**VIETNAM NATIONAL UNIVERSITY-HO CHI MINH CITY**

**UNIVERSITY OF SCIENCE**

Faculty of Information Technology

Logo

Description automatically generated

**REPORT PROJECT**

Nhập môn mã hóa mật mã

20MMT

**Mã hóa thông điệp với RSA**

20127245- Hồ Bá Nam

**Lectures:**

Nguyễn Văn Quang Huy – Ngô Đình Hy – Lê Phúc Lữ - Nguyễn Đình Thúc

Ho Chi Minh - 2022

Mục lục

[1. Thông tin 3](#_Toc123251872)

[1.1. Thành viên 3](#_Toc123251873)

[1.2. Đồ án 3](#_Toc123251874)

[2. Mã hóa thông điệp sử dụng thuật toán RSA 3](#_Toc123251875)

[2.1. Vấn đề: 3](#_Toc123251876)

[2.2. Giải quyết 4](#_Toc123251877)

[2.2.1. Tạo khóa 5](#_Toc123251878)

[2.2.2. Mã hóa 7](#_Toc123251879)

[2.2.3. Giải mã 7](#_Toc123251880)

[3. Tài liệu tham khảo 8](#_Toc123251881)

1. Thông tin
   1. Thành viên
      * **Tên:** Hồ Bá Nam
      * **MSSV:** 20127245
      * **Mail:** [honambsn@gmail.com](mailto:honambsn@gmail.com)
   2. Đồ án
      * **Tên:** Mã hóa thông điệp sử dụng thuật toán RSA
      * **Nội dung:** Thông điệp được gửi qua lại giữ server và client bằng socket của Python được mã hóa bằng cách sử dụng thuật toán RSA.
      * **Ngôn ngữ lập trình:** Python
2. Mã hóa thông điệp sử dụng thuật toán RSA
   1. Vấn đề:

A và B liên lạc cho nhau một cách bí mật. Với thuật toán RSA, A sẽ gửi cho B khóa công khai của mình (A\_public\_key) và giữ lại cặp khóa bí mật (A\_private\_key).

* 1. Giải quyết

**Phía B:**

Lúc này, khi B muốn gửi thông điệp **M** của B cho A. M sẽ được chuyển đổi thành **m** sao cho **m** < **n** thông qua hàm có thể đảo ngược, tức là chuyển đổi từ **m** sang **M** và ngược lại, từ **M** sang **m** bằng hàm nghịch đảo/ 2 chiều. Quá trình mã hóa diễn ra:

Với:

**c** là bản mã hóa **của** m theo công thức trên

**m** là thông điệp **M** đã được chuyển đổi bằng hàm 2 chiều

**n, e** là khóa công khai mà A đã cho B biết

Sau đó, B sẽ gửi **c** cho A

**Phía A:**

A nhận được **c** từ B và có khóa bí mật. A giải mã thông điệp c theo công thức:

Chứng minh:

Theo định lý Fermat nhỏ:

ed 1 (mod p-1)

ed 1 (mod q-1)

Nên:

Và:

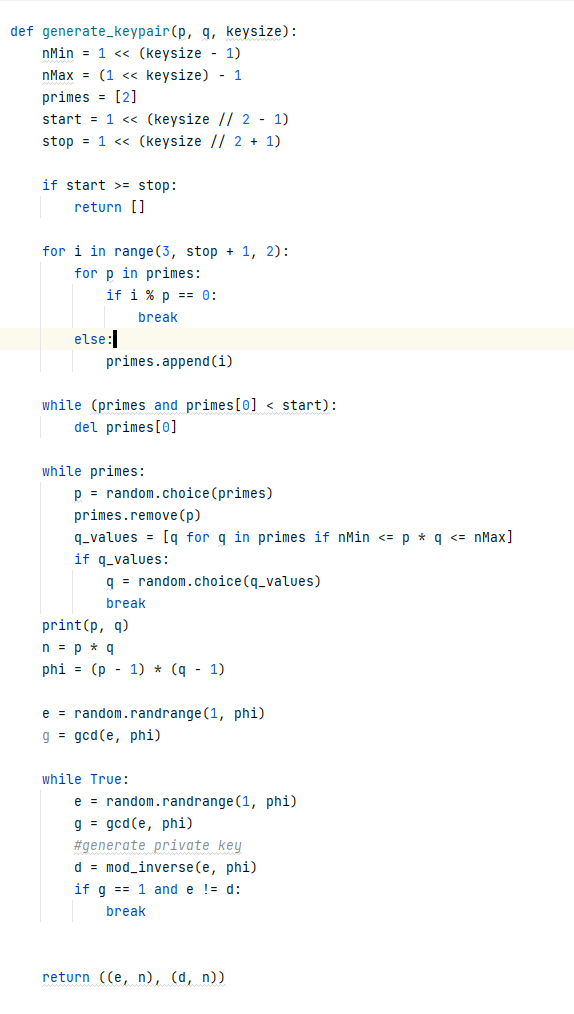
Mà **p**, **q** là 2 số nguyên tố cùng nhau, nên theo định lý đồng dư Trung Quốc:

Hoặc:

* + 1. Tạo khóa

1. Chọn ***p*** và ***q*** ngẫu nhiên và độc lập. Sao cho p,q là số nguyên tố và
2. Tính ***mô đun-n*** = **pq**
3. Tính giá trị của phi Euler
4. Chọn ***e-số mũ công khai*** sao cho 1 < ***e* <** và ***e*** là số nguyên tố cùng nhau với . Thực hiện bằng Euler mở rộng
5. Tính ***d***  sao cho **de** 1 (mod )

* Khóa công khai: **n,e**
* Khóa bí mật: **n,d**



* + 1. Mã hóa

Ở đây, m và M được chuyển đổi thông qua hàm **chr()** và **ord()** của Python

* **Hàm chr():** trả về một kí tự (một chuỗi) từ một số nguyên mà số nguyên ấy là đại diện cho mã unicode của ký tự được trả về.
* **Hàm ord():** trả về số nguyên đại diện cho mã Unicode của ký tự được chỉ địnhGraphical user interface, text

  Description automatically generated.
  + 1. Giải mã

Quá trình chuyển đổi từ m sang M cũng diễn ra tại đây

A screenshot of a computer

Description automatically generated with medium confidence

1. Tài liệu tham khảo

* [Mã hóa RSA hoạt động thế nào? (viblo.asia)](https://viblo.asia/p/ma-hoa-rsa-hoat-dong-the-nao-3Q75w119ZWb)
* [Hệ mã hóa RSA và chữ ký số (viblo.asia)](https://viblo.asia/p/he-ma-hoa-rsa-va-chu-ky-so-6J3ZgkgMZmB)
* [RSA (mã hóa) – Wikipedia tiếng Việt](https://vi.wikipedia.org/wiki/RSA_(m%C3%A3_h%C3%B3a))
* [Định lý nhỏ Fermat – Wikipedia tiếng Việt](https://vi.wikipedia.org/wiki/%C4%90%E1%BB%8Bnh_l%C3%BD_nh%E1%BB%8F_Fermat)
* [Số học 4.5 - Nghịch đảo modulo (vnoi.info)](https://vnoi.info/wiki/algo/math/modular-inverse.md)
* [Giải thuật Euclid mở rộng – Wikipedia tiếng Việt](https://vi.wikipedia.org/wiki/Gi%E1%BA%A3i_thu%E1%BA%ADt_Euclid_m%E1%BB%9F_r%E1%BB%99ng)
* [Thuật toán Euclid mở rộng, Nghịch đảo Modulo, và Định lý số dư Trung Quốc | Thien Hoang (tvhoang.com)](https://www.tvhoang.com/articles/2017/11/extended-euclid#:~:text=Ngh%E1%BB%8Bch%20%C4%91%E1%BA%A3o%20modulo%20l%C3%A0%20c%C3%A1ch,thu%E1%BA%ADt%20to%C3%A1n%20m%C3%A3%20h%C3%B3a%20RSA.&text=c%C3%B3%20nghi%E1%BB%87m%20khi%20v%C3%A0%20ch%E1%BB%89%20khi%20b1%2Cb2,B%3Db1b2%E2%80%A6)
* [7.5 Implementing RSA in Python (toronto.edu)](https://www.cs.toronto.edu/~david/course-notes/csc110-111/07-cryptography/05-rsa-cryptosystem-implementation.html)
* [Mã hóa RSA - w3seo tìm hiểu kiến thức của mã hóa công khai RSA (websitehcm.com)](https://websitehcm.com/ma-hoa-rsa/)
* [RSA là gì? Cách thức hoạt động của mã hóa RSA (vietnix.vn)](https://vietnix.vn/rsa/)
* [Số học 4 - Phi hàm Euler (vnoi.info)](https://vnoi.info/wiki/translate/he/Number-Theory-4.md)
* [Thuật toán RSA - Tính đúng đắn, Tính an toàn và Ví dụ tính toán cụ thể - YouTube](https://www.youtube.com/watch?v=9KohZt8EFNc&ab_channel=Ph%E1%BA%A1mThanhScience%26Tech)
* [Hàm phi Euler – Wikipedia tiếng Việt](https://vi.wikipedia.org/wiki/H%C3%A0m_phi_Euler)
* [Hàm chr() trong Python - HKT SOFT](https://hktsoft.com/ham-chr-trong-python/)
* [Hàm chr() trong Python - QuanTriMang.com](https://quantrimang.com/hoc/ham-chr-trong-python-159985#:~:text=Trong%20Python%2C%20h%C3%A0m%20chr(),k%C3%BD%20t%E1%BB%B1%20%C4%91%C6%B0%E1%BB%A3c%20tr%E1%BA%A3%20v%E1%BB%81.)
* [What is the difference between an Ord () and a CHR () function? - Quora](https://www.quora.com/What-is-the-difference-between-an-Ord-and-a-CHR-function)
* [Python Socket Programming - Server, Client Example | DigitalOcean](https://www.digitalocean.com/community/tutorials/python-socket-programming-server-client)