BÁO CÁO THỰC HÀNH

**Bài thực hành số 02**

**MÃ HÓA KHOÁ CÔNG HAI**

|  |  |
| --- | --- |
| **Môn học:** An toàn Mạng máy tính | **Điểm tự đánh giá** |
| **Lớp:** NT101.N11.1  **Giảng viên hướng dẫn:** Văn Thiên Luân | **10** |

**PHÂN CÔNG NHIỆM VỤ NHÓM 1:**

|  |  |  |
| --- | --- | --- |
| **MSSV** | **Họ và Tên** | **Nhiệm vụ** |
| 20521086 | Trang Kỳ Anh | - Đảm nhiệm nội dung thực hành bài 1 (số nguyên tố, benmark) và bài 2.  - Góp ý, nhận xét các bài còn lại cho các thành viên khác.  - Tổng hợp viết báo cáo. |
| 20521280 | Lê Thanh Hằng | - Đảm nhiệm nội dung thực hành bài 1 (a^x mod p) và bài 3.2  - Góp ý, nhận xét các bài còn lại cho các thành viên khác. |
| 20520131 | Dương Đức Anh | - Đảm nhiệm nội dung thực hành và báo cáo bài 1 (random, GCD)  - Góp ý, nhận xét các bài còn lại cho các thành viên khác. |

**ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| Tổng thời gian thực hiện | 100 tiếng |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất, kiến nghị | - Bài dài, tốn nhiều thời gian, thuật toán khó  - Bài thực hành viết bằng tiếng anh gây một chút khó khăn trong việc đọc – hiểu một số thuật từ. |

**MỤC LỤC**

[I. BÁO CÁO CHI TIẾT 3](#_Toc118326085)

[**1.** **Lý thuyết số học** 3](#_Toc118326086)

[*a.* *Mô tả hàm* 3](#_Toc118326087)

[*b.* *Chạy thử và đánh giá* 9](#_Toc118326088)

[**2.** **Mã hóa khóa công khai RSA** 12](#_Toc118326089)

[*a.* *Mô tả thuật toán* 12](#_Toc118326090)

[*b.* *Kiểm thử chương trình* 12](#_Toc118326091)

[**3.** **Ứng dụng chat có bảo mật** 14](#_Toc118326092)

[*a.* *Mô tả hoạt động của ứng dụng chat có mã hóa bằng RSA* 14](#_Toc118326093)

[*b.* *Một số đoạn code quan trọng* 16](#_Toc118326094)

[II. TÀI LIỆU THAM KHẢO 19](#_Toc118326095)

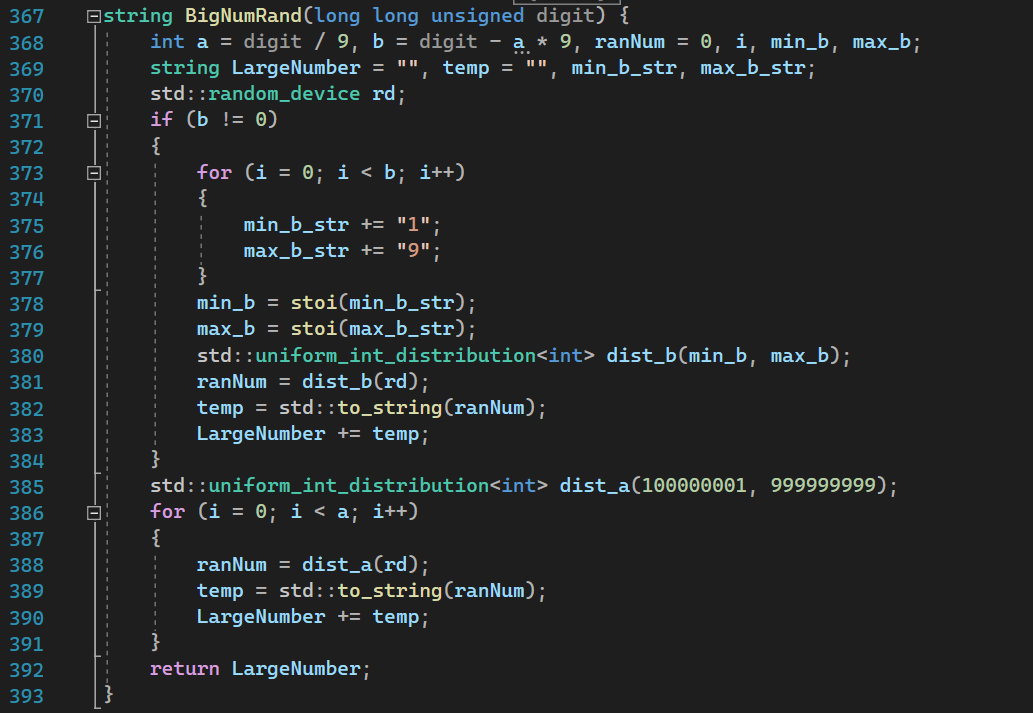
1. **BÁO CÁO CHI TIẾT**
2. **Lý thuyết số học**

Ngôn ngữ: C++

Thư viện ngôn ngữ:

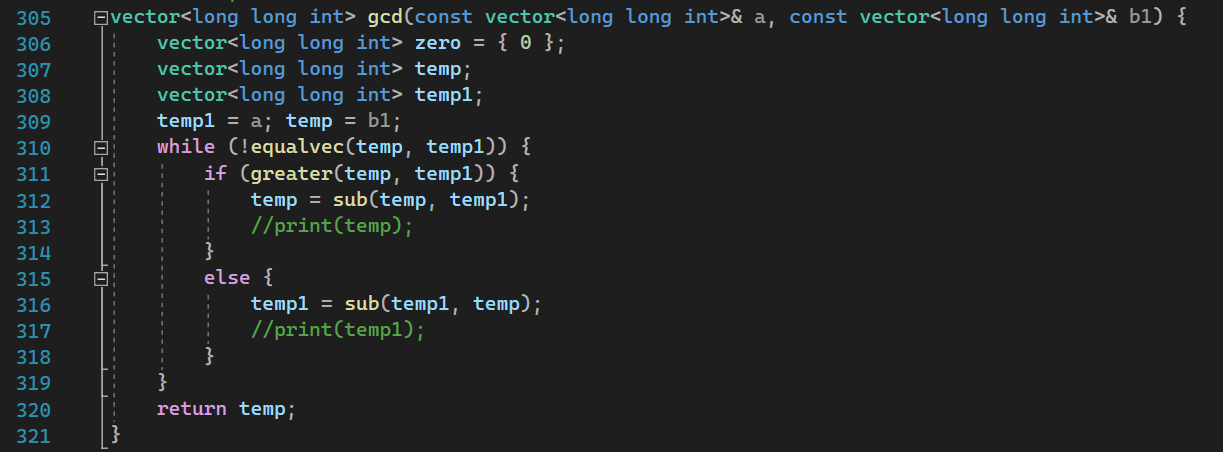
* string: tương tác với chuỗi
* math.h: sử dụng các phép tính số học
* ctime: theo dõi thời gian thực thi
* vector: tương tác với số lớn
* random: tạo ngẫu nhiên các số nhỏ

1. *Mô tả hàm*
2. Tạo ngẫu nhiên một số nguyên lớn

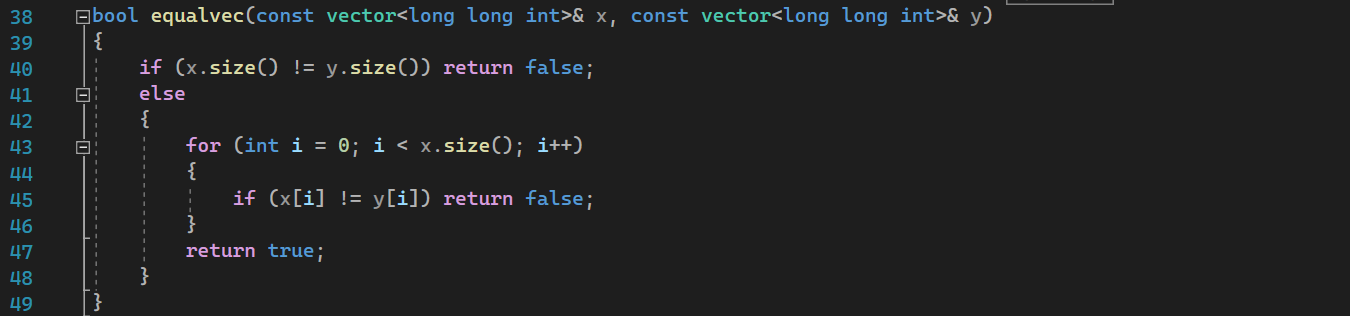


* Tạo ngẫu nhiên một dãy số có 9 chữ số từ 100000001 đến 999999999
* Ghép các dãy số lại với nhau cho đến khi được độ dài đã truyền vào trước đó
* Trả về dãy số đã được ghép, ta sẽ được một số nguyên lớn

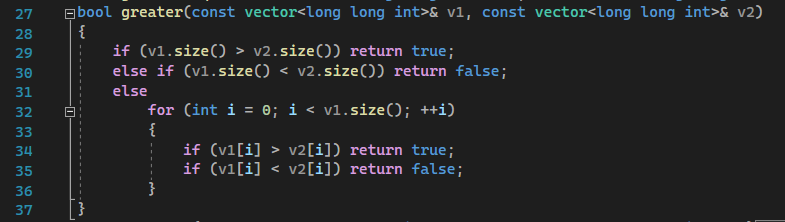
1. Tính GCD của 2 số nguyên lớn

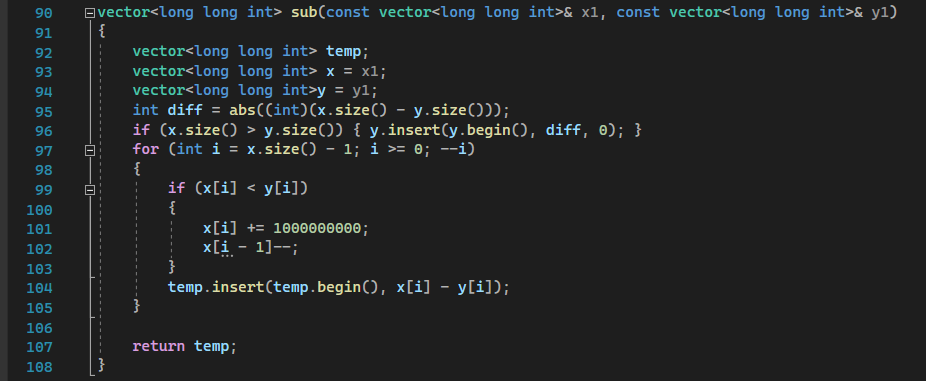


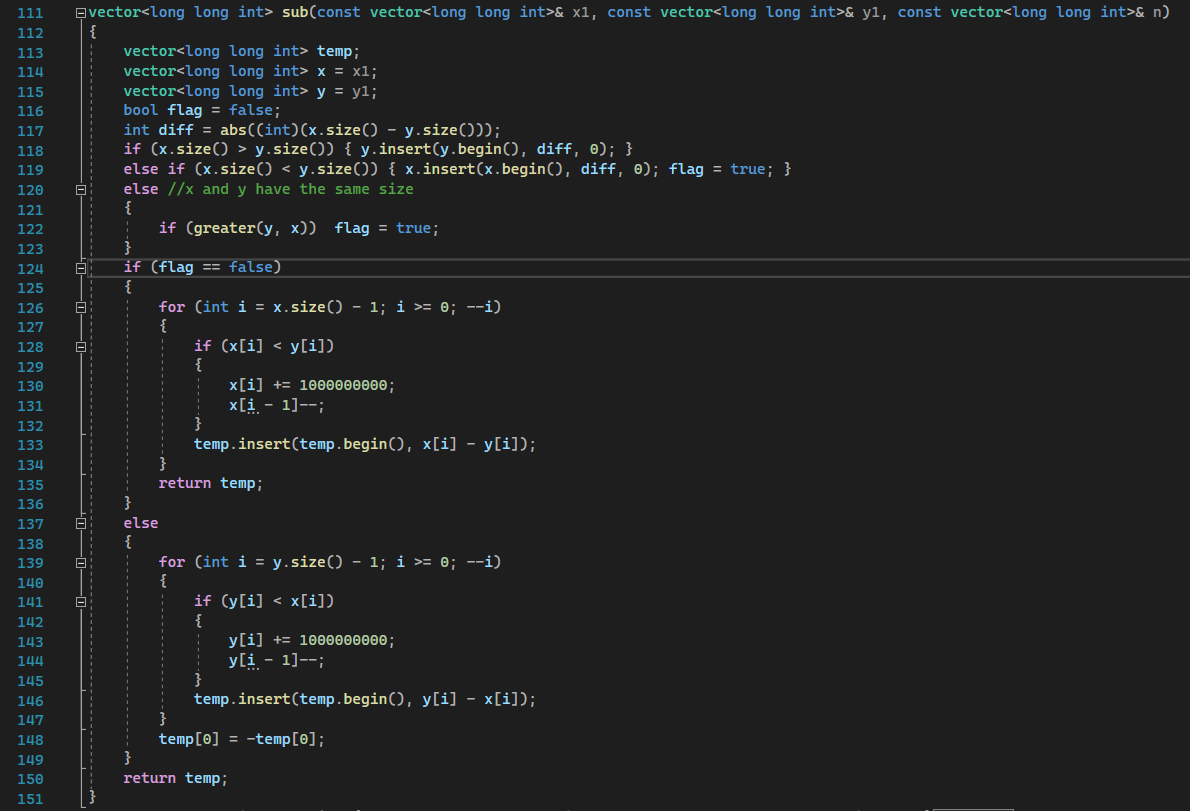
* Truyền vài 2 số nguyên lớn bằng cách tạo ngẫu nhiên từ hàm trên
* Tạo 2 biến khác và gán giá trị đã truyền vào ở trên vào 2 biến vừa tạo
* So sánh 2 số có khác nhau không bằng hàm **equalvec** và thêm **!** trước hàm đó



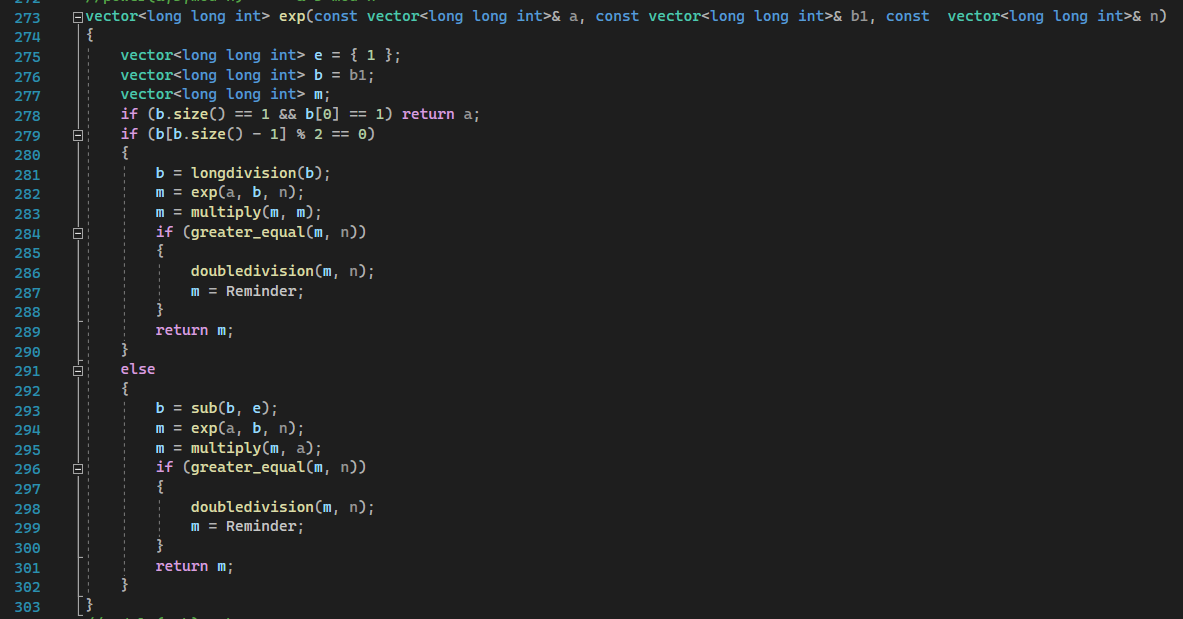
* So sánh 2 số với nhau bằng hàm **greater**, số nào lớn hơn sẽ lấy số đó trừ cho số còn lại (dùng hàm **sub**) cho đến khi nào chúng bằng nhau thì trả về giá trị đó.







1. Tinh a^x mod p voi x > 80



* Tính a mũ b bằng hàm longdivision(b) và gọi đệ quy thực hiện hàm longdivision(b) nhiều lần và sau đó gán cho biến m.
* Sau đó tính mod bằng cách dùng các hàm longdivision, exp, multiply, greater\_equal, doubledivision

Text

Description automatically generated

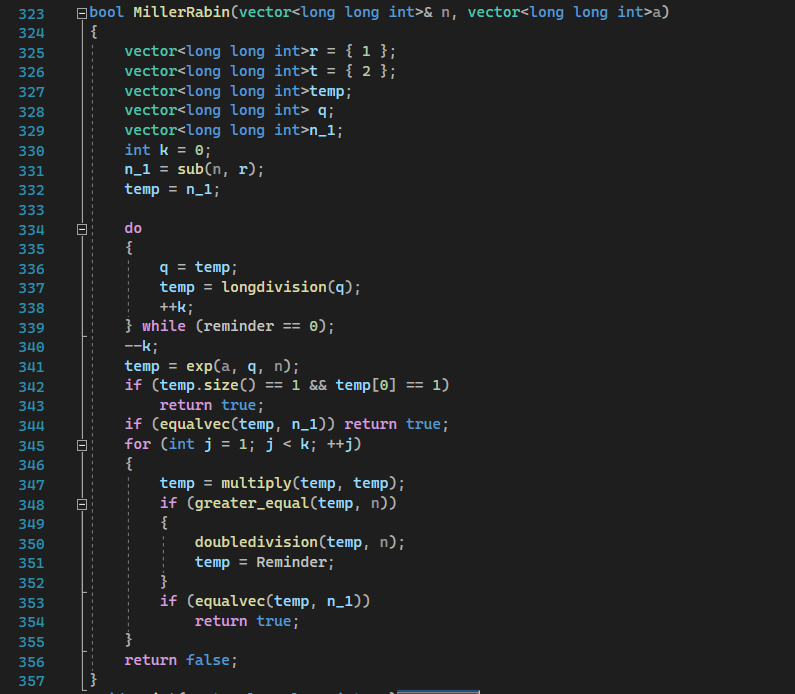
Text

Description automatically generated

Text

Description automatically generated

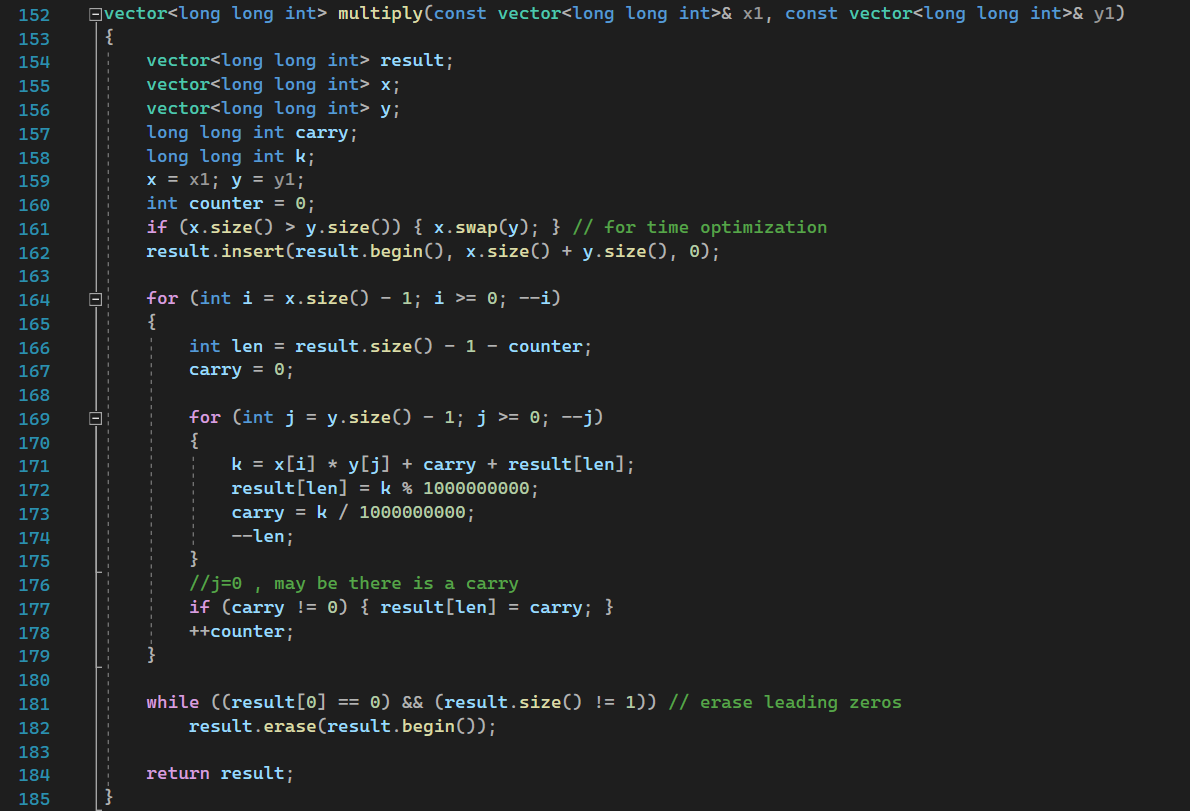
1. Thuật toán MillerRabin



* Phân tích n−1 thành dạng 2x×d
* Thử lần lượt các số a trong bảng sau:

|  |  |
| --- | --- |
| Giới hạn của n | Các số a cần dùng |
| n < 2,047 | 2 |
| n < 1,373,653 | 2, 3 |
| n < 9,080,191 | 31, 73 |
| n < 4,759,123,141 | 2, 7, 61 |
| n < 1,122,004,669,633 | 2, 13, 23, 1662803 |
| n < 2,152,302,898,747 | 2, 3, 5, 7, 11 |
| n < 3,474,749,660,383 | 2, 3, 5, 7, 11, 13 |
| n < 341,550,071,728,321 | 2, 3, 5, 7, 11, 13, 17 |
| n < 3,825,123,056,546,413,051 | 2, 3, 5, 7, 11, 13, 17, 19, 23 |
| n < 318,665,857,834,031,151,167,461 | 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37 |
| n < 3,317,044,064,679,887,385,961,981 | 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41 |

* Sau đó tiếp tục kiểm tra xem số truyền vào có phải số nguyên tố không bằng các hàm **equalvec, multiply, greater\_equal, doubledividision**.



A screenshot of a computer

Description automatically generated with medium confidence

1. *Chạy thử và đánh giá*
2. Tạo ngẫu nhiên một số nguyên lớn

* Có thể chạy không giới hạn, nhưng đối với chuỗi số gồm 500 chữ số thì thời giant trung bình ẽ vào khoảng 0.002 giây.

A screenshot of a computer

Description automatically generated with medium confidence

Text

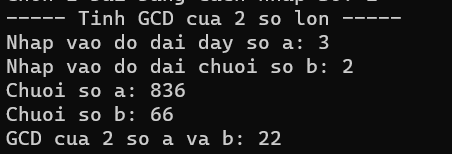
Description automatically generated

Text

Description automatically generated

1. Tính GCD của 2 số lớn

* Ta sẽ kiểm tra tính đúng đắn với số nhỏ trước



Text

Description automatically generated

* Đối với các số có cùng độ dài thì sẽ tốn tầm 0.15 giây

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

* Đối với các số có sự chênh lệch lớn hơn sẽ tốn nhiều thời gian hơn, tùy vào độ chênh lệch của các số.

1. Tính ax mod p

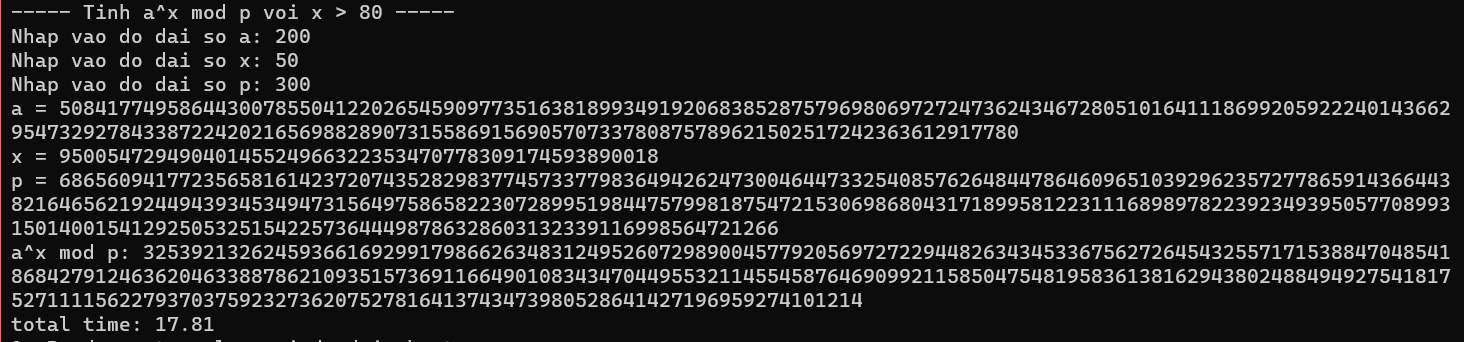
* Kiểm tra tính đúng đắn với số nhỏ trước

Text

Description automatically generatedText

Description automatically generated

* Đối với số lớn thì sẽ mất trung bình 20 giây



Text

Description automatically generated

Text

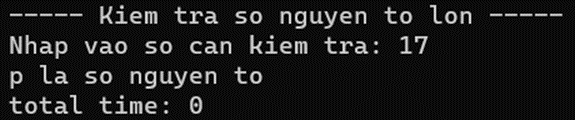
Description automatically generated

1. Kiểm tra số nguyên tố

* Kiểm tra tính đúng đắn với số nhỏ

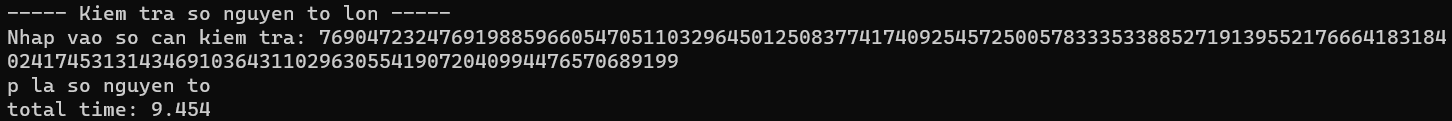
Text

Description automatically generated



* Tạo ngẫu nhiên một số nguyên tố lớn bất kì từ <https://bigprimes.org/> rồi kiểm tra thì đối với các số lớn có kích thước tầm 150 chữ số thì sẽ tốn khoảng 9.5 giây để kiểm tra.



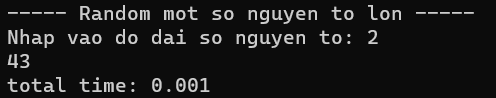


1. Tạo ngẫu nhiên số nguyên số lớn

* Thử tính đúng đắn đối với số nhỏ

Text

Description automatically generated



* Đối với các số lớn có độ dài 35 kí tự thì sẽ tốn trung bình 10 giây

Text

Description automatically generated with medium confidence

Text

Description automatically generated

A black background with white text

Description automatically generated with medium confidence

1. **Mã hóa khóa công khai RSA**
2. *Mô tả thuật toán*

* Sẽ dùng lại các hàm từ câu trước để tính

1. *Kiểm thử chương trình*

* Kiểm tra tính đúng đắn đối với số nhỏ

Text

Description automatically generated

Text

Description automatically generated

* Đối với số lớn với độ dài p và q là 70 chữ số và e là 5 chữ số thì trung bình sẽ tốn tầm 15 giây

Text

Description automatically generated

Text

Description automatically generated

1. **Ứng dụng chat có bảo mật**
2. *Mô tả hoạt động của ứng dụng chat có mã hóa bằng RSA*

Graphical user interface, website

Description automatically generated

* Chỉ được phép tạo 1 server
* Có thể tạo nhiều client
* Nhấn vào nút Listen để kết nối server.

Graphical user interface

Description automatically generated

Graphical user interface, text, application, chat or text message

Description automatically generated

Graphical user interface, text, application

Description automatically generated

* Khi nhập tên vào ô Client name và nhấn nút Connect thì sẽ tạo đồng thời cặp khóa của mỗi client và gửi Public key của mình cho client còn lại.
* Server cũng sẽ nhận được Public key của 2 client.

Graphical user interface, text, application, chat or text message

Description automatically generated

* Khi client soạn tin nhắn và nhấn nút Send thì tin nhắn đó sẽ được mã hóa và gửi sang client khác.
* Client kia khi nhận được tin nhắn thì tin nhắn đó đã được giải mã trong quá trình gửi từ server về.
* Một vài đoạn code quan trọng

Graphical user interface, text, application

Description automatically generated

* Server nhận được và chỉ xem được nội dung đã mã hóa, không biết nội dung chính là gì.

1. *Một số đoạn code quan trọng*

* Hàm tạo khóa:

Text

Description automatically generated

* Hàm gửi khóa từ client:

Text

Description automatically generated

* Hàm server nhận thông tin từ client:

Text

Description automatically generated

* Hàm gửi thông tin đã mã hóa từ client:

Text

Description automatically generated

* Hàm nhận thông tin đã được mã hóa đến client khác trong server và hiển thị thông tin đã được giải mã:Text

  Description automatically generated

1. **TÀI LIỆU THAM KHẢO**

[1] <https://vietcodes.github.io/algo/miller>