BÌA

CC

DCMM

MẤY ML

**Mục lục**

[Chương 1. Giới thiệu chung. 3](#_Toc151040299)

[1.1. Lý do chọn đề tài 3](#_Toc151040300)

[1.2. Mục tiêu 4](#_Toc151040301)

[1.3. Phạm vi 4](#_Toc151040302)

[Chương 2. Tìm hiểu về RSA. 5](#_Toc151040303)

[2.1. Tổng quan về mật mã học 5](#_Toc151040304)

[2.2. Hệ mã hóa công khai 6](#_Toc151040305)

[2.2.1. Tìm hiểu về mã hóa công khai 6](#_Toc151040306)

[2.2.2. Lịch sử 7](#_Toc151040307)

[2.2.4. Cách tạo khóa 8](#_Toc151040308)

[2.2.5. Mã hóa 8](#_Toc151040309)

[2.2.6. Giải mã 8](#_Toc151040310)

[2.2.7. Tính bảo mật 8](#_Toc151040311)

[2.2.8. Quá trình tạo khóa 8](#_Toc151040312)

[2.2.9. Tốc độ 8](#_Toc151040313)

[Chương 3. Giới thiệu mã hóa RSA trong tin nhắn văn bản. 9](#_Toc151040314)

[3.1. Giới thiệu 9](#_Toc151040315)

[3.2. Mô tả hệ thống 9](#_Toc151040316)

[3.3. Giao diện chương trình 9](#_Toc151040317)

[3.4. Kết quả thực nghiệm 9](#_Toc151040318)

[Chương 4. Kết luận 9](#_Toc151040319)

[4.1. Các vấn đề đạt được 9](#_Toc151040320)

[4.2. Hạn chế 9](#_Toc151040321)

# Chương 1. Giới thiệu chung.

Cùng với sự phát triển của công nghệ thông tin, công nghệ mạng máy tính và sự phát triển của mạng internet ngày càng phát triển đa dạng và phong phú. Các dịch vụ trên mạng đã thâm nhập vào hầu hết các lĩnh vực trong đời sống xã hội. Các thông tin trên Internet cũng đa dạng về nội dung và hình thức, trong đó có rất nhiều thông tin cần được bảo mật cao hơn bởi tính kinh tế, tính chính xác và tính tin cậy của nó.

## Lý do chọn đề tài

Công nghệ thông tin đang phát triển, giúp ích rất nhiều trong đời sống chúng ta. Nhờ có nó mà mọi người có thể liên lạc với nhau một cách dễ dàng hơn bằng nhiều cách như gọi điện, call video hay nhắn tin, … Bên cạnh đó, thì luôn có nhưng kẻ nhòm ngó để có thể lấy cắp được thông tin nhằm mục đích xấu cho bản thân. Vậy nên đã có rất nhiều người chọn cách mã hóa tin nhắn để tăng tính bảo mật. Nhưng nói đến tin nhắn thì sẽ tồn tại người gửi và người nhận, vậy làm thế nào có thể gửi cho ai đó một tin nhắn được mã hóa mà không có cô hội trước đó? Đây cũng là nội dung mà nhóm chúng em đã tìm hiểu, chính là chuẩn mã hóa RSA.

Trước đây khi công nghệ máy tính chưa phát triển, khi nói đến vấn đề an toàn bảo mật thông tin, chúng ta thường hay nghĩ đến các biện pháp nhằm đảm bảo cho thông tin được trao đổi hay cất giữ một cách an toàn và bí mật, chẳng hạn là các biện pháp như: Đóng dấu và ký niêm phong một bức thư để biết rằng lá thư có được chuyển nguyên vẹn đến người nhận hay không, dùng mật mã mã hóa thông điệp để chỉ có người gửi và người nhận hiểu được thông điệp, lưu giữ tài liệu trong các két sắt có khóa tại nơi được bảo vệ nghiêm ngặt.

Ngày nay với sự phát triển của khoa học công nghệ, đặt biệt là sự phát triển của Internet, việc sử dụng máy tính và điện thoại cá nhân càng trở lên rộng rãi, dẫn đến càng nhiều thông tin được lưu trữ trên máy tính và gửi đi trên mạng Intemet. Do đó nhu cầu về an toàn và bảo mật thông tin trên máy tính càng nhiều và việc sử dụng mật mã mã hóa càng được phổ biến. Trong đồ án này, em thực hiện xây dựng chương trình mã hóa và giải mã mật mã hóa công khai RSA.

Trong quá trình tìm hiểu về RSA, tuy thời gian không nhiều nhưng với sự hướng dẫn và giúp đỡ của thầy, nhóm em đã hoàn thành. Do thời gian hạn chế nên phạm vi nghiên cứu và vẫn còn một số vấn đề chưa được giải quyết triệt để. Nhóm em mong nhận được sự đóng góp của thầy và các bạn, nhóm em xin chân thành cảm ơn thầy và các bạn!

## Mục tiêu

## Phạm vi

Tìm hiểu về thuật toán mã hóa RSA

# Chương 2. Tìm hiểu về RSA.

## 2.1. Tổng quan về mật mã học

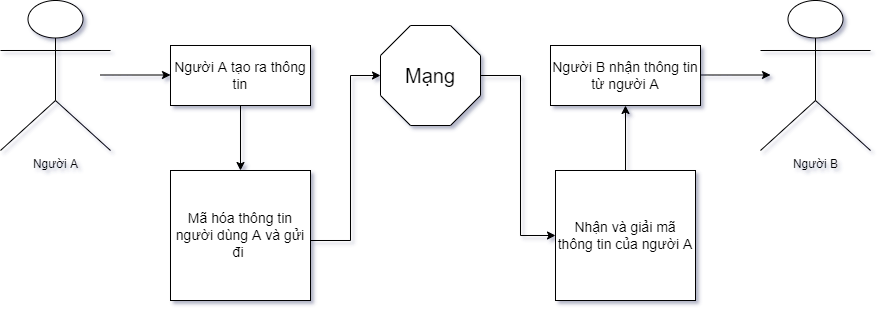
Trong mọi lĩnh vực kinh tế, chính trị, xã hội, quân sự... luôn có nhu cầu trao đổi thông tin giữa các cá nhân, các công ty, tổ chức, hoặc giữa các quốc gia với nhau. Ngày nay, với sự phát triển của công nghệ thông tin đặt biệt là mạng internet thì việc truyền tải thông tin đã dễ dàng và nhanh chóng hơn.

A white hexagon with black text

Description automatically generated

Hình 2. 1. Mô hình trao đổi thông tin qua mạng theo cách thông thường

Và vấn đề đặt ra là tính bảo mật trong quá trình truyền tải thông tin, đặt biệt quan trọng đối với những thông tin liên quan đến chính trị, quân sự, hợp đồng kinh tế.... Vì vậy nghành khoa học nghiên cứu về mã hóa thông tin được phát triển. Việc mã hóa là làm cho thông tin biến sang một dạng khác khi đó chỉ có bên gửi và bên nhận mới đọc được, còn người ngoài dù nhận được thông tin nhưng cũng không thể hiểu được nội dung.



Hình 2.2. Mô hình trao đổi thông tin qua mạng theo phương pháp mã hóa

Như chúng ta thấy ở mô hình 1.1: Việc trao đổi thông tin được thực hiện qua các bước sau:

* Tạo ra thông tin cần gửi đi.
* Gửi thông tin này cho đối tác.

Ở mô hình 1.2: Việc trao đổi thông tin được thực hiện:

* Tạo thông tin cần gửi
* Mã hóa và gửi thông tin đã được mã hóa đi. Đối tác nhận và giải mã thông tin
* Đối tác có được thông tin ban đầu của người gửi.

Với 2 thao tác mã hóa và giải mã ta đã đảm bảo thông tin được gửi an toàn và chính xác.

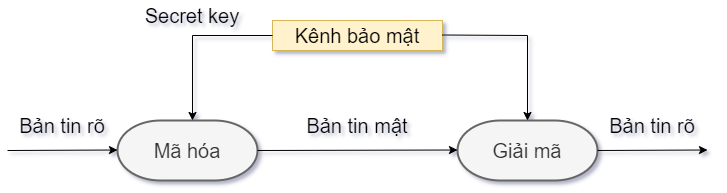
Chúng ta có nhiều phương pháp để mã hóa thông tin: Ở đây ta tìm hiểu về hệ mã hóa công khai RSA.

## 2.2. Hệ mã hóa công khai

### 2.2.1. Tìm hiểu về mã hóa công khai

* *Phân biệt mã hóa bí mật và mã hóa công khai*

Mã hóa bí mật: thông tin sẽ được mã hóa theo một phương pháp ứng với một key, key này dùng để lập mã và đồng thời cũng để giải mã. Vì vậy key phải được giữ bí mật, chỉ có người lập mã và người nhận biết được, nếu key bị lộ thì người ngoài sẽ dễ dàng giải mã và đọc được thông tin.



Hình 2.3. Mô hình mã hóa bí mật

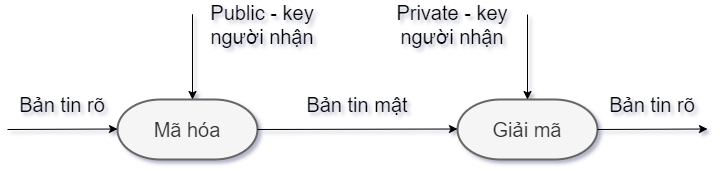
Mã hóa công khai: sử dụng 2 key public key private key.

Public key: Được sử dụng để mã hoá những thông tin mà ta muốn chia sẻ với bất cứ ai. Chính vì vậy ta có thể tự do phân phát nó cho bất cứ ai mà ta cần chia sẻ thông tin ở dạng mã hoá.

Privite key: Đúng như cái tên, Key này thuộc sở hữu riêng tư của bạn(ứng với public key) và nó được sử dụng để giải mã thông tin. Chỉ mình bạn sở hữu nó, Key này không được phép và không lên phân phát cho bất cứ ai.

Nghĩa là mỗi người sẽ giữ 2 key 1 dùng để mã hóa, key này được công bố rộng rãi, 1 dùng để giải mã, key này giữ kín.

Khi ai đó có nhu cầu trao đổi thông tin với bạn, sẻ dùng public key mà bạn công bố để mã hóa thông tin và gửi cho bạn, khi nhận được bạn dùng private key để giải mã. Những người khác dù có nhận được thông tin nhưng không biết được private key thì cũng không thể giải mã và đọc được thông tin.



Hình 2.4. Mô hình mã hóa công khai

Hàm một phía.

Một hàm một phía là hàm mà dễ dàng tính toán ra quan hệ một chiều nhưng rất khó để tính ngược lại. Ví như : biết giả thiết x thì có thể dễ dàng tính ra f(x), nhưng nếu biết f(x) thì rất khó tính ra được x. Trong trường hợp này “khó” có nghĩa là để tính ra được kết quả thì phải mất hàng triệu năm để tính toán, thậm chí tất cả máy tính trên thế giới này đều tính toán công việc đó.

Vậy thì hàm một phía tốt ở những gì ? Chúng ta không thể sử dụng chúng cho sự mã hoá. Một thông báo mã hoá với hàm một phía là không hữu ích, bất kỳ ai cũng không giải mã được. Đối với mã hoá chúng ta cần một vài điều gọi là cửa sập hàm một phía.(khóa)

Hộp thư là một ví dụ rất tuyệt về hàm một phía cũng như hình thức mã hóa này. Bất kỳ ai cũng có thể bỏ thư vào thùng. Bỏ thư vào thùng là một hành động công cộng. Mở thùng thư không phải là hành động công cộng. Nó là việc khó khăn, khi bạn không có chìa khóa ứng với thùng thư. Hơn nữa nếu bạn có điều bí mật (chìa khóa), nó thật dễ dàng mở hộp thư. Hệ mã hóa công khai có rất nhiều điều giống nhau như vậy.

### 2.2.2. Lịch sử

RSA được **R**ivest, **S**hamir và **A**dleman phát triển, là một thuận toán mật mã hóa khóa công khai. Nó đánh dấu một sự tiến hóa vượt bậc của lĩnh vực mật mã học trong việc sử dụng khóa công khai. RSA đang 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.

Thuật toán được Ron Rivest, Adi Shamir và Len Adleman mô tả lần đầu tiên vào năm 1977 tại Học viện Công nghệ Massachusetts (MIT). Tên của thuật toán lấy từ 3 chữ cái đầu của tên 3 tác giả.

Trước đó, vào năm 1973, Clifford Cocks, một nhà toán học người Anh làm việc tại GCHQ, đã mô tả một thuật toán tương tự. Với khả năng tính toán tại thời điểm đó thì thuật toán này không khả thi và chưa bao giờ được thực nghiệm. Tuy nhiên, phát minh này chỉ được công bố vào năm 1997 vì được xếp vào loại tuyệt mật.

RSA là một thí dụ điển hình về một đề tài toán học trừu tượng lại có thể áp dụng thực tiễn vào đời sống thường nhật . Khi nghiên cứu về các số nguyên tố, ít có ai nghĩ rằng khái niệm số nguyên tố lại có thể hữu dụng vào lãnh vực truyền thông.

### 2.2.4. Cách tạo khóa

### 2.2.5. Mã hóa

### 2.2.6. Giải mã

### 2.2.7. Tính bảo mật

### 2.2.8. Quá trình tạo khóa

### 2.2.9. Tốc độ

# Chương 3. Giới thiệu mã hóa RSA trong tin nhắn văn bản.

## 3.1. Giới thiệu

## 3.2. Mô tả hệ thống

## 3.3. Giao diện chương trình

## 3.4. Kết quả thực nghiệm

# Chương 4. Kết luận

## 4.1. Các vấn đề đạt được

## 4.2. Hạn chế