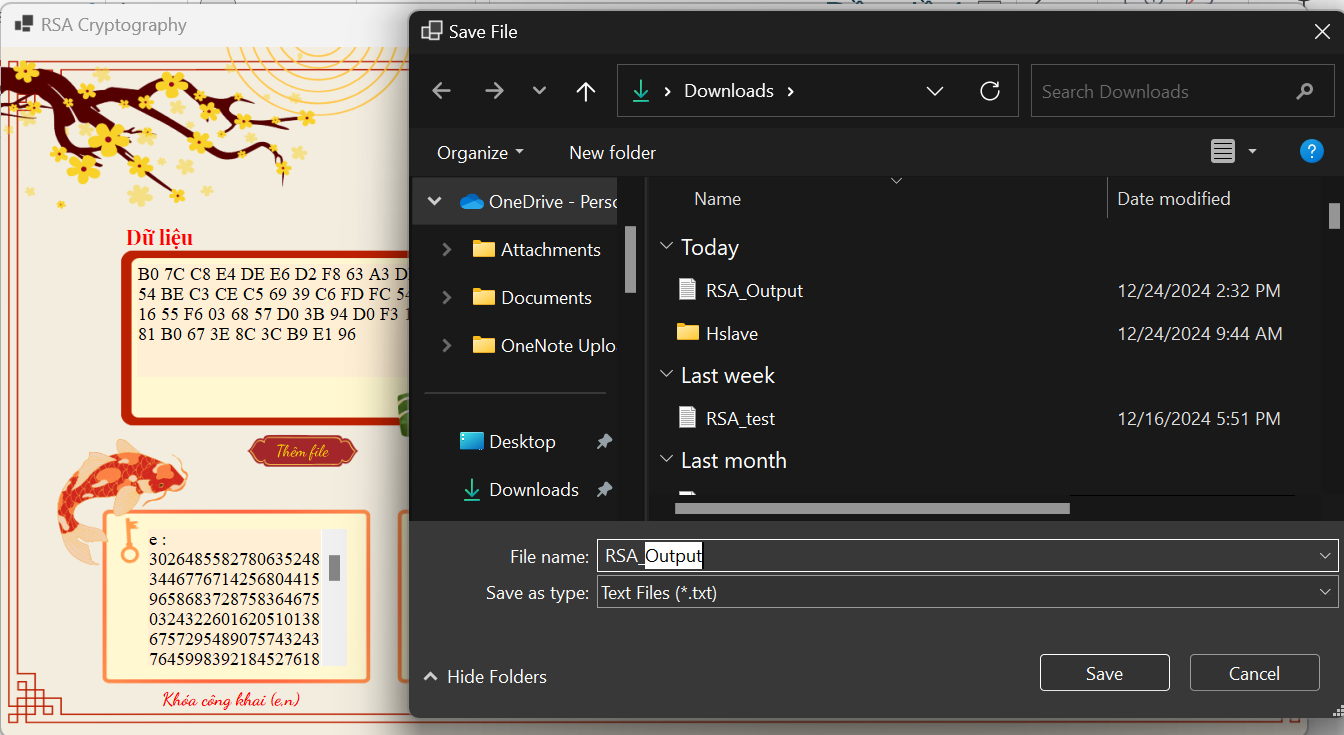
*Giải mã thông điệp với khóa ngẫu nhiên vừa tạo*

* Thêm file / Xuất file:

Ảnh có chứa văn bản, phần mềm, ảnh chụp màn hình, Phần mềm đa phương tiện

Mô tả được tạo tự động

*Thêm file (Input)*



*Xuất file Output*

Ảnh có chứa văn bản, ảnh chụp màn hình, thiết kế

Mô tả được tạo tự động

*Xuất file thành công*

**6. Lỗi của ứng dụng (nếu có)**

**7. Hướng phát triển**

**PlayFair:**

1. **Mở rộng tính năng:**

* Cho phép người dùng chọn cách chèn ký tự đệm khác ngoài "X".
* Thêm tùy chọn để mã hóa/giải mã văn bản không cần chuẩn hóa (giữ nguyên ký tự gốc).
* Hỗ trợ xử lý file văn bản lớn hoặc xử lý hàng loạt.

1. **Đa nền tảng:**

* Phát triển thêm phiên bản dựa trên web hoặc ứng dụng di động để mở rộng đối tượng sử dụng.
* Tách biệt phần xử lý thuật toán (logic) với giao diện người dùng, giúp dễ dàng triển khai trên nhiều môi trường khác nhau.

1. **Kiểm tra và bảo mật:**

* Thêm các test case tự động để kiểm tra tính đúng đắn của mã hóa/giải mã trong các trường hợp khác nhau.
* Cải thiện bảo mật bằng cách thêm tùy chọn kết hợp với các thuật toán mã hóa hiện đại khác (AES, RSA...).

**RSA Cryptography:**

1. **Tối ưu hóa hiệu suất mã hóa và giải mã:**

* Sử dụng đa luồng (Multithreading): Chia nhỏ quá trình mã hóa/giải mã thành nhiều luồng xử lý song song để tăng tốc độ xử lý dữ liệu lớn.
* Cải thiện thuật toán số nguyên tố: Thay thế kiểm tra số nguyên tố bằng các thuật toán nhanh hơn như Miller-Rabin với cải tiến hoặc AKS primality test.
* Giảm bộ nhớ sử dụng: Tối ưu các thao tác xử lý chuỗi và bộ đệm để giảm bộ nhớ tiêu thụ.

1. **Hỗ trợ kích thước khóa lớn hơn:**

* Mở rộng khả năng sinh khóa RSA với kích thước lớn hơn (tối thiểu 2048 bit hoặc 4096 bit) để tăng cường tính bảo mật.
* Thêm kiểm tra và cảnh báo khi người dùng nhập kích thước khóa nhỏ không an toàn.

1. **Thêm giao diện quản lý khóa:**

* Xuất/Nhập khóa: Hỗ trợ lưu và đọc khóa từ file (ví dụ: định dạng PEM hoặc XML).
* Quản lý danh sách khóa: Cho phép lưu trữ nhiều cặp khóa công khai/riêng tư để quản lý tập trung.

**8. Các file thuộc ứng dụng:**

* **Link Google Drive :** <https://drive.google.com/drive/folders/1A0KNsaPUVndgQOL3-CpoSiVJ2wDEw1i_>
* **Link Github:** <https://github.com/TranDai108/DoAn_ATM.git>