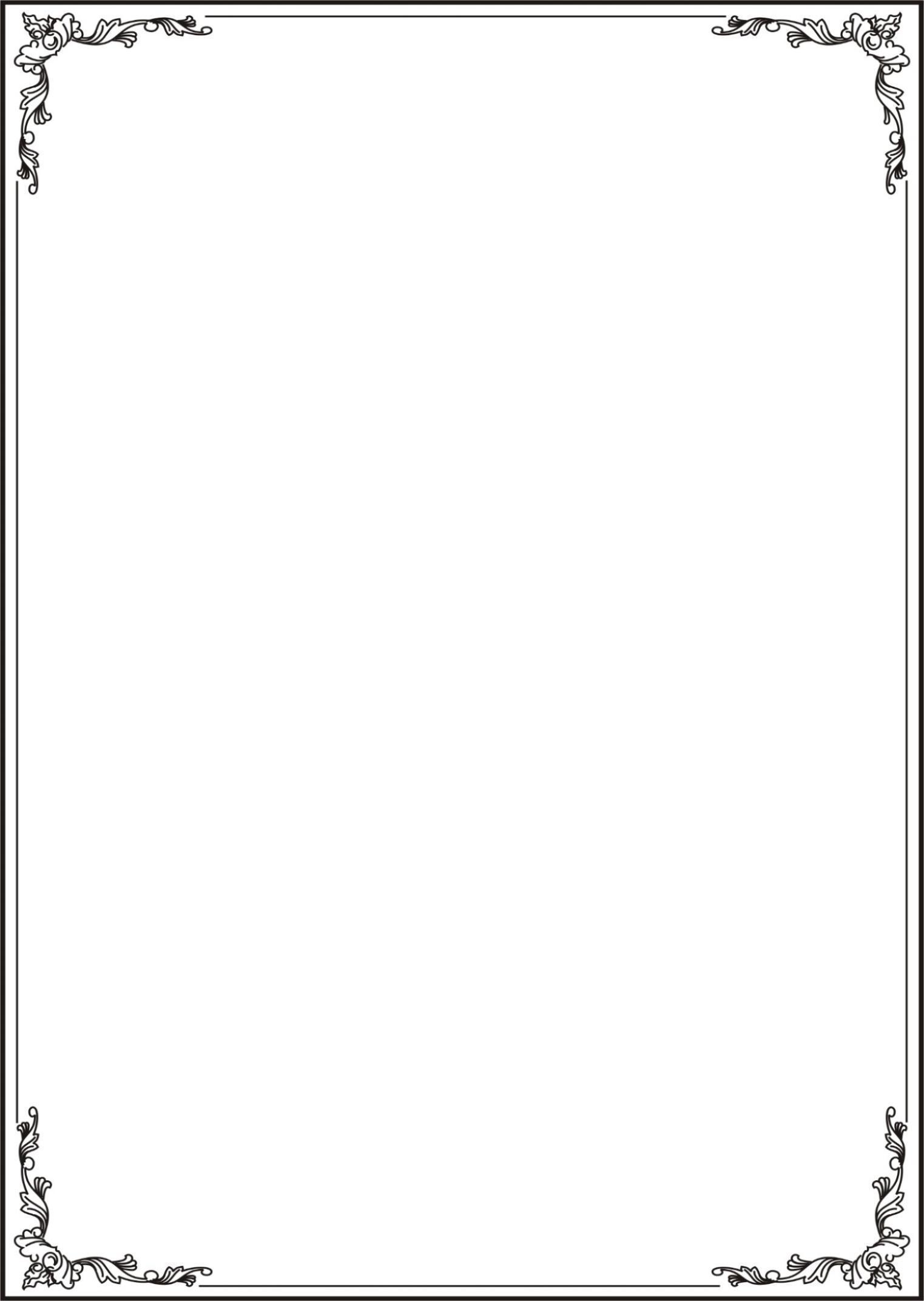
**BỘ CÔNG THƯƠNG**

**TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP HÀ NỘI**

**-----------------------------------------**



**BÀI TẬP LỚN**

**Môn: An toàn và bảo mật thông tin**

**XÂY DỰNG CHƯƠNG TRÌNH**

**MÃ HÓA VÀ GIẢI MÃ RSA**

| **CBHD: *ThS. Trần Phương Nhung*** | |
| --- | --- |
| **Nhóm: 5** | |
| **Thành viên nhóm:** | |
| 1. **Bạch Văn Hải** 2. **Nguyễn Chí Hải** 3. **Trần Thu Hằng** | **- 2019604483**  **- 2020608686**  **- 2019605379** |

**Hà Nội - Năm 2022**

**MỤC LỤC**

[LỜI CẢM ƠN 1](#_heading=h.1fob9te)

[LỜI NÓI ĐẦU 2](#_heading=h.3znysh7)

[CHƯƠNG 1: TỔNG QUAN 3](#_heading=h.2et92p0)

[1.1. Ý tưởng và đề tài nghiên cứu 3](#_heading=h.tyjcwt)

[1.2. Nội dung nghiên cứu 3](#_heading=h.3dy6vkm)

[1.3. Kiến thức 3](#_heading=h.1t3h5sf)

[1.3.1. Một số khái niệm 3](#_heading=h.4d34og8)

[1.3.2. Thuật toán Euclid 4](#_heading=h.2s8eyo1)

[1.3.3. Định lý Fermat 8](#_heading=h.17dp8vu)

[1.3.4. Hàm số Euler 8](#_heading=h.3rdcrjn)

[1.3.5. Thuật toán Miller-Rabin 9](#_heading=h.26in1rg)

[1.3.6. Định lý phần dư Trung Hoa 11](#_heading=h.lnxbz9)

[1.3.7. Hệ mã hóa RSA 12](#_heading=h.35nkun2)

[CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU 14](#_heading=h.1ksv4uv)

[2.1. Giới thiệu 14](#_heading=h.44sinio)

[2.2. Nội dung thuật toán 14](#_heading=h.2jxsxqh)

[2.3. Thiết kế, cài đặt chương trình demo thuật toán 15](#_heading=h.z337ya)

[2.3.1. Giao diện chương trình demo theo ngôn ngữ Python 15](#_heading=h.3j2qqm3)

[2.3.2. Giao diện chương trình demo theo ngôn ngữ PHP 17](#_heading=h.1ci93xb)

[2.3.3. Giao diện chương trình demo theo ngôn ngữ Java 17](#_heading=h.2bn6wsx)

[2.4. Cài đặt và triển khai 19](#_heading=h.49x2ik5)

[2.4.1. Giới thiệu công cụ 19](#_heading=h.2p2csry)

[2.4.1.1. Giới thiệu công cụ Visual Studio Code 19](#_heading=h.147n2zr)

[2.4.1.2. Giới thiệu công cụ NetBeans 19](#_heading=h.3o7alnk)

[2.4.1.3. Giới thiệu công cụ máy chủ ảo XAMPP 19](#_heading=h.23ckvvd)

[2.4.2. Hướng dẫn cài đặt và chạy chương trình 20](#_heading=h.ihv636)

[2.4.2.1. Cài đặt Visual Studio Code và chạy chương trình demo 20](#_heading=h.32hioqz)

[2.4.2.2. Cài đặt Xampp và chạy chương trình demo 25](#_heading=h.28h4qwu)

[2.4.2.3. Cài đặt NetBeans và chạy chương trình demo 29](#_heading=h.206ipza)

[2.5. Thực hiện bài toán 34](#_heading=h.2r0uhxc)

[2.5.1. Phân công công việc 34](#_heading=h.1664s55)

[2.5.2. Bạch Văn Hải - Tìm hiểu thuật toán Miller-Rabin và cài đặt chương trình demo 34](#_heading=h.3q5sasy)

[2.5.3. Nguyễn Chí Hải - Tìm hiểu thuật toán Euclid, định lý Fermat, hàm số Euler và cài đặt chương trình demo 35](#_heading=h.25b2l0r)

[2.5.4. Trần Thu Hằng - Tìm hiểu định lý phần dư Trung Hoa và cài đặt chương trình demo 35](#_heading=h.kgcv8k)

[CHƯƠNG 3: KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM 36](#_heading=h.34g0dwd)

[3.1. Nội dung đã thực hiện 36](#_heading=h.1jlao46)

[3.1.1. Các kiến thức đã lĩnh hội 36](#_heading=h.43ky6rz)

[3.1.2. Các kỹ năng đã tiếp thu 36](#_heading=h.2iq8gzs)

[3.1.3. Bài học kinh nghiệm 37](#_heading=h.xvir7l)

[3.2. Hướng phát triển 37](#_heading=h.3hv69ve)

[3.2.1. Tính khả thi của chủ đề nghiên cứu 37](#_heading=h.1x0gk37)

[3.2.2. Những thuận lợi, khó khăn 37](#_heading=h.4h042r0)

[3.2.3. Hướng phát triển và mở rộng của đề tài 38](#_heading=h.2w5ecyt)

[KẾT LUẬN 39](#_heading=h.1baon6m)

[TÀI LIỆU THAM KHẢO 40](#_heading=h.3vac5uf)

**DANH MỤC HÌNH ẢNH**

[*Hình 1: Giao diện tạo khóa bằng ngôn ngữ Python* 15](#_heading=h.1y810tw)

[*Hình 2: Giao diện mã hóa bằng ngôn ngữ Python* 16](#_heading=h.4i7ojhp)

[*Hình 3: Giao diện giải mã bằng ngôn ngữ Python* 16](#_heading=h.2xcytpi)

[*Hình 4: Giao diện bằng ngôn ngữ PHP* 17](#_heading=h.3whwml4)

[*Hình 5: Giao diện tạo khóa bằng ngôn ngữ Java* 17](#_heading=h.qsh70q)

[*Hình 6: Giao diện mã hóa bằng ngôn ngữ Java* 18](#_heading=h.3as4poj)

[*Hình 7: Giao diện giải mã bằng ngôn ngữ Java* 18](#_heading=h.1pxezwc)

[*Hình 8: Chọn project bằng công cụ Visual Studio Code* 20](#_heading=h.1hmsyys)

[*Hình 9: Giao diện tạo khóa bằng ngôn ngữ Python* 21](#_heading=h.41mghml)

[*Hình 10: Giao diện mã hóa bằng ngôn ngữ Python* 21](#_heading=h.2grqrue)

[*Hình 11: Giao diện giải mã bằng ngôn ngữ Python* 22](#_heading=h.vx1227)

[*Hình 12: Sinh khóa bằng ngôn ngữ Python* 22](#_heading=h.3fwokq0)

[*Hình 13: Mã hóa text bằng ngôn ngữ Python* 23](#_heading=h.1v1yuxt)

[*Hình 14: Mã hóa file .txt bằng ngôn ngữ Python* 23](#_heading=h.4f1mdlm)

[*Hình 15: Mã hóa file .docx bằng ngôn ngữ Python* 24](#_heading=h.2u6wntf)

[*Hình 16: Mã hóa thông tin bằng ngôn ngữ Python* 24](#_heading=h.19c6y18)

[*Hình 17: Giải mã thông tin bằng ngôn ngữ Python* 25](#_heading=h.3tbugp1)

[*Hình 18: Công cụ Xampp* 26](#_heading=h.nmf14n)

[*Hình 19: Giao diện chương trình bằng ngôn ngữ PHP* 26](#_heading=h.37m2jsg)

[*Hình 20: Giao diện mã hóa bằng ngôn ngữ PHP* 27](#_heading=h.1mrcu09)

[*Hình 21: Chọn file bằng ngôn ngữ PHP* 27](#_heading=h.46r0co2)

[*Hình 22: Mã hóa thông tin bằng ngôn ngữ PHP* 28](#_heading=h.2lwamvv)

[*Hình 23: Giao diện giải mã bằng ngôn ngữ PHP* 28](#_heading=h.111kx3o)

[*Hình 24: Mã hóa thông tin bằng ngôn ngữ PHP* 29](#_heading=h.3l18frh)

[*Hình 25: Mở project bằng công cụ NetBeans* 29](#_heading=h.4k668n3)

[*Hình 26: Chạy project* 30](#_heading=h.2zbgiuw)

[*Hình 27: Giao diện chương trình bằng ngôn ngữ Java* 30](#_heading=h.1egqt2p)

[*Hình 28: Tạo khóa bằng ngôn ngữ Java* 31](#_heading=h.3ygebqi)

[*Hình 29: Nhập thông tin mã hóa bằng ngôn ngữ Java* 31](#_heading=h.2dlolyb)

[*Hình 30: Nhập file .txt bằng ngôn ngữ Java* 32](#_heading=h.sqyw64)

[*Hình 31: Nhập file .docx bằng ngôn ngữ Java* 32](#_heading=h.3cqmetx)

[*Hình 32: Mã hóa thông tin bằng ngôn ngữ Java* 33](#_heading=h.1rvwp1q)

[*Hình 33: Giải mã thông tin bằng ngôn ngữ Java* 33](#_heading=h.4bvk7pj)

# LỜI CẢM ƠN

Bài báo cáo học phần An Toàn Và Bảo Mật Thông Tin với đề tài *“Xây dựng chương trình mã hóa và giải mã RSA”* là kết quả của quá trình học tập không ngừng nghỉ của các thành viên trong nhóm và nhận được sự giúp đỡ tận tình, động viên, khích lệ của thầy cô, bạn bè. Qua đây, nhóm chúng em xin gửi lời cảm ơn chân thành đến những người đã giúp đỡ chúng em trong thời gian học tập, nghiên cứu vừa qua.

Trước hết, chúng em xin chân thành cảm ơn ban giám hiệu cùng toàn thể quý thầy, cô khoa Công nghệ thông tin trường Đại học Công nghiệp Hà Nội đã tạo điều kiện cho nhóm chúng em hoàn thành tốt bài tiểu luận này.

Em xin trân trọng gửi đến cô Trần Phương Nhung - người đã trực tiếp hướng dẫn cũng như cung cấp tài liệu, thông tin khoa học cần thiết để hoàn thành bài báo cáo này lời cảm ơn chân thành và sâu sắc nhất. Đó là những góp ý hết sức quý báu không chỉ trong quá trình thực hiện bài tiểu luận này mà còn là hành trang tiếp bước trong quá trình học tập và lập nghiệp sau này.

Và cuối cùng, xin gửi lời cảm ơn đến gia đình, bạn bè, tập thể lớp 20214IT6001001, những người luôn sẵn sàng sẻ chia và giúp đỡ chúng em trong học tập và cuộc sống. Mong rằng, chúng ta sẽ mãi mãi gắn bó với nhau.

Xin chúc những điều tốt đẹp nhất sẽ luôn đồng hành cùng mọi người.

Chúng em xin chân thành cảm ơn!

*Nhóm sinh viên thực hiện*

# LỜI NÓI ĐẦU

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, đặc 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 Internet. Do đó nhu cầu về an toàn và bảo mật thông tin trên máy tính càng nhiều và việc sử dụng mật mã mã hoá càng phổ biến hơn.

Từ nhu cầu thực tế đó, nhằm có cái nhìn bao quát về các hệ mã hóa, cách mã hóa, giải mã dữ liệu và ứng dụng thực tế của các hệ mã hóa, nhóm chúng em lựa chọn thực hiện đề tài *“Xây dựng chương trình mã hóa và giải mã RSA”*.

Bài báo cáo gồm 3 chương:

Chương 1. Tổng quan

Chương 2. Kết quả nghiên cứu

Chương 3. Kiến thức lĩnh hội và bài học kinh nghiệm

Trong quá trình thực hiện đề tài sẽ không thể tránh khỏi những thiếu sót, vì vậy chúng em mong nhận được sự đóng góp của cô và các bạn để hoàn thiện hơn.

# CHƯƠNG 1: TỔNG QUAN

## Ý tưởng và đề tài nghiên cứu

Ý tưởng về một hệ mật khoá công khai đã được Diffie và Hellman đưa ra vào 1976. Còn việc hiện thực hóa hệ mật khoá công khai thì do Rivest, Shamir và Adleman đưa ra đầu tiên vào 1977, họ đã tạo nên hệ mật RSA nổi tiếng.

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. RSA đang được sử dụng phổ biến trong [thương mại điện tử](https://vi.wikipedia.org/wiki/Th%C6%B0%C6%A1ng_m%E1%BA%A1i_%C4%91i%E1%BB%87n_t%E1%BB%AD) và được cho là đảm bảo an toàn với điều kiện độ dài khóa đủ lớn.

Xuất phát từ những lý do đó, nhóm đã quyết định lựa chọn đề tài nghiên cứu về mã hóa và giải mã trong hệ mã hóa RSA để xây dựng chương trình gồm các chức năng: tạo khóa, mã hóa và giải mã nhằm ứng dụng vào thực tiễn cuộc sống, đáp ứng nhu cầu xã hội.

## Nội dung nghiên cứu

- Kiến thức:

* Thuật toán Euclid
* Định lý Fermat
* Hàm số Euler
* Thuật toán Miller-Rabin
* Định lý phần dư Trung hoa
* Hệ mã hóa RSA

- Ngôn ngữ: Java, Python, PHP

## Kiến thức

### 1.3.1. Một số khái niệm

- Định nghĩa modulo: Cho số tự nhiên n và số nguyên a. Ta định nghĩa a mod n là phần dư dương khi chia a cho n.

VD: 5 mod 3 = 2

- Phép đồng dư ký hiệu a ≡ b mod n wps a và b có phần dư như nhau khi chia cho n.

VD: wps wps

- Ước số chung lớn nhất (ƯCLN) của hai hay nhiều số là số lớn nhất trong tập hợp các ước chung. Ước chung lớn nhất của a và b ký hiệu là GCD(a, b).

VD: GCD(6, 36) = 6 vì 6 mod 6 = 0 và 36 mod 6 = 0

- Số nguyên tố là số tự nhiên chỉ có đúng hai ước số là 1 và chính nó. Các số tự nhiên lớn hơn 1 không phải là số nguyên tố được gọi là hợp số.

VD: 3 là số nguyên tố vì

- Nguyên tố cùng nhau: a và b được gọi là nguyên tố cùng nhau nếu

GCD(a, b) = 1

VD: a = 8, b = 5 là nguyên tố cùng nhau vì GCD(8, 5) = 1.

### 1.3.2. Thuật toán Euclid

1. *Định nghĩa thuật toán*

- Thuật toán Euclid dùng để tìm ước số chung lớn nhất của hai số nguyên a và b. Ta ký hiệu ước số chung lớn nhất này là GCD(a,b). Thuật toán này dựa trên định lý sau

o **Định lý**: với mọi số nguyên a ≥ 0 và b > 0 thì:

gcd(a, b) = gcd(b, a mod b).

1. *Thuật toán Euclid tìm ước chung lớn nhất*

**Bài toán:** Cho 2 số nguyên dương A và B. Tìm ƯCLN(A, B)

If(A=0) return B

If(B=0) return A

While(B>0){

R=A mod B;

A=B; B=R;

}

return A

**Nhận xét:** Như vậy để tìm ước số chung lớn nhất của 1 cặp số cho trước, ta đưa về bài toán ƯCLN của cặp số gồm số nhỏ hơn gồm thương 2 số đó và phần dư của số lớn hơn khi chia cho số nhỏ hơn. Thuật toán Euclid tạo nên vòng lặp, ở mỗi bước ta áp dụng tinh chất trên khi phần dư đó còn khác 0.

**Ví dụ vận dụng:** Hãy áp dụng thuật toán Euclid tìm ước chung lớn nhất của 270 và 192.

Ta có: A = 270, B = 192, A ≠ 0, B ≠ 0

o Ta có: 270 / 192 = 1 dư 78

- Theo thuật toán Euclid ta có

o GCD(270, 192) = GCD(192, 78)

- Tìm GCD(192, 78)

o A = 192, B = 78, A ≠ 0, B ≠ 0

o Ta có: 192 / 78 = 2 dư 36

- Theo Euclid ta có:

o GCD(192, 78) = GCD(78, 36)

- Tìm GCD(78, 36)

o A = 78, B = 36, A ≠ 0, B ≠ 0

o Ta có: 78 / 36 = 2 dư 6

- Theo thuật toán Euclid ta có:

o GCD(78, 36) = GCD(36, 6)

- Tìm GCD(36, 6)

o A = 36, B = 6, A ≠ 0, B ≠ 0

o Ta có: 36 / 6 = 6 dư 0

- Theo thuật toán Euclid ta có GCD(36, 6) = GCD(6, 0) = 6

Vậy GCD(270, 192) = 6

1. *Thuật toán Euclid mở rộng tìm phần tử nghịch đảo*

**Định nghĩa**

Cho a , nếu sao cho . Khi đó b được gọi là phần tử nghịch đảo của a. Ký hiệu: .

**Định lý về sự tồn tại của phần tử nghịch đảo**

Nếu GCD(a, n) = 1 thì tồn tại duy nhất một số là phần tử nghịch đảo của a thỏa mãn

**Bổ đề Bezout**

Cho 2 số nguyên , tồn tại 2 số nguyên khác s và t sao cho

Khi đó .

**Thuật toán**

- Input:

- Output: (nếu tồn tại)

1) Dùng thuật toán Euclid mở rộng để tìm các số nguyên tố s và t sao cho

2) Nếu d > 1 thì không tồn tại. Ngược lại nếu d = 1 thì return (t).

Công thức tính s và t:

i=0

i=1

i

- Trong đó:

+ i = 0, 1, 2, 3,…

+

- Thuật toán dừng lại khi

**Ví dụ vận dụng:** Tìm

| **Bước i** |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **0** | 29 | 3 | 8 | 5 | 1 | 0 |
| **1** | 8 | 1 | 5 | 3 | 0 | 1 |
| **2** | 5 | 1 | 3 | 2 | 1 | -3 |
| **3** | 3 | 1 | 2 | 1 | -1 | 4 |
| **4** | 2 | 2 | 1 | 0 | 2 | -7 |
| **5** |  |  |  |  | -3 | 11 |

Bước i = 0 có ri = r0 = 29, ri+1 = r1 = 8

Lấy r0 = 29 chia cho r1 = 8 được thương qi+1 = q1 = 3, dư ri+2 = r2 = 5

Bước i = 1 có ri = r1 = 8, ri+1 = r2 = 5

Lấy r1 = 8 chia cho r2 = 5 được thương qi+1 = q2 = 1, dư ri+2 = r3 = 3

Bước i = 2 có ri = r2 = 5, ri+1 = r3 = 3

Lấy r2 = 5 chia cho r3 = 3 được thương qi+1 = q3 = 1, dư ri+2 = r4 = 2

Bước i = 3 có ri = r3 = 3, ri+1 = r4 = 2

Lấy r3 = 3 chia cho r4 = 2 được thương qi+1 = q4 = 1, dư ri+2 = r5 = 1

Bước i = 4 có ri = r4 = 2, ri+1 = r5 = 1

Lấy r4 = 2 chia cho r5 = 1 được thương qi+1 = q5 = 2, dư ri+2 = r6 = 0

Bước i = 5 có

Vậy t = t5 = 11 = 8-1 mod 29.

### 1.3.3. Định lý Fermat

Hay

**Ví dụ:** Tính (mod 7)

Ta thấy 7 là số nguyên tố và

Theo định lý Fermat nhỏ thì

Kiểm tra lại có

### 1.3.4. Hàm số Euler

1. *Định nghĩa*

- Hàm phi Euler của 1 số nguyên dương n là số các số nguyên tố cùng nhau với n và nhỏ hơn n.

- Ký hiệu:

1. *Tính chất của hàm phi Euler*

- Tính chất 1: Nếu n là số nguyên tố thì

- Tính chất 2: Nếu p và q là 2 số nguyên tố cùng nhau thì

- Tính chất 3: Nếu p là số nguyên tố thì

1. *Định lý Euler*

- Nếu a, m là nguyên tố cùng nhau thì:

1. *Ví dụ vận dụng*

Ta có: m = 6, a = 5

o GCD(5, 6)=1

o Theo định lý Euler

6

- Chứng minh :

o Ta có: GCD(3, 2) = 1

o Theo TC2 ta có:

o Vì 3 và 2 là số nguyên tố nên theo TC1 ta có:

### 1.3.5. Thuật toán Miller-Rabin

Thuật toán Miller-Rabin là thuật toán kiểm tra số nguyên tố dựa trên phương pháp chứng minh theo xác suất, có độ chính xác khá cao ngay cả khi đầu vào là số Carmichael.

1. *Định lý*

Giả sử là một số nguyên tố lẻ. Gọi k, m là hai số thỏa mãn trong đó là một số lẻ. Gọi 1 ≤ ≤ . Ta có:

1. hoặc
2. Tồn tạithỏa mãn và
3. *Giải thuật kiểm tra tính nguyên tố của một số nguyên p*

Miller\_Rabin(p)

Tìm k, q với k> 0, q lẻ thỏa mãn p = 2kq + 1

Chọn số ngẫu nhiên a trong khoảng [2, p - 1]

If aq mod p = 1 Then

return "p có thể là số nguyên tố";

For j= 0 to k-1 do

If a2^j\*q mod p != 1 and a2^j\*q mod p != p - 1 Then

return "p không phải là số nguyên tố";

return "p có thể là số nguyên tố";

1. *Xác suất sai và nguyên tắc kiểm tra*

Người ta đã tính được xác suất để trong trường hợp p là hợp số, thuật toán Miller\_Rabin đưa ra khẳng định, không phải là số nguyên tố là 75%. Trong 25% còn lại, Miller\_Rabin không xác định được p là nguyên tố hay hợp số. Do đó nếu chúng ta áp dụng thuật toán t lần (mỗi lần với các giá trị a khác nhau) thì xác suất không xác định (trong cả t lần) là 0.25t. Với t = 10, xác suất trên là rất bé, nhỏ hơn 0.000001.

Tóm lại nguyên tắc kiểm tra tính nguyên tố của số nguyên p thực hiện như sau:

* Thực hiện thuật toán Miller\_Rabin 10 lần với 10 số a ngẫu nhiên khác nhau.
* Nếu cả 10 lần thuật toán cho ra kết quả “có thể là số nguyên tố”, thì ta khẳng định p là số nguyên tố.
* Chỉ cần một lần thuật toán cho ra kết quả “không phải là số nguyên tố” thì ta khẳng định p là hợp số.

1. *Ví dụ vận dụng*

p = 41 = 23 \* 5 + 1 do đó k = 3, q = 5, p-1 = 40

| a | aq mod p | a2q mod p | a4q mod p |
| --- | --- | --- | --- |
| 7 | 38 | 9 | **40** |
| 8 | 9 | **40** |  |
| 9 | 9 | **40** |  |
| 12 | 3 | 9 | **40** |
| 13 | 38 | 9 | **40** |
| 16 | **1** |  |  |
| 24 | 14 | 32 | **40** |
| 25 | **40** |  |  |
| 31 | **40** |  |  |
| 37 | **1** |  |  |

Vậy 41 là số nguyên tố.

### 1.3.6. Định lý phần dư Trung Hoa

1. *Định lý*

Cho k số nguyên dương đôi một nguyên tố cùng nhau m1, m2, …, mk và a1, a2, …, ak là k số nguyên tùy ý. Khi đó hệ phương trình đồng dư tuyến tính

có nghiệm duy nhất modulo M = m1m2…mn.

1. *Thuật toán giải hệ phương trình đồng dư tuyến tính*

Bước 1: Đặt M = m1m2…mn = Nimi với i = 1,2,3,…n

Bước 2: Tìm các nghiệm của phương trình Nix ≡ 1 (mod m)

Bước 3: Tìm được một nghiệm của hệ là:

Bước 4: Kết luận nghiệm:

1. *Ví dụ vận dụng*

Giải hệ phương trình đồng dư:

**Giải**

Ta có: M = 3×5×7 = 105

N1 = 105÷3 = 35 → 2

N2 = 105÷5 = 21 → 1

N3 = 105÷7 = 15 → 1

wps

Vậy nghiệm x có dạng:

### 1.3.7. Hệ mã hóa RSA

1. *Mô tả hoạt động*

RSA hoạt động theo các bước cơ bản như sau:

* Mỗi thực thể cần chia sẻ khoá công khai với nhau và thiết lập cặp khoá của riêng mình. Để thông tin liên lạc được đảm bảo bảo mật, hai thực thể cần giữ bí mật các chìa khoá riêng tư.
* Sau khi người gửi đã có được chìa khoá riêng tư của người nhận, họ có thể mã hoá dữ liệu mà họ muốn bảo mật bằng chìa khoá này. Tuy nhiên, khi các dữ liệu đã được mã hoá bằng khoá công khai thì chỉ có khoá riêng tư đi kèm với khoá công khai mới có thể giải mã chúng. Tất cả những điều này được hình thành do chức năng cửa bẫy.
* Khi người nhận nhận được tin nhắn đã được mã hoá, họ có thể truy cập vào dữ liệu bằng cách sử dụng khoá riêng của mình. Nếu người nhận muốn đảm bảo mức độ an toàn cho việc liên lạc thì họ có thể sử dụng khoá công khai của bên mà mình liên lạc để mã hoá tin nhắn. Và tất nhiên, cách duy nhất để đối phương truy cập được vào thông tin bị mã hoá bằng khoá công khai là sử dụng chìa khoá riêng tư phù hợp.

Bằng cách này, mã hoá RSA được sử dụng khi các bên không biết gửi dữ liệu một cách an toàn.

1. *Tạo khóa*

Bước 1: Chọn ngẫu nhiên 2 số nguyên tố lớn p và q

Bước 2: Tính số làm modulo

Bước 3: Chọn ngẫu nhiên khóa mã hóa b thỏa mãn:

Bước 4: Giải phương trình tìm khóa giải mã a

Bước 5: Khóa công khai

Khóa bí mật

1. *Mã hóa*

Sử dụng khóa

1. *Giải mã*

Sử dụng khóa

# CHƯƠNG 2: KẾT QUẢ NGHIÊN CỨU

## 2.1. Giới thiệu

- Tên đề tài nghiên cứu: Xây dựng chương trình mã hóa và giải mã RSA.

- Các bước thực hiện triển khai đề tài bao gồm:

* Nghiên cứu nội dung kiến thức.
* Tìm hiểu thuật toán.
* Thiết kế và cài đặt chương trình.

- Hình thức sản phẩm: Sản phẩm ứng dụng.

- Kết quả đạt được: Nghiên cứu, cài đặt demo thuật toán.

## 2.2. Nội dung thuật toán

Bước 1: Tạo khóa

* Chọn ngẫu nhiên 2 số nguyên tố lớn p và q
* Tính số làm modulo
* Chọn ngẫu nhiên khóa mã hóa b thỏa mãn:
* Giải phương trình tìm khóa giải mã a

Từ đó ta tạo được khóa:

Bước 2: Mã hóa

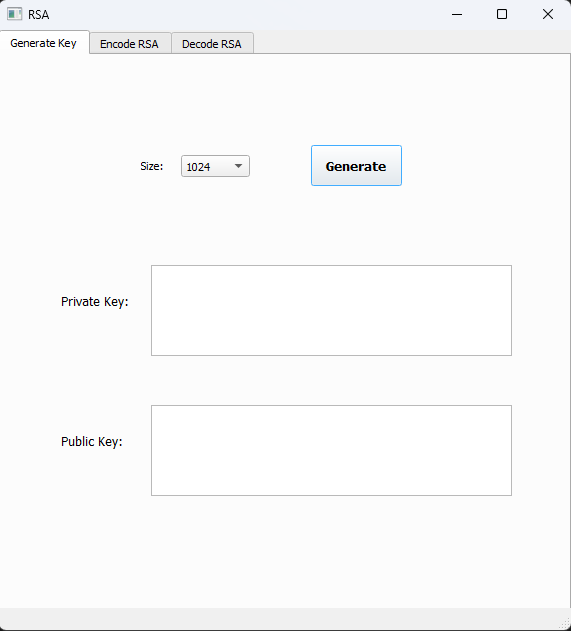
Sử dụng khóa

Bước 3: Giải mã

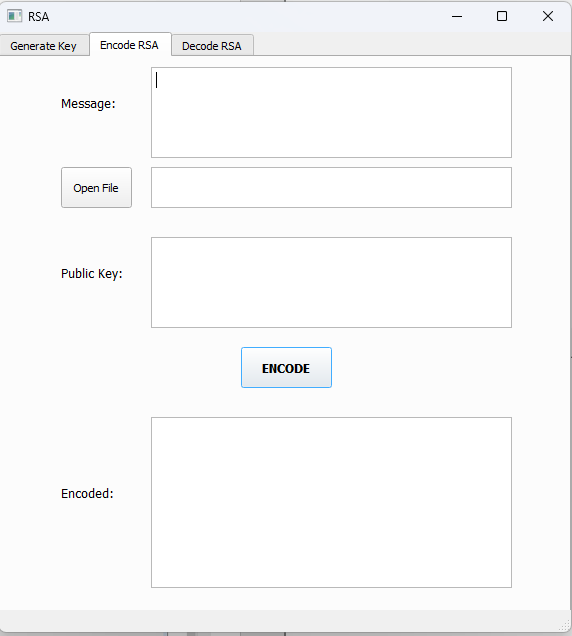
Sử dụng khóa

## 2.3. Thiết kế, cài đặt chương trình demo thuật toán

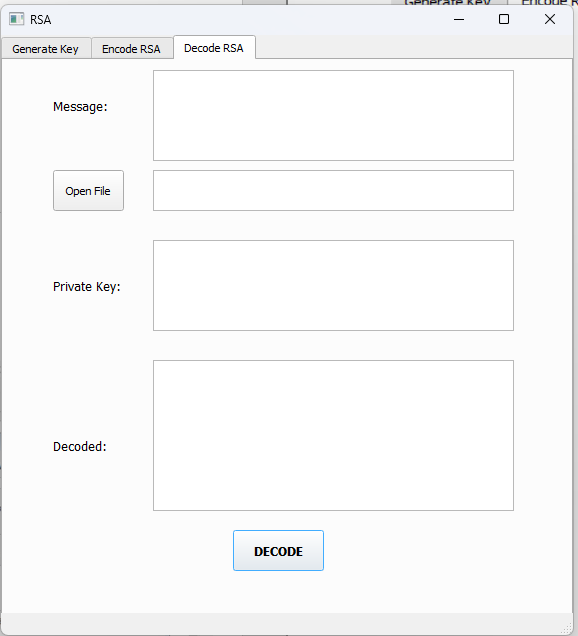
### 2.3.1. Giao diện chương trình demo theo ngôn ngữ Python



*Hình 1: Giao diện tạo khóa bằng ngôn ngữ Python*

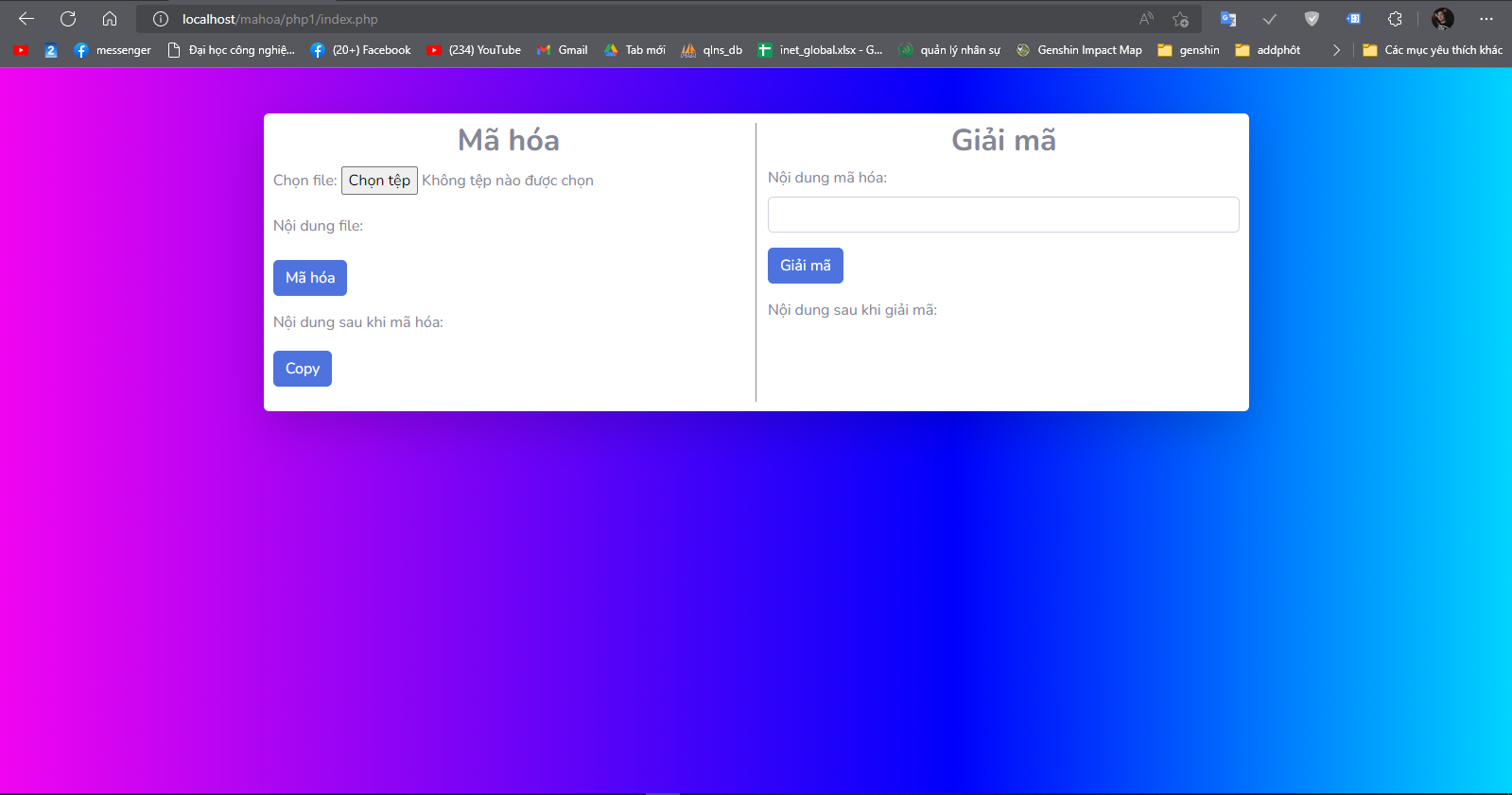


*Hình 2: Giao diện mã hóa bằng ngôn ngữ Python*



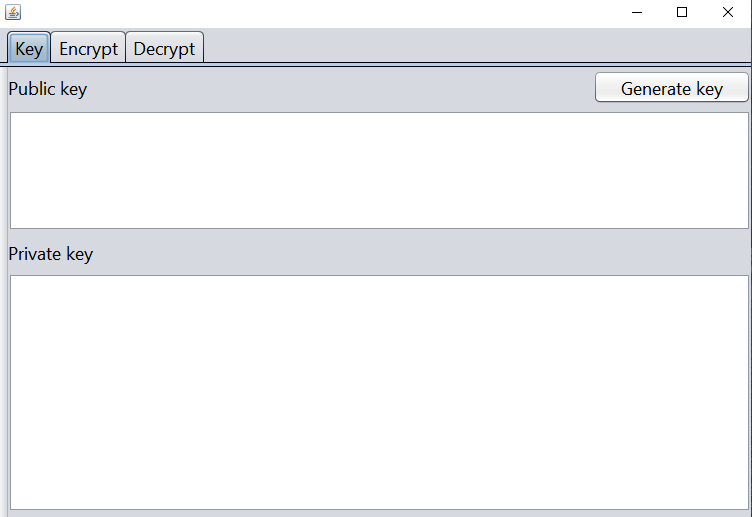
*Hình 3: Giao diện giải mã bằng ngôn ngữ Python*

### 2.3.2. Giao diện chương trình demo theo ngôn ngữ PHP

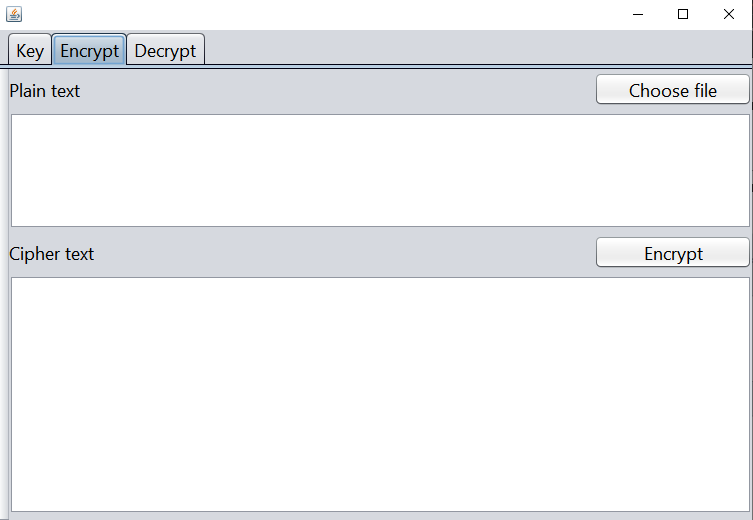


*Hình 4: Giao diện bằng ngôn ngữ PHP*

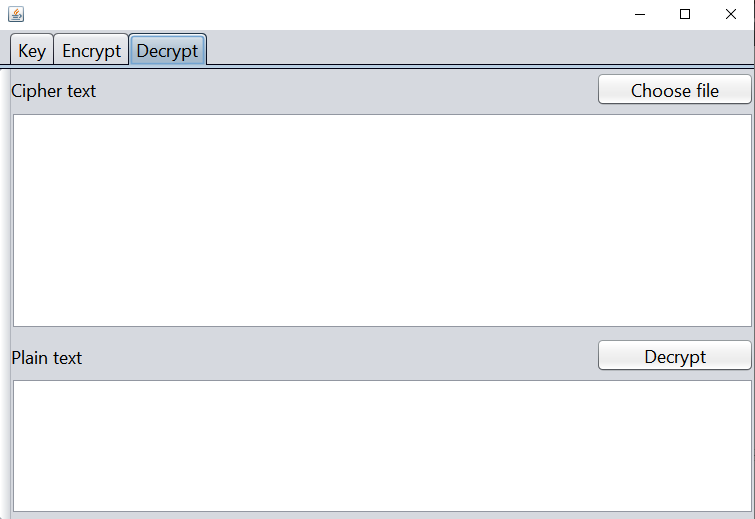
### 2.3.3. Giao diện chương trình demo theo ngôn ngữ Java



*Hình 5: Giao diện tạo khóa bằng ngôn ngữ Java*



*Hình 6: Giao diện mã hóa bằng ngôn ngữ Java*



*Hình 7: Giao diện giải mã bằng ngôn ngữ Java*

## 2.4. Cài đặt và triển khai

### 2.4.1. Giới thiệu công cụ

#### 2.4.1.1. Giới thiệu công cụ Visual Studio Code

Visual Studio Code là một trình soạn thảo mã nguồn được phát triển bởi Microsoft dành cho Windows, Linux và macOS. Nó hỗ trợ chức năng debug, đi kèm với Git, có chức năng nổi bật cú pháp, tự hoàn thành mã thông minh, snippets, và cải tiến mã nguồn.

Với giao diện đơn giản, dễ dàng tùy biến theo nhu cầu của ngôn ngữ Python giúp người dùng lập trình một cách dễ dàng ví dụ như lập trình ứng dụng bằng Python.

#### 2.4.1.2. Giới thiệu công cụ NetBeans

NetBeans là một môi trường phát triển tích hợp (IDE) cho Java. Nó cho phép các ứng dụng được phát triển từ một tập hợp các thành phần phần mềm được gọi là modules và chạy trên Windows, macOS, Linux và Solaris.

Với giao diện đơn giản, dễ sử dụng, tích hợp đầy đủ các thư viện của ngôn ngữ Java giúp người lập trình sử dụng các API một cách dễ dàng. Ngoài ra NetBeans còn hỗ trợ người lập trình dễ dàng thiết kế giao diện với thư viện Java Swing hay Java AWT.

#### 2.4.1.3. Giới thiệu công cụ máy chủ ảo XAMPP

Phần mềm XAMPP là một loại ứng dụng phần mềm khá phổ biến và thường hay được các lập trình viên sử dụng để xây dựng và phát triển các dự án website theo ngôn ngữ PHP. XAMPP được sử dụng cho mục đích nghiên cứu, phát triển website qua localhost của máy tính cá nhân. XAMPP được ứng dụng trong nhiều lĩnh vực từ học tập đến nâng cấp, thử nghiệm website của các lập trình viên.

### 2.4.2. Hướng dẫn cài đặt và chạy chương trình

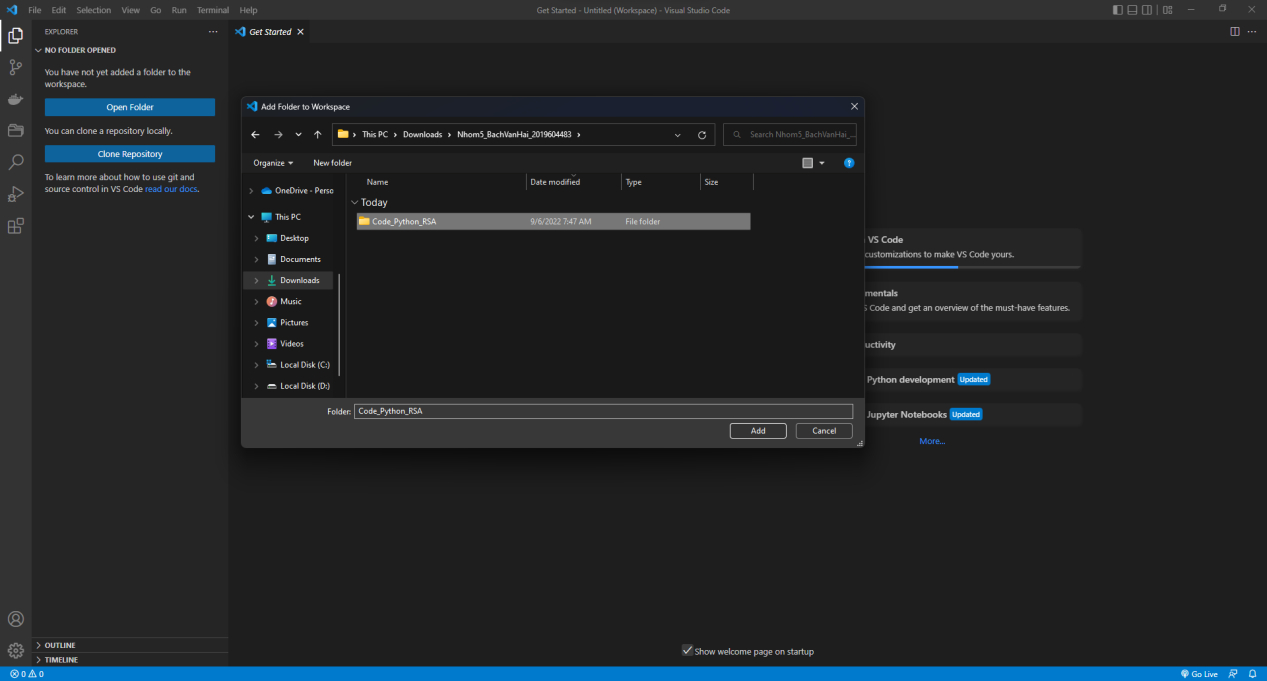
#### 2.4.2.1. Cài đặt Visual Studio Code và chạy chương trình demo

*a. Cài đặt Visual Studio Code*

* + Truy cập trang web: <https://code.visualstudio.com> và <https://www.python.org> để tải công cụ Visual Studio Code và python 3.10.4 về máy.
  + Mở file sau khi đã tải thành công.
  + Ấn theo hướng dẫn đã cài đặt của phần mềm.
  + Thiết lập biến môi trường.
  + Mở công cụ và hoàn tất cài đặt

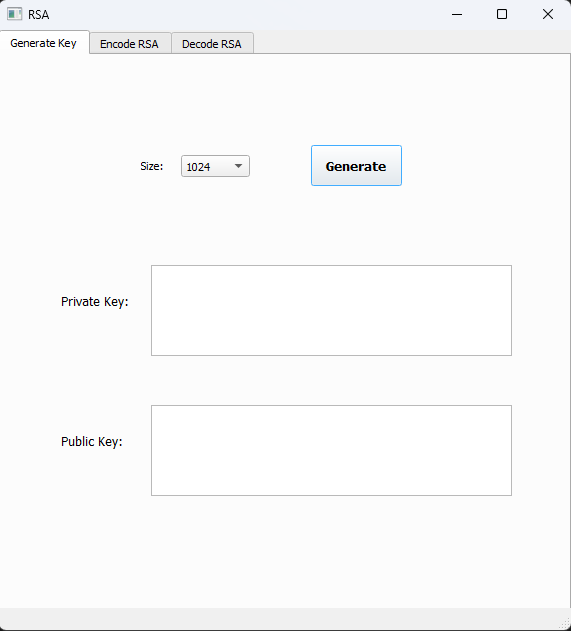
*b. Chạy chương trình demo*

* + Ở giao diện làm việc của Visual Studio Code, chọn folder có project cần chạy

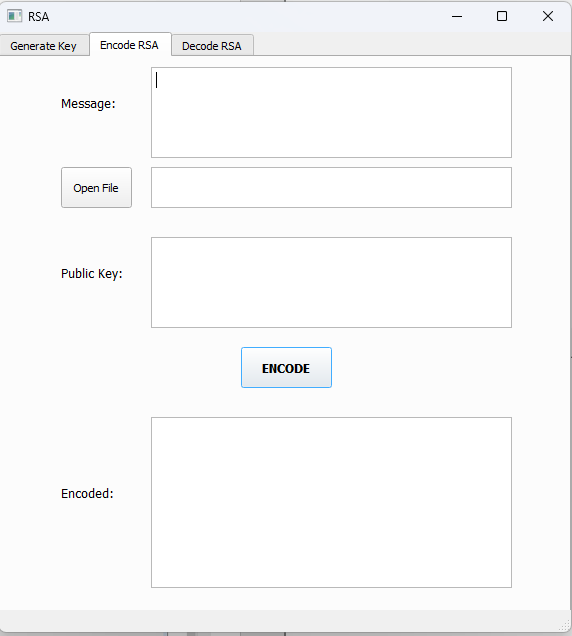


*Hình 8: Chọn project bằng công cụ Visual Studio Code*

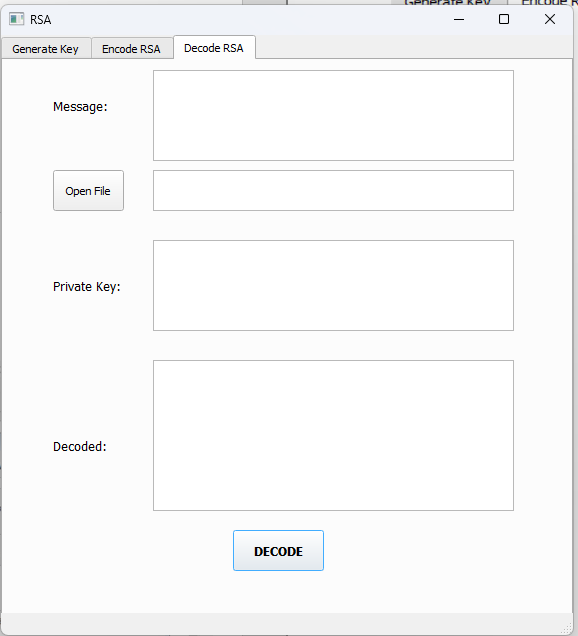
* + Click vào nút run trên thanh công cụ để chạy chương trình



*Hình 9: Giao diện tạo khóa bằng ngôn ngữ Python*

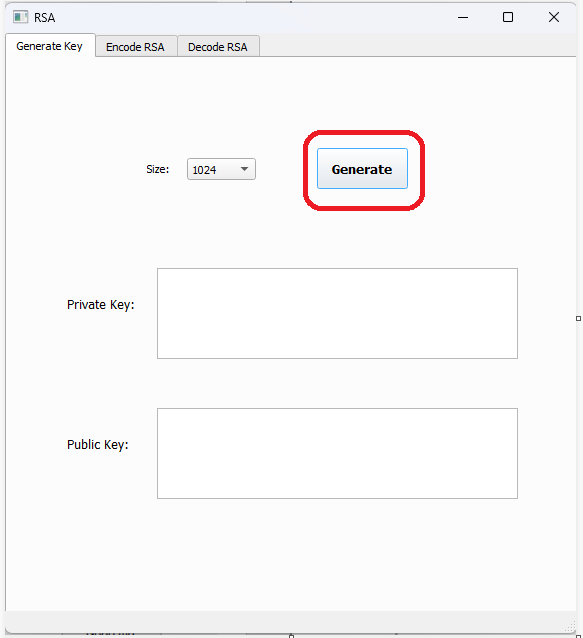


*Hình 10: Giao diện mã hóa bằng ngôn ngữ Python*



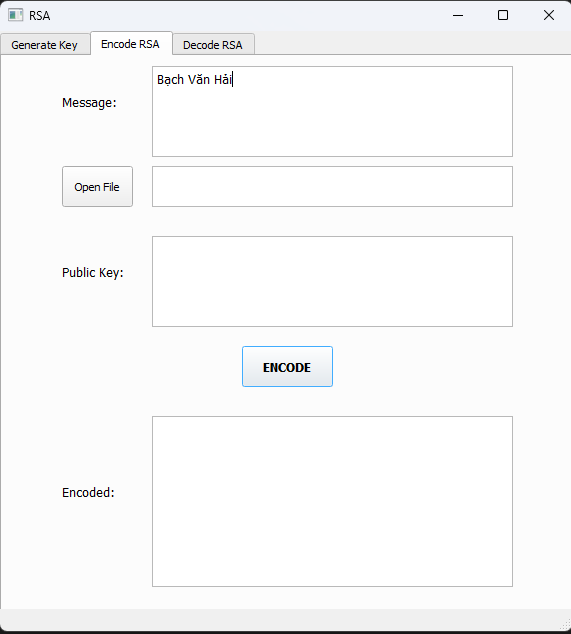
*Hình 11: Giao diện giải mã bằng ngôn ngữ Python*

* + Để sử dụng chương trình mã hóa thì người dùng nhấn nút “Generate” để chương trình tự sinh khóa:



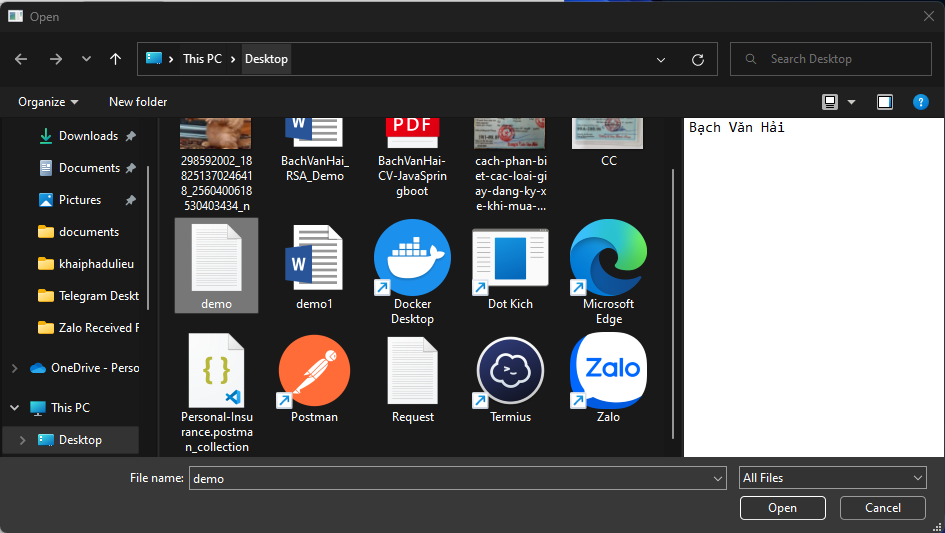
*Hình 12: Sinh khóa bằng ngôn ngữ Python*

* + Tiếp theo người dùng có thể tự nhập thông tin muốn mã hóa hoặc tải một file text hoặc file docx chứa thông tin muốn mã hóa.
    - **Cách 1: Nhập thông điệp trực tiếp vào ô text**



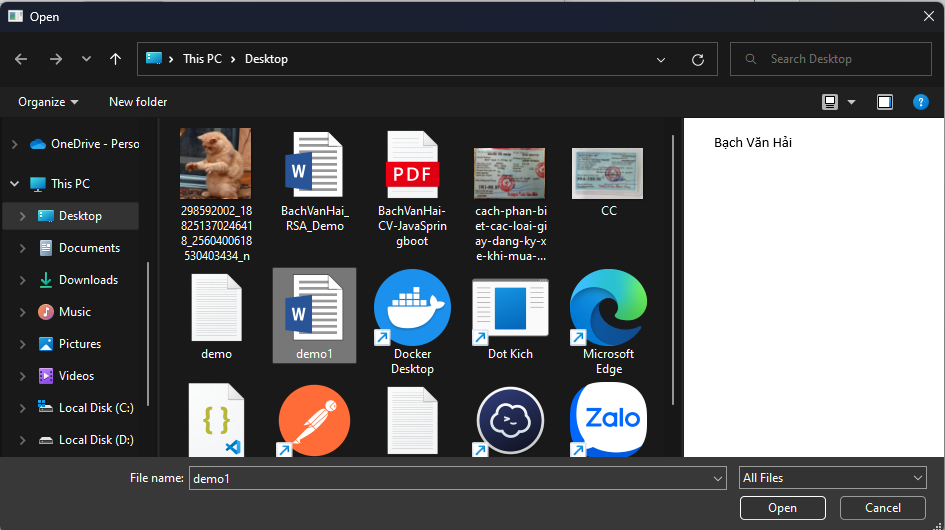
*Hình 13: Mã hóa text bằng ngôn ngữ Python*

* + - **Cách 2: chọn một file .txt rồi nhấn open**



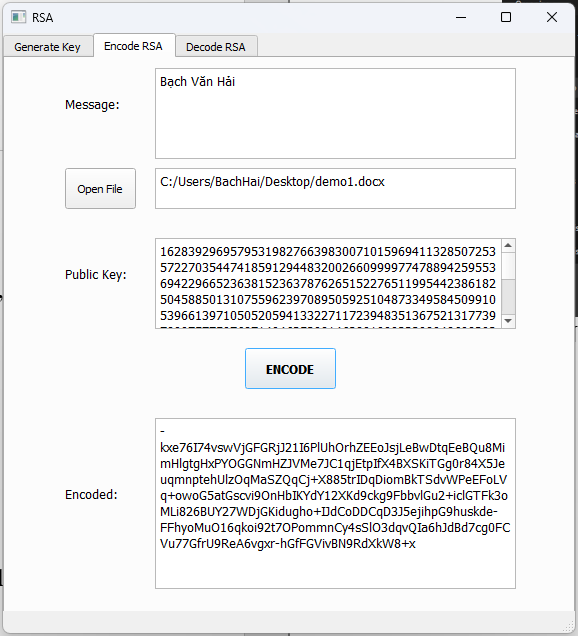
*Hình 14: Mã hóa file .txt bằng ngôn ngữ Python*

* + - **Cách 3: chọn một file .docx rồi nhấn open**



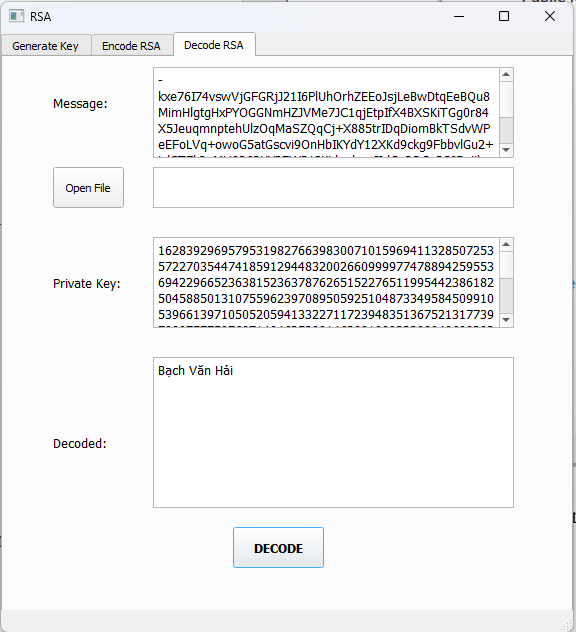
*Hình 15: Mã hóa file .docx bằng ngôn ngữ Python*

* + Nhấn nút “ENCODE” để mã hóa thông tin, ta được chuỗi mã hóa



*Hình 16: Mã hóa thông tin bằng ngôn ngữ Python*

* + Tiếp theo chọn “DECODE” để giải mã thông tin mã hóa ta được bản rõ



*Hình 17: Giải mã thông tin bằng ngôn ngữ Python*

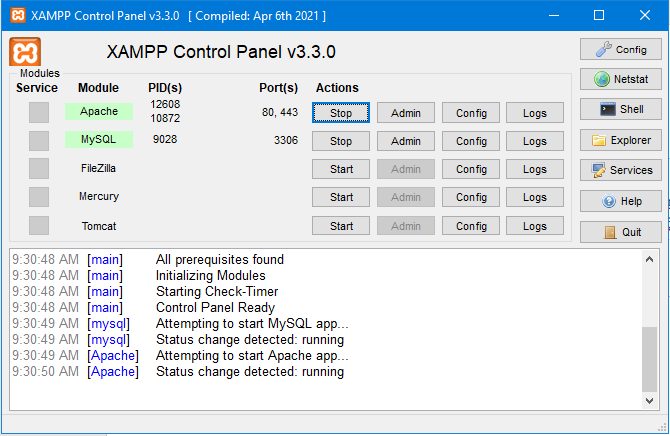
#### 2.4.2.2. Cài đặt Xampp và chạy chương trình demo

*a. Cài đặt Xampp*

* Bước 1: Tải file cài đặt xampp tại: https://www.apachefriends.org/download.html
* Bước 2: Nhấp vào file có đuôi .exe trên file tải xuống.
* Bước 3: Trên cửa sổ Set up, tích chọn các phần mềm mà bạn muốn cài đặt. Nếu bạn muốn cài WordPress trên XAMPP, các phần mềm bắt buộc phải chọn là MySQL, Apache, PHPMyAdmin. Sau khi chọn xong, nhấn Next.
* Bước 4: Chọn thư mục cài đặt và nhấn Next.
* Bước 5: Chờ vài phút để cài đặt, sau khi cài đặt hoàn tất nhấn finish để kết thúc.

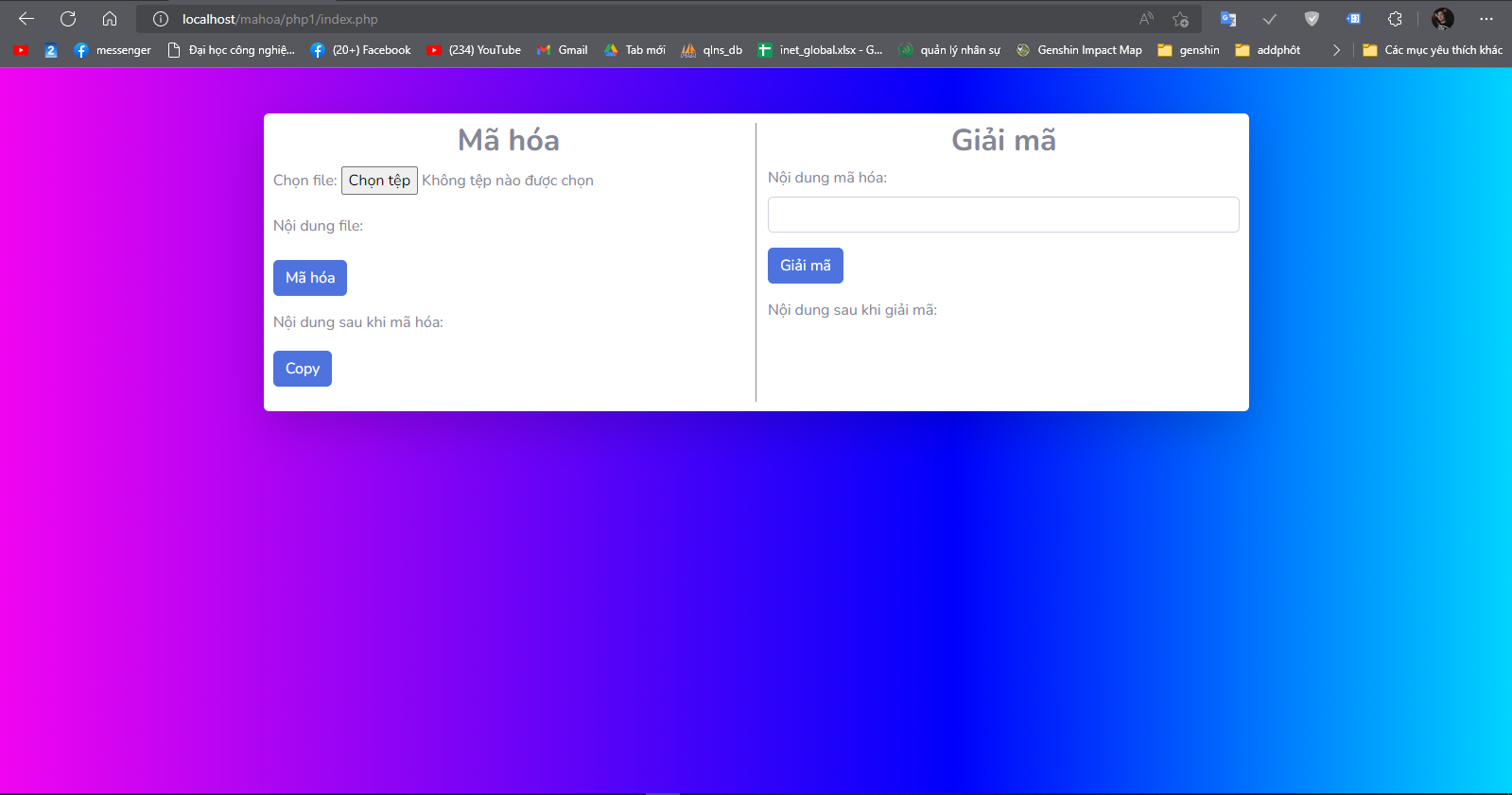
*b. Chạy chương trình demo*

- Mở xampp và click start ở 2 module Apache và MySql



*Hình 18: Công cụ Xampp*

- Mở trình duyệt và truy cập theo đường dẫn sau: localhost/thu-muc-chua-code-trong-file-htdocs-cua-xampp. Ví dụ : <http://localhost/mahoa/php1/index.php>

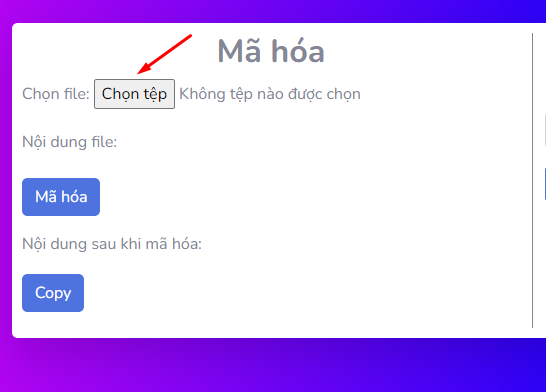


*Hình 19: Giao diện chương trình bằng ngôn ngữ PHP*

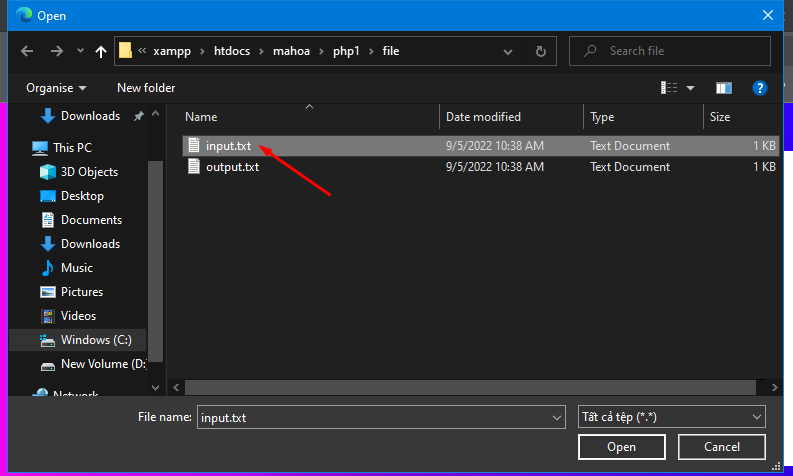
- Thực hiện mã giá và giải mã

* **Mã hóa**

- Bước 1: bấm nút chọn tệp và chọn tệp txt chứa nội dung muốn mã hóa

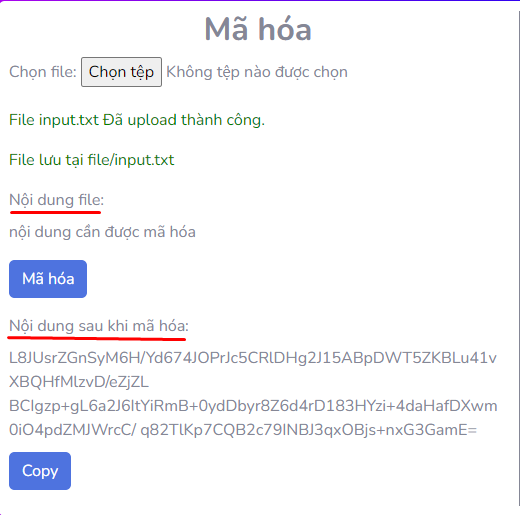


*Hình 20: Giao diện mã hóa bằng ngôn ngữ PHP*



*Hình 21: Chọn file bằng ngôn ngữ PHP*

- Tiếp theo bấm nút bấm nút “Mã hóa” để thực hiện mã hóa nội dung nội dung file được hiển thị ra ở mục nội dung file và kết quả trả về chuỗi mã hóa ở mục nội dung sau khi mã hóa:



*Hình 22: Mã hóa thông tin bằng ngôn ngữ PHP*

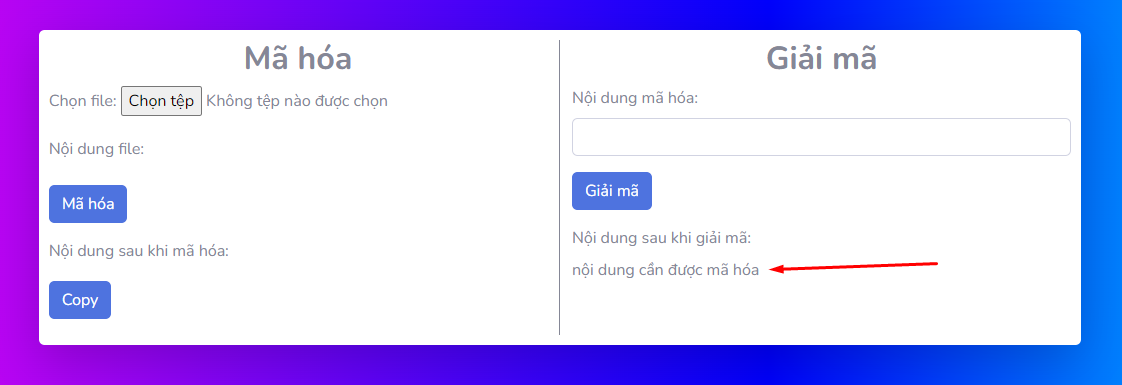
* **Giải mã**

- Nội dung sau khi mã hóa được chuyển sang ô nhập giải



*Hình 23: Giao diện giải mã bằng ngôn ngữ PHP*

- Bấm nút giải mã để giải mã nội dung mã hóa vừa được mã hóa. Ta được chuỗi ban đầu:



*Hình 24: Mã hóa thông tin bằng ngôn ngữ PHP*

#### 2.4.2.3. Cài đặt NetBeans và chạy chương trình demo

*a. Cài đặt NetBeans*

B1: Tải các file cài đặt JDK và công cụ NetBeans IDE về máy

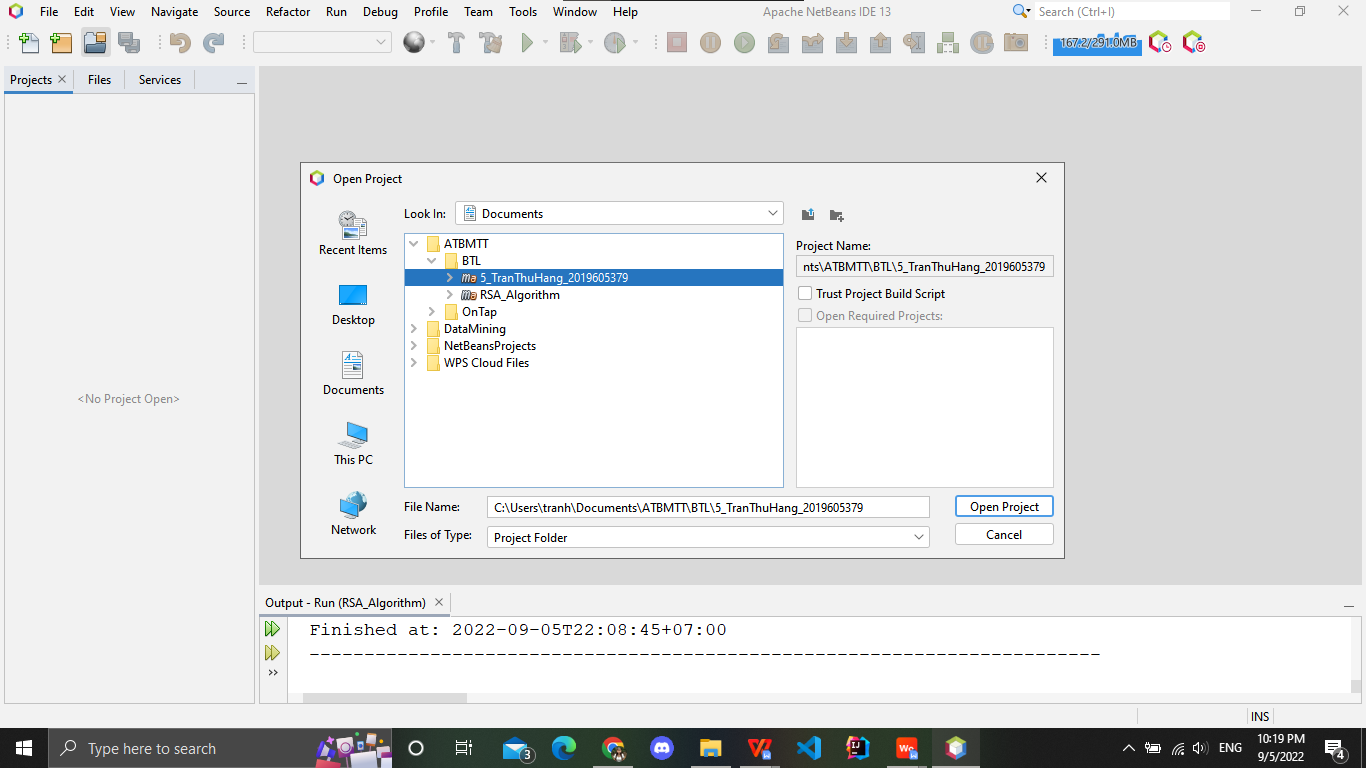
B2: Mở file vừa tải và làm theo hướng dẫn cài đặt của phần mềm

B3: Thiết lập biến môi trường

B4: Mở công cụ và hoàn tất cài đặt

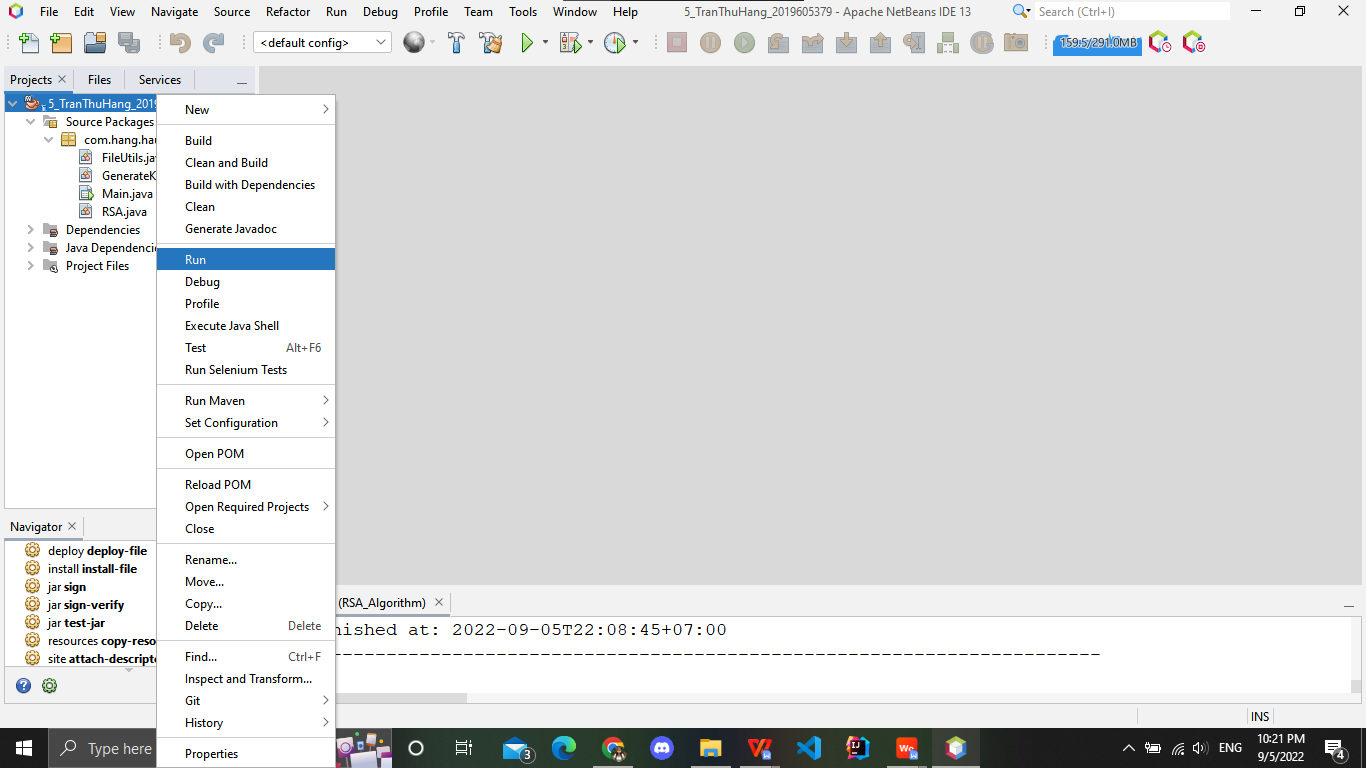
*b. Chạy chương trình demo*

B1: Mở phần mềm NetBeans, vào file chọn open project rồi lựa chọn project cần chạy.



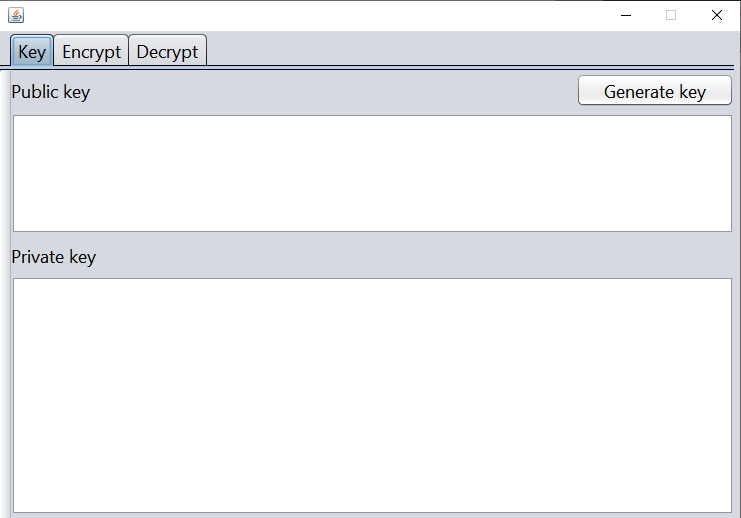
*Hình 25: Mở project bằng công cụ NetBeans*

B2: Nhấn chuột phải vào tên project vừa mở, chọn run.



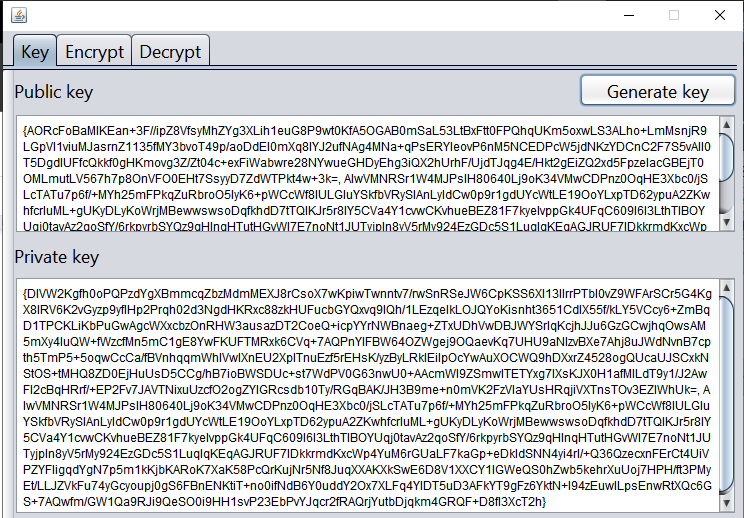
*Hình 26: Chạy project*

B3: Chương trình chạy thành công sẽ hiển thị giao diện:



*Hình 27: Giao diện chương trình bằng ngôn ngữ Java*

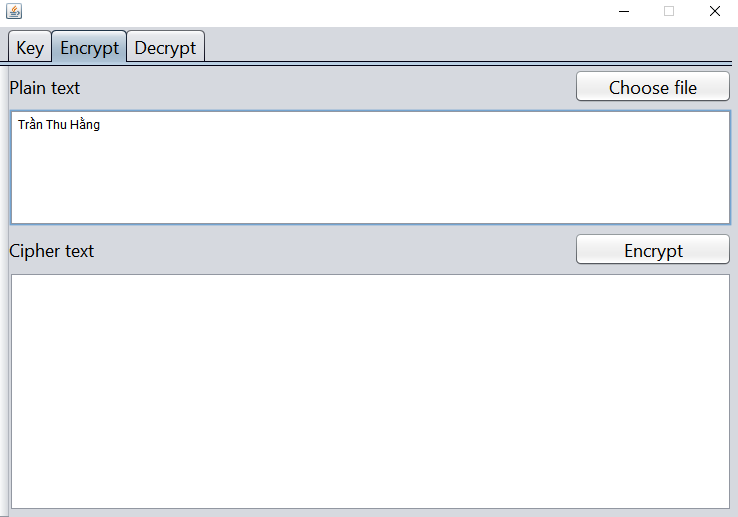
B4: Để sử dụng chương trình, click nút “Generate key” để chương trình tự tạo khóa:



*Hình 28: Tạo khóa bằng ngôn ngữ Java*

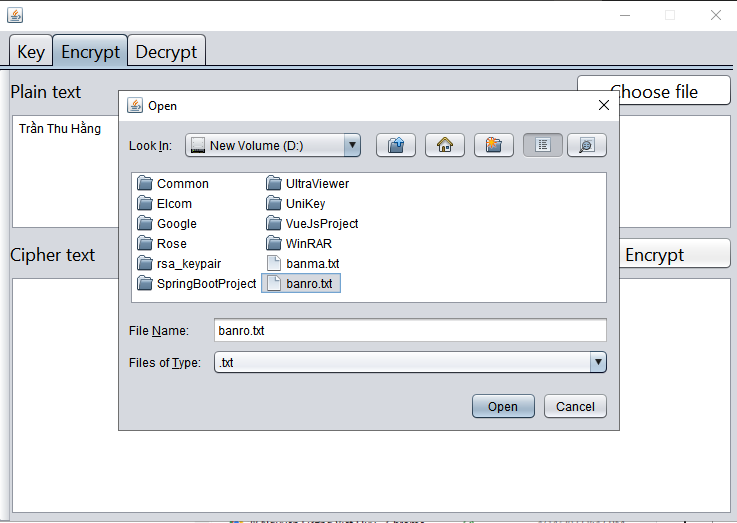
B5: Nhập thông tin mã hóa

* Cách 1: Nhập thông tin trực tiếp



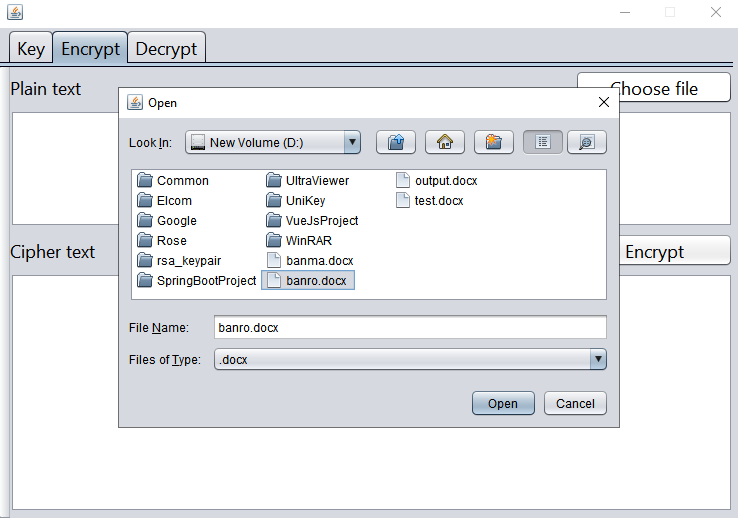
*Hình 29: Nhập thông tin mã hóa bằng ngôn ngữ Java*

* Cách 2: Chọn 1 file .txt



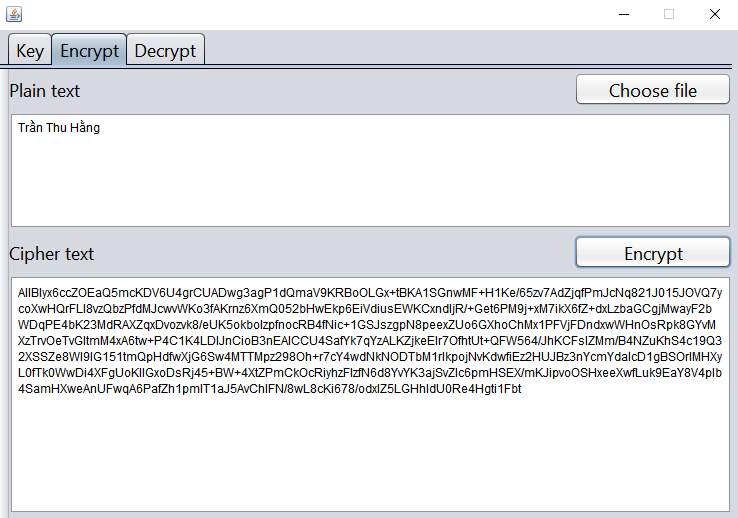
*Hình 30: Nhập file .txt bằng ngôn ngữ Java*

* Cách 3: Chọn 1 file .docx



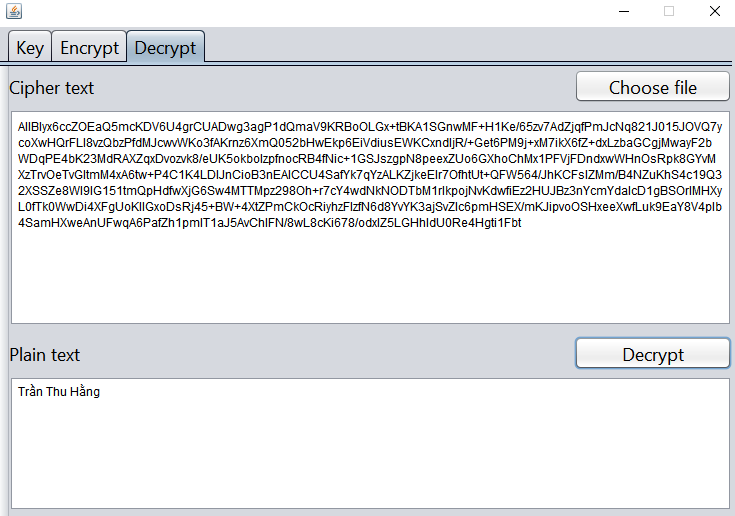
*Hình 31: Nhập file .docx bằng ngôn ngữ Java*

B6: Click nút “Encrypt” để mã hóa thông tin



*Hình 32: Mã hóa thông tin bằng ngôn ngữ Java*

B7: Click nút “Decrypt” để giải mã thông tin



*Hình 33: Giải mã thông tin bằng ngôn ngữ Java*

## 2.5. Thực hiện bài toán

### 2.5.1. Phân công công việc

| **Tên sinh viên** | **Tên công việc** |
| --- | --- |
| Bạch Văn Hải | - Tìm hiểu hệ mã hóa RSA  - Nghiên cứu thuật toán Miller-Rabin  - Cài đặt các chức năng:   * Tạo khóa * Mã hóa * Giải mã |
| Nguyễn Chí Hải | - Tìm hiểu hệ mã hóa RSA  - Nghiên cứu thuật toán Euclid, định lý Fermat, hàm số Euler  - Cài đặt các chức năng:   * Mã hóa * Giải mã |
| Trần Thu Hằng | - Tìm hiểu hệ mã hóa RSA  - Nghiên cứu định lý phần dư Trung Hoa  - Viết báo cáo  - Cài đặt các chức năng:   * Tạo khóa * Mã hóa * Giải mã |

### 2.5.2. Bạch Văn Hải - Tìm hiểu thuật toán Miller-Rabin và cài đặt chương trình demo

- Tìm hiểu thuật toán Miller-Rabin.

- Viết chương trình demo với ngôn ngữ Python.

### 2.5.3. Nguyễn Chí Hải - Tìm hiểu thuật toán Euclid, định lý Fermat, hàm số Euler và cài đặt chương trình demo

- Tìm hiểu thuật toán Euclid, định lý Fermat, hàm số Euler.

- Viết chương trình demo với ngôn ngữ PHP.

### 2.5.4. Trần Thu Hằng - Tìm hiểu định lý phần dư Trung Hoa và cài đặt chương trình demo

- Tìm hiểu định lý, thuật toán và ví dụ về định lý phần dư Trung Hoa.

- Viết chương trình demo với ngôn ngữ Java.

# CHƯƠNG 3: KIẾN THỨC LĨNH HỘI VÀ BÀI HỌC KINH NGHIỆM

## 3.1. Nội dung đã thực hiện

### 3.1.1. Các kiến thức đã lĩnh hội

* Thuật toán Euclid
* Định lý Fermat
* Hàm số Euler
* Thuật toán Miller-Rabin
* Định lý phần dư Trung Hoa
* Hệ mã khóa công khai RSA
* Thuật toán hình thành tham số và khóa
* Cơ sở lý thuyết xây dựng hệ mật mã RSA
* Quá trình tạo khóa
* Quá trình mã hóa
* Quá trình giải mã
* Tính đúng đắn của hệ mật mã RSA
* Ưu và nhược điểm của hệ mật mã RSA
* Độ an toàn của hệ mật mã RSA

### 3.1.2. Các kỹ năng đã tiếp thu

* Đánh giá được vai trò của bảo mật thông tin, các cơ chế, chính sách bảo mật, các kiểu tấn công và phương pháp phòng chống.
* Phân tích được các kỹ thuật sử dụng để mã hóa và xác thực thông tin.
* Hiểu và áp dụng các thuật toán liên quan đến hệ mã hóa RSA như (thuật toán sinh khóa, thuật toán mã hóa, thuật toán giải mã cùng với các thuật toán liên quan như thuật toán nghịch đảo của phép nhân modulo hay thuật toán bình phương và nhân trong modulo) vào việc mã hóa và giải mã để giải quyết bài toán có tính ứng dụng vào thực tiễn.
* Tổ chức được hoạt động nhóm.
* Áp dụng được các phương pháp thuyết trình hiệu quả trong công việc.
* Bên cạnh đó còn có kỹ năng quản lý thời gian hiệu quả, kỹ năng viết báo cáo, thành thạo các công cụ trong bộ office…

### 3.1.3. Bài học kinh nghiệm

* Các tài liệu quan trọng và chính thống liên quan đến hệ mật mã RSA chủ yếu được viết bằng tiếng anh nên các thành viên trong nhóm phải trau rồi khả năng ngoại ngữ để có thể đọc hiểu được một số tài liệu liên quan đến hệ mã hóa RSA và công cụ, ngôn ngữ lập trình.
* Trong quá trình thực hiện viết chương trình các thành viên trong nhóm gặp rất nhiều vấn đề về việc mã hóa và giải mã thông qua file, đặc biệt là lấy bản rõ bằng cách open file docx. Do đó các thành viên trong nhóm đã đúc kết được kinh nghiệm về việc xử lý file và hiểu được trách nhiệm phải quan tâm nhiều hơn đến dữ liệu người dùng nhập vào, người dùng có thể nhập bản rõ vào phần mềm bằng nhiều cách khác nhau và phải xử lý để các dữ liệu đó hoạt động thật mượt mà và trơn tru.

## 3.2. Hướng phát triển

### 3.2.1. Tính khả thi của chủ đề nghiên cứu

Chủ đề nghiên cứu của nhóm chúng em khá phù hợp với thời gian được cho phép để hoàn thiện bài tập lớn, bên cạnh đó các thuật toán và mã hóa đều đã có sẵn được thử nghiệm bởi các nhà nghiên cứu bảo mật nên trong thời gian nghiên cứu, nhóm nhận thấy cần phải thực sự hiểu rõ về hệ mật mã RSA và có kỹ thuật lập trình ở mức khá là đã có thể hoàn thiện đề tài nghiên cứu.

### 3.2.2. Những thuận lợi, khó khăn

- Thuận lợi:

* Do đã có kiến thức lập trình từ năm học trước nên vấn đề về phân chia ngôn ngữ lập trình cho các thành viên trong nhóm khá dễ dàng, và việc chuyển từ ngôn ngữ sở trường sang các ngôn ngữ khác đều không gặp nhiều vấn đề.
* Có thể đọc hiểu được tài liệu tiếng anh nên có thể dễ dàng tiếp cận các nguồn tài liệu chính thống.
* Các thuật toán đã có sẵn, chỉ cần áp dụng một chút kỹ thuật xử lý về Form, File là đã có thể hoàn thành bài toán của đề tài.
* Các thành viên trong nhóm hòa đồng, cởi mở, tương tác với các thành viên khác trong nhóm khá sôi nổi nên các công việc liên quan đến cả nhóm thường diễn ra khá suôn sẻ.

- Khó khăn:

* Công đoạn thiết giao diện phần mềm mã hóa chưa được bắt mắt do chưa có nhiều kinh nghiệm trong kỹ thuật xử lý giao diện.
* Ở phần xử lý về File Docx sử dụng để lấy bản rõ khá mới mẻ với các thành viên trong nhóm nên giai đoạn hoàn thiện chức năng tốn khá nhiều thời gian.

### 3.2.3. Hướng phát triển và mở rộng của đề tài

Nhận thấy việc sử dụng hệ mật mã RSA vô cùng hữu ích trong việc bảo mật thông tin, tuy nhiên sản phẩm của nhóm chỉ có thể mã hóa 1 thông điệp 1 lúc và chỉ 1 thông điệp từ 1 người gửi đến cho 1 người nên khá bất tiện trong nhiều trường hợp. Cho nên nhóm có đề xuất hướng phát triển là sẽ xây dựng thêm chức năng nhập file excel để có thể nhập nhiều bản rõ cùng một lúc và mã hóa cùng lúc. Điều này sẽ rất thuận tiện trong nhiều trường hợp trong thực tế.

# KẾT LUẬN

Sau thời gian tìm hiểu và nghiên cứu, nhóm chúng em đã xây dựng thành công chương trình “Mã hóa và giải mã RSA”. Đây là một trong những hệ mã hóa phổ biến ở Việt Nam cũng như trên thế giới. Vì lý do đó, nhóm đã lựa chọn đề tài với mong muốn góp phần đưa ra các giải pháp hữu ích có thể ứng dụng vào thực tế.

Trong quá trình thực hiện đề tài, chúng em đã gặp không ít khó khăn vì đề tài đòi hỏi nhiều kiến thức chuyên ngành, các thành viên chưa có nhiều kinh nghiệm trong việc xây dựng ứng dụng nên việc tìm hiểu, nghiên cứu và xây dựng còn chậm. Ngoài ra, do lịch học khác nhau nên các thành viên gặp khó khăn khi muốn liên lạc và trao đổi công việc. Tuy nhiên nhờ việc thu thập được nhiều tài liệu để tìm hiểu và nghiên cứu cũng như nhận được sự góp ý, hướng dẫn nhiệt tình của giảng viên, chúng em đã có thể hoàn thành tốt nhất bài báo cáo này.

Qua quá trình học tập và làm việc cùng nhau, chúng em đã trau dồi thêm những kiến thức về thuật toán Euclid, định lý Fermat, hàm số Euler, thuật toán Miller-Rabin, định lý phần dư Trung Hoa… Bên cạnh đó, các thành viên cũng có cơ hội rèn luyện các kỹ năng mềm như kỹ năng làm việc nhóm, kỹ năng giao tiếp, kỹ năng quản lý thời gian hiệu quả, sử dụng thành thạo các công cụ hỗ trợ như word, powerpoint, Visual Studio Code… Đây chắc chắn sẽ là những bài học quý báu, hành trang bổ ích để chúng em có thể tự tin vững bước trên con đường lập nghiệp và thành công trong cuộc sống sau này.

Tuy nhiên, do kiến thức còn hạn hẹp nên chương trình còn đơn giản và chưa thật sự tối ưu.

Trong tương lai, nhóm sẽ tiếp tục tích lũy kinh nghiệm và kiến thức để phát triển hoàn thiện chương trình này hơn nữa và có thể sẽ áp dụng nó trong thực tế cuộc sống.

# TÀI LIỆU THAM KHẢO

| [1] | V. Phạm, "Bizflycloud," 06 05 2022. [Online]. Available: https://bizflycloud.vn/tin-tuc/rsa-la-gi-20220506153312797.htm. |
| --- | --- |
| [2] | "Wikipedia," [Online]. Available: https://vi.wikipedia.org/wiki/RSA\_(m%C3%A3\_h%C3%B3a). |
| [3] | N. V. Q. E, "Viblo," 23 7 2021. [Online]. Available: https://viblo.asia/p/co-che-hoat-dong-va-ung-dung-cua-rsa-eW65G4XOKDO. |
| [4] | T. A. Vu, "Viblo," 6 8 2017. [Online]. Available: https://viblo.asia/p/java-ma-hoa-va-giai-ma-voi-thuat-toan-rsa-bJzKmW3Xl9N. |