Trường Đại học Công nghiệp Hà Nội

BÁO CÁO THỰC NGHIỆM

HỌC PHẦN
AN TOÀN &BẢO MẬT THÔNG TIN

Nhóm 13

Giảng viên: TS. Phạm Văn Hiệp

06/2023

HAUI

Nhóm 13

ĐỀ TÀI
XÂY DỰNG CHƯƠNG TRÌNH MÃ HÓA VÀ GIẢI MÃ RSA SỬ DỤNG NGÔN NGỮ JAVA, C#

Trương Công Mạnh

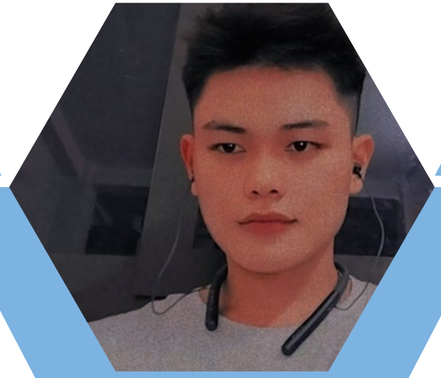
2021601910

Nguyễn Thị Thu Phương

2020602360

Nguyễn Văn Nguyên

2020605636



Nguyễn Nam Phi

2020606964

Trần Hồng Nhung

2020608128

HAUI

Nội dung

- I. Tổng quan
- II. Kết quả nghiên cứu
- III. Kết luận và bài học kinh nghiệm

HAUI

I. Tổng quan

1. Tổng quan về An toàn & bảo mật thông tin
2. Lý do chọn đề tài
3. Nội dung nghiên cứu
4. Các kiến thức cơ sở

Tổng quan
An toàn & bảo mật thông tin

An toàn thông tin là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi hoặc phá hủy thông tin một cách trái phép

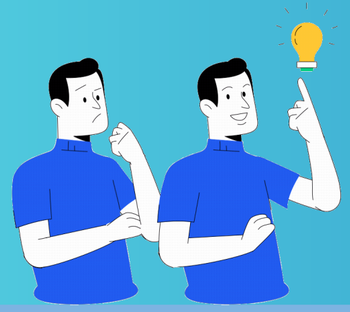
Các loại hình tấn công:
->Xem trộm thông tin
->Thay đổi thông điệp
->Phát lại thông tin
->Mạo danh

Các yêu cầu an toàn bảo mật thông tin
->Tính bảo mật
->Tính toàn vẹn
->Tính sẵn sàng

Hệ mật mã

An toàn thông tin bằng mật mã
Lập mã: mã hóa và giải mã
Phá mã: phá mã hoặc tạo mã giả

Các mức độ bảo vệ
Tường lửa ->Bảo vệ vật lý->Mã hóa dữ liệu ->Đăng ký và mật khẩu ->Quyền truy cập ->Thông tin



1

Lý do chọn đề tài

Trong phương pháp mã hóa bất đối xứng nổi bật là phương pháp mã hóa RSA- một thuật toán mật mã hóa khóa công khai. Đây là thuật toán đầu tiên phù hợp với việc tạo ra chữ ký điện tử đồng thời với việc mã hóa. Nó đánh dấu một sự tiến bộ vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công cộng.

2

Nội dung nghiên cứu

1. **Tìm hiểu mã hóa công khai**
2. **Nghiên cứu, tìm hiểu về hệ mật mã RSA**
3. **Tìm hiểu nội dung các thuật toán được ứng dụng trong chương trình**
4. **Thiết kế chương trình, cài đặt thuật toán**

3

Các kiến thức cơ sở

1. **Định lý Euclid,**
2. **Thuật toán Euclid mở rộng**
3. **Định lí Fermat**
4. **Hàm số Euler**
5. **Thuật toán Miller-Rabin**
6. **Thuật toán Bình phương và nhân**
7. **Sử dụng một số ngôn ngữ khá phổ biến hiện nay như C#, Java**
8. **Phương pháp tạo khóa, mã hóa và giải mã RSA**

HAUI

II. Kết quả nghiên cứu

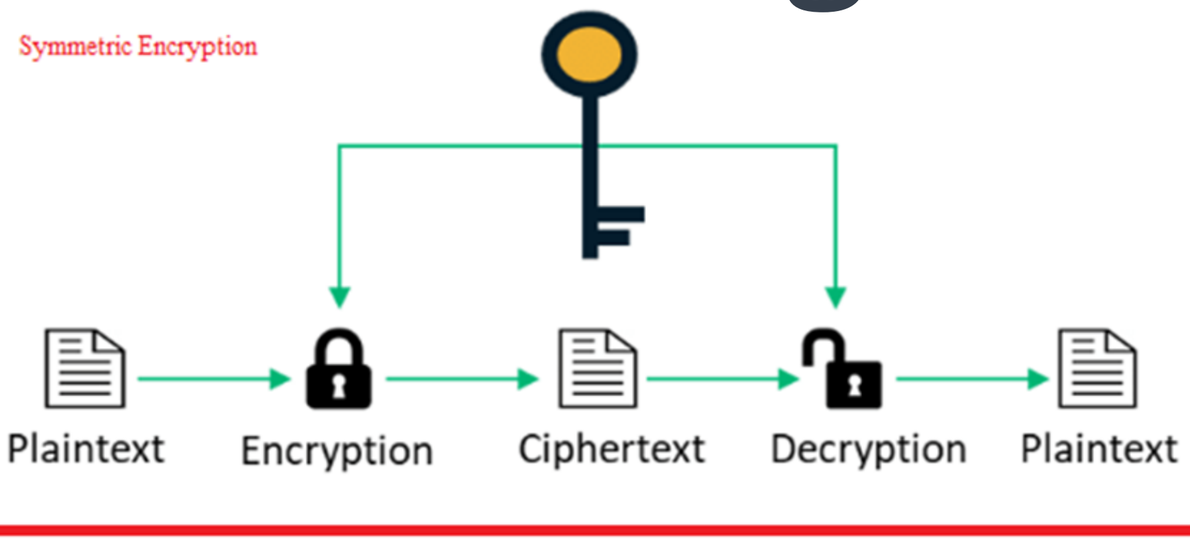
1. Nghiên cứu, tìm hiểu hệ mã hóa công khai

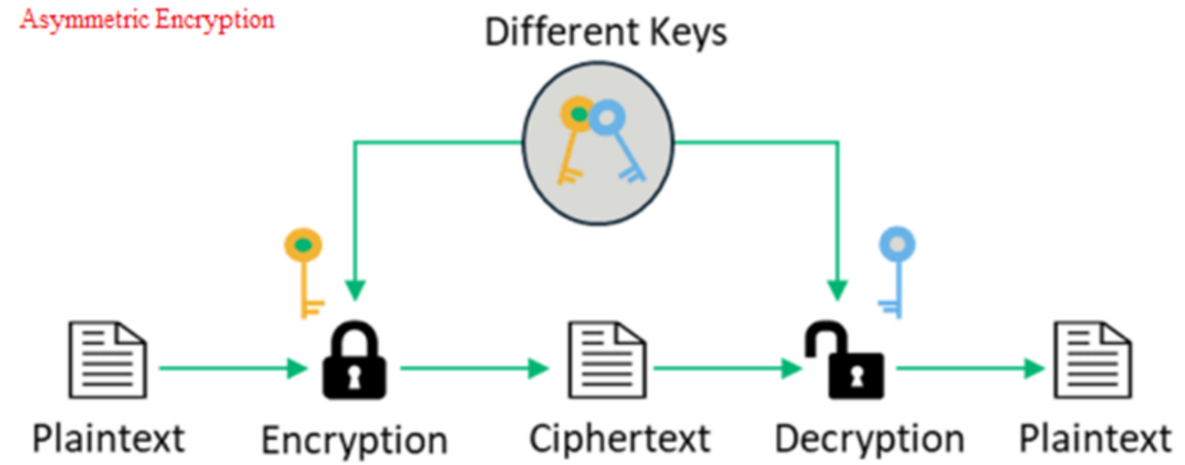
2. Nghiên cứu, tìm hiểu về hệ mật mã RSA

3. Nội dung thuật toán

4. Thiết kế chương trình, cài đặt thuật toán

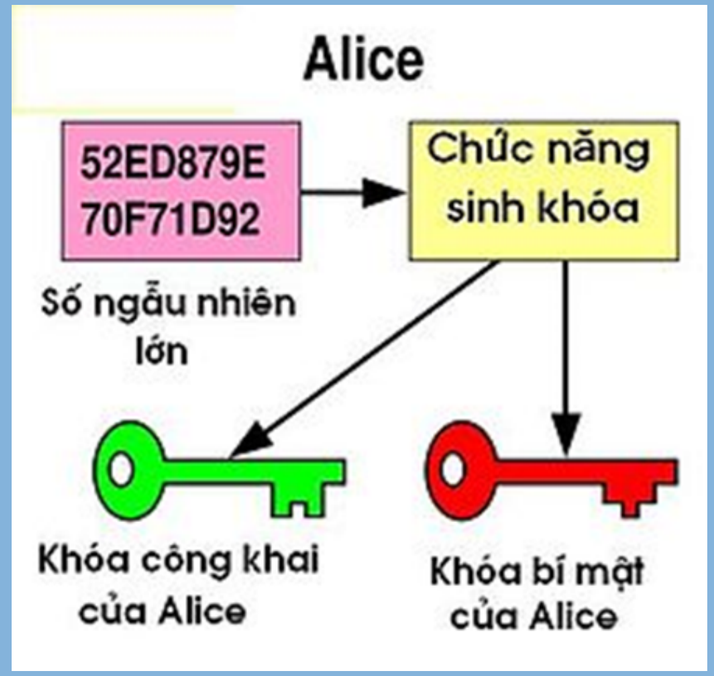
Mã hóa công khai





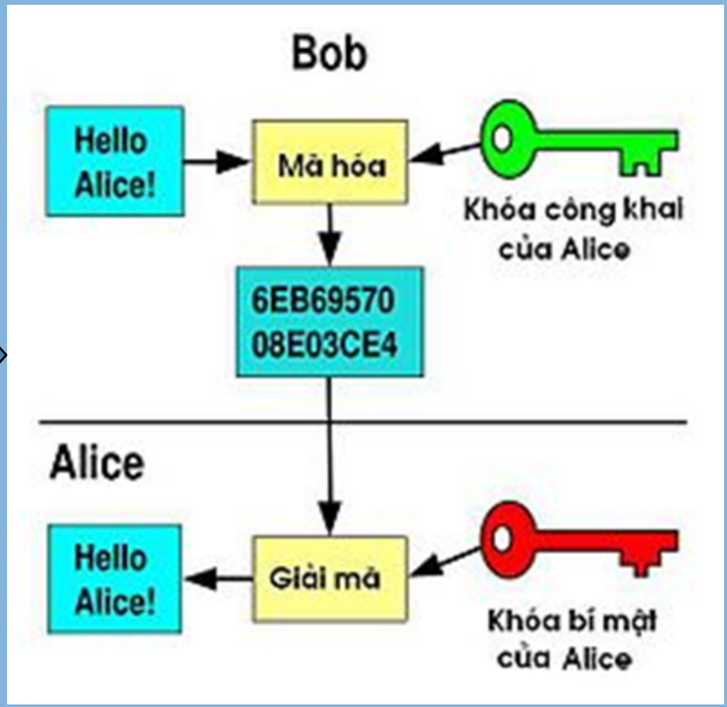
Mã khóa đối xứng và mã hóa bất đối xứng

Nhóm 13



Chọn một số ngẫu nhiên lớn để sinh cặp khóa

Dùng khóa công khai để mã hóa, khóa bí mật để giải mã



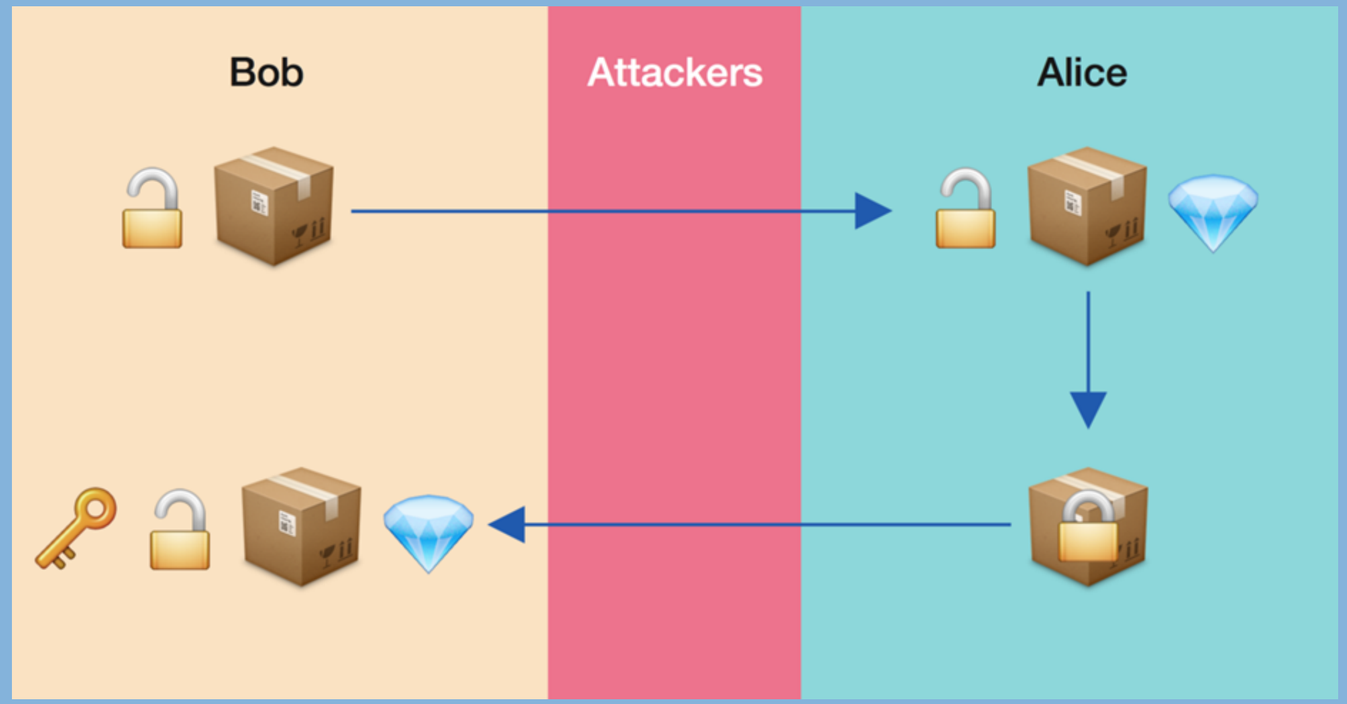
HAUI

Hệ mật mã RSA

RSA là một thuật toán mật mã hóa khóa công khai, mã hóa bất đối xứng

Được sử dụng phổ biến trong thương mại điện tử và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

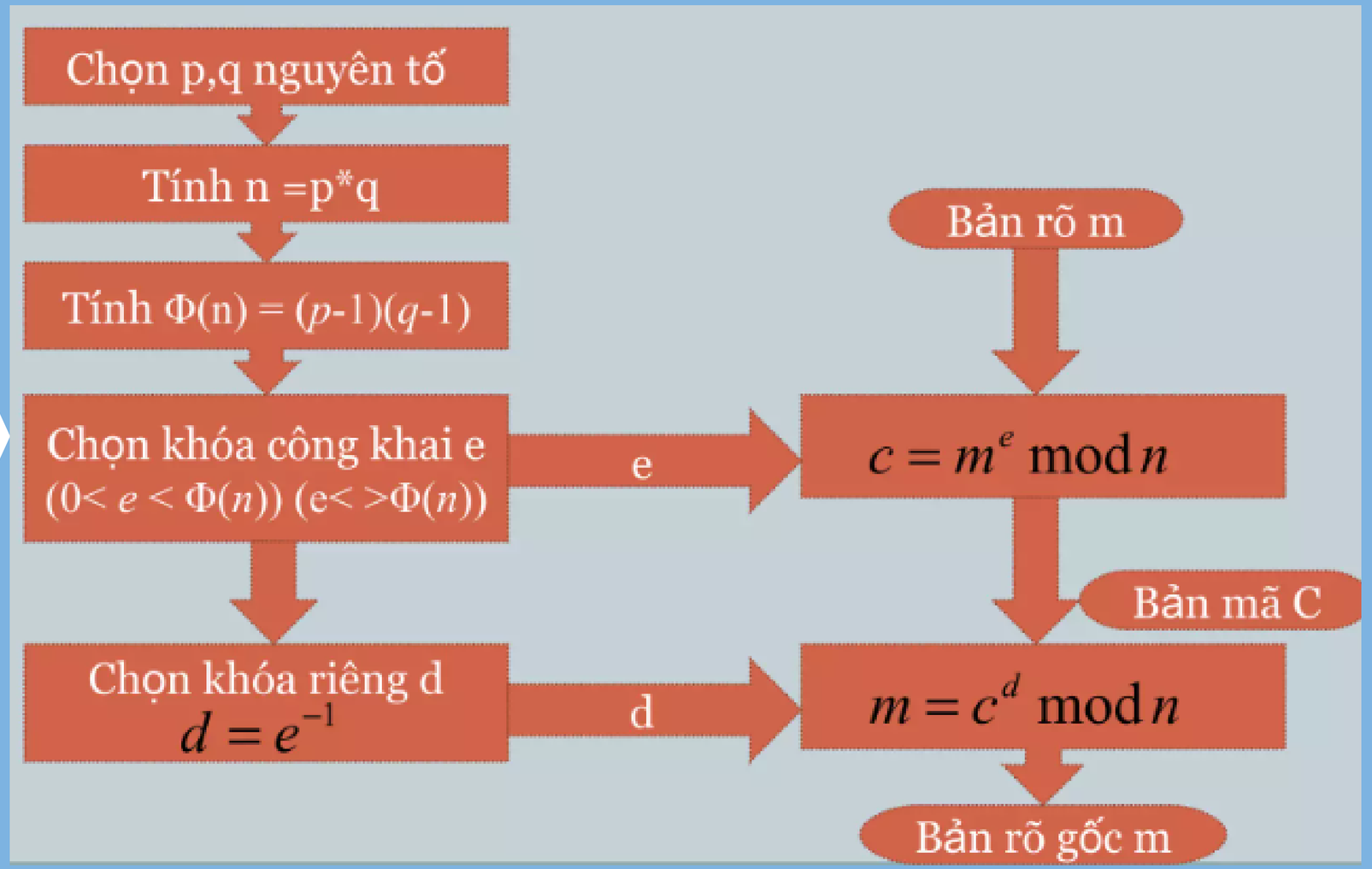
RSA được xây dựng dựa trên tính khó của bài toán phân tích các số lớn ra thừa số nguyên tố: Biết một số nguyên tố nhân chúng với nhau để thu được một hợp số là dễ còn biết hợp số phân tích nó ra thừa số nguyên tố là khó.



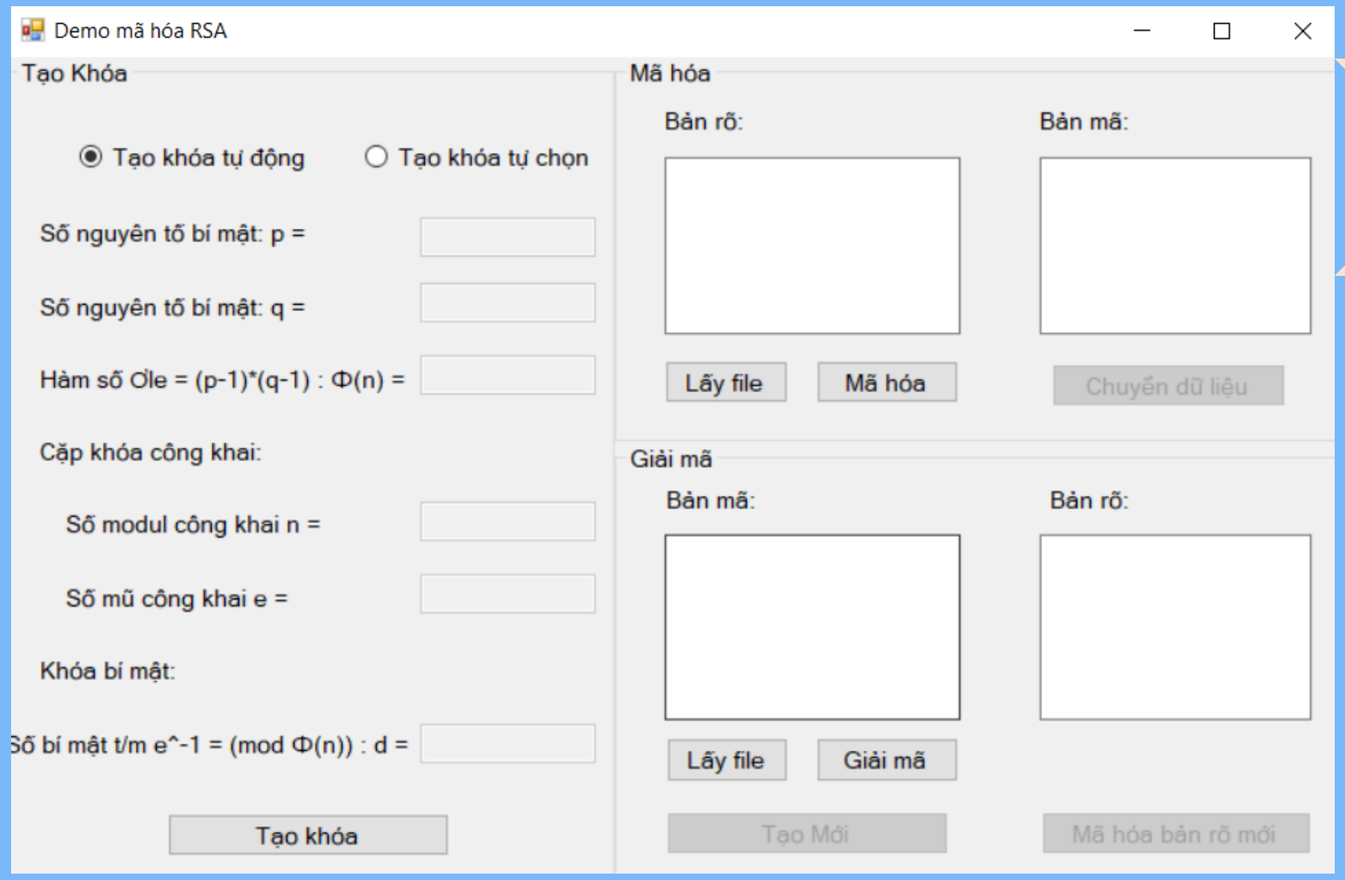
Minh họa ý tưởng Hệ mật RSA

HAUI

3. Nội dung thuật toán



Thiết kế chương trình, cài đặt thuật toán C#



Giao diện chương trình

1. Chọn chức năng tạo khóa tự động hoặc tự chọn.

2. Nhập p, q nếu chọn tạo khóa tự chọn.

3.Nhập bản rõ hoặc lấy file sẵn có cần mã hóa và chọn "Mã hóa".

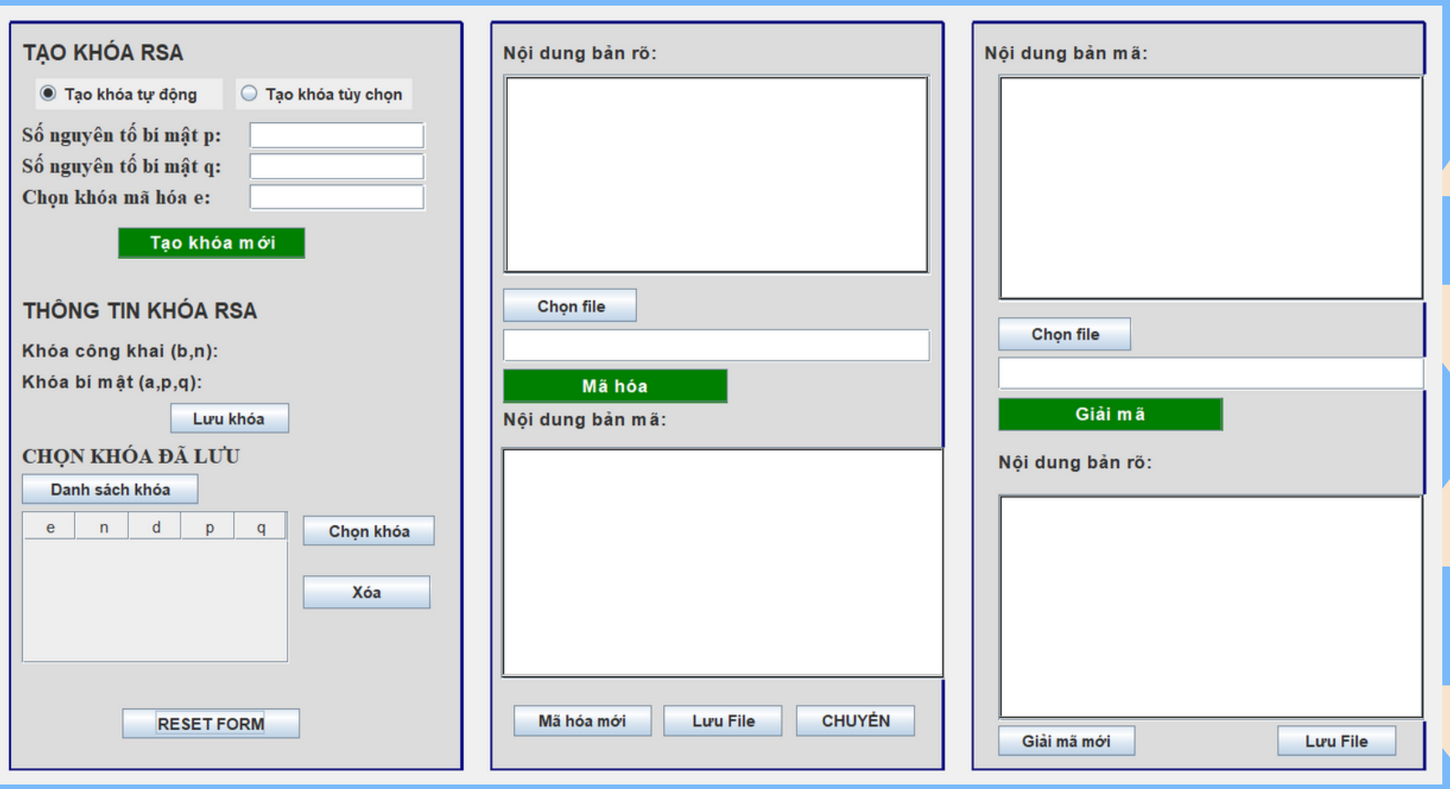
4. Chọn "Chuyển dữ liệu nếu muốn giải mã ngay sau khi mã hóa hoặc nhập bản mã / chọn"Lấy file" để chọn bản mã muốn giải mã.

5. Chọn "Giải mã".

6. Sau khi mã hóa, nội dung đoạn mã sẽ đượ lưu vào file txt.

7. Khi muốn tạo mới các nội dung, người dùng nhấn nút "Tạo mới" hoặc chọn "Mã hóa bản rõ mới" để sử dụng lại khóa cũ đã tạo.

Thiết kế chương trình, cài đặt thuật toán Java



1. Chọn chức năng tạo khóa tự động hoặc tùy chọn.

2. Nhập p, q ,e nếu chọn tạo khóa tùy chọn. Tạo khóa xong có thể lưu lại khóa bằng cách chọn "Lưu khóa".

3.Nhập bản rõ hoặc lấy file sẵn có cần mã hóa và chọn "Mã hóa".

4. Chọn "Chuyển dữ liệu nếu muốn giải mã ngay sau khi mã hóa hoặc nhập bản mã / chọn"Lấy file" để chọn bản mã muốn giải mã.

5. Chọn "Giải mã".

6. Sau khi mã hóa, bạn có thể chọn "Lưu File" để lưu file.

7. Khi muốn tạo mới các nội dung, người dùng nhấn nút "reset form" hoặc chọn "Mã hóa mới" để sử dụng lại khóa cũ đã tạo.

III. Kết luận và bài học kinh nghiệm.

Kiến thức lĩnh hội

- Kỹ năng làm việc nhóm
- Kỹ năng tìm kiếm và chắt lọc thông tin cần tìm
- Kiến thức về mã hóa và giải mã RSA

Bài học kinh nghiệm

- Kỹ năng làm việc nhóm
- Hiểu rõ hơn về giải thuật RSA
- Tăng cường kỹ năng giải quyết vấn đề
- Học hỏi từ kinh nghiệm của các thành viên khác trong nhóm

TÀI LIỆU THAM KHẢO

01 TS. Phạm Văn Hiệp – Bài giảng, tài liệu môn *An toàn bảo mật thông tin* – Đại học Công nghiệp Hà Nội.

02 Tài liệu điện tử trên Internet.

03 Bùi Doãn Khanh, Nguyễn Đình Thúc, Mã hóa thông tin – *Lý thuyết và ứng dụng*, NXB Lao động xã hội, 2011.

HAUI

THANK YOU