**TRƯỜNG ĐẠI HỌC HÀNG HẢI VIỆT NAM  
KHOA CÔNG NGHỆ THÔNG TIN**

**-----\*\*\*-----**

****

**BÁO CÁO BÀI TẬP LỚN**

**HỌC PHẦN AN TOÀN VÀ BẢO MẬT THÔNG TIN**

***Bài tập:* Mã hóa và giải mã RSA cho văn bản ngắn**

***GVHD: Phạm Tuấn Đạt***

***Sinh viên thực hiện: Nguyễn Ngọc Nguyên–87009***

***Phạm Bảo Ngọc–85797***

***Phạm Minh Hiệp–92465***

***Hải Phòng, tháng 05 năm 2023***

**TRƯỜNG ĐẠI HỌC HÀNG HẢI**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BỘ MÔN KHOA HỌC MÁY TÍNH**

**-----\*\*\*-----**

**BÀI TẬP LỚN**

**HỌC PHẦN AN TOÀN VÀ BẢO MẬT THÔNG TIN**

**Mã bài tập: 04**

1. **Tên bài tập: Mã hóa và giải mã RSA cho văn bản ngắn**
2. **Mục đích**

Nhằm mô phỏng cơ chế mã hóa và giải mã RSA cho văn bản ngắn

1. **Công việc cần thực hiện**

* Phân tích bài toán
* Code
* Giải thích code

1. **Yêu cầu**

* Kết quả làm bài tập lớn: Báo cáo bài tập lớn
* Báo cáo bài tập lớn phải được trình bày theo mẫu quy định (kèm theo), báo cáo có thể kết xuất thành tệp định dạng PDF và nộp qua email (không bắt buộc phải in ấn)
* Hạn nộp báo cáo bài tập lớn:

1. **Tài liệu tham khảo**
   * Giáo trình An toàn và bảo mật thông tin của trường Đại Học Hàng Hải Việt Nam.

***Hải Phòng, tháng … năm …***

**NGƯỜI HƯỚNG DẪN**

# MỤC LỤC

[MỤC LỤC 1](#_Toc134880651)

[DANH MỤC CÁC HÌNH VẼ, BẢNG BIỂU 2](#_Toc134880652)

[CHƯƠNG 1. CƠ SỞ LÝ THUYẾT 1](#_Toc134880653)

[CHƯƠNG 2. BÀI TOÁN: 2](#_Toc134880654)

[1. Giao diện chương trình: 2](#_Toc134880655)

[2. Các chức năng phục vụ cho mã hoá , giải mã 2](#_Toc134880656)

[2.1. Hàm GCD: 2](#_Toc134880657)

[2.2 Hàm kiểm tra số nguyên tố: 3](#_Toc134880658)

[2.3. Tạo khoá bí mật, khoá công khai: 3](#_Toc134880659)

[3. Chức năng mã hoá: 4](#_Toc134880660)

[4. Chức năng giải mã 5](#_Toc134880661)

[CHƯƠNG 3. KẾT QUẢ THỬ NGHIỆM 5](#_Toc134880662)

# DANH MỤC CÁC HÌNH VẼ, BẢNG BIỂU

|  |  |
| --- | --- |
| Hình vẽ | Trang |
|  |  |
|  |  |
|  |  |

# [CHƯƠNG 1. CƠ SỞ LÝ THUYẾT](#_35nkun2)

- Hệ mã RSA được đặt tên dựa theo các chữ cái đầu của 3 tác giả của hệ mã là Rivest, Shamir và Adleman. Đây là thuật toán mã hoá nổi tiếng nhất và cũng là thuật toán được ứng dụng thực tế nhất.

- Để cài đặt RSA, ban đầu mỗi người dùng sinh khoá công khai và khoá bí mật của mình bằng cách:

+ Chọn 2 số nguyên tố lớn ngẫu nhiên (gần 100 chữ số) khác nhau p và q.

+ tính N = p\*q

+ Chọn một số e nhỏ hơn N và (e, Ø(N)) = 1, e là số mũ sinh mã.

+ Tìm phần tử ngược của e trên vành module Ø(N), d là số mũ giải mã.

+ khóa công khai là = (e, N)

+ Khoá bí mật là = = (d, p, q)

- Việc thiết lập khoá này được thực hiện 1 lần khi người dùng thiết lập (thay thế) khoá công khai của họ. Mũ e thường là khá nhỏ (để mã hoá nhanh), và phải là nguyên tố cùng nhau với Ø(N). Các giá trị thường được chọn cho e là 3 hoặc – 1 = 65355. Tuy nhiên khi e nhỏ thì d sẽ tương đối lớn. Khoá bí mật là (d, p, q). Các số p và q thường xấp xỉ nhau nhưng không được bằng nhau. Chú ý là việc để lộ một trong các thành phần trên sẽ làm cho hệ mã hoá trở thành không an toàn.

- Sử dụng RSA:

+ Mã hoá 1 thông điệp M: C = (mod N ) (0 <= M < N)

+ Giải mã: M = (mod N)

Thuật toán mã hoá RSA làm việc được bởi vì nó dựa trên cơ sở toán học là sự tổng quát định lý Fermat nhỏ của Ơclit: = 1 (mod N). Trong thuật toán RSA, ta chọn e và d là nghịch đảo của nhau trên vành với e được chọn trước.

Do đó chúng ta sẽ có e.d = 1 mod Ø(N), suy ra:

M = = = = M. = M mod N

Công thức này đảm bảo việc giải mã sẽ cho kết quả đúng là bản rõ ban đầu (chú ý là chỉ đúng khi p khác q).

# CHƯƠNG 2. BÀI TOÁN:

\* Mục đích: Xây dựng chương trình mã hóa và giải mã RSA cho văn bản ngắn.

\* Có sử dụng ngôn ngữ lập trình C# để tạo Windows Form, sử dụng Visual Studio 2022.

\*Các chức năng chính:

## 1. Giao diện chương trình:

A screenshot of a computer

Description automatically generated

## 2. Các chức năng phục vụ cho mã hoá , giải mã

### 2.1. Hàm GCD:

public int GCD(int a, int b)

{

if (b == 0) return a;

return GCD(b, a % b);

}

### 2.2 Hàm kiểm tra số nguyên tố:

public static bool IsPrime(int num)

{

for(int i = 2; i <= Math.Sqrt(num); i++)

{

if (num % i == 0)

return false;

}

return num > 2;

}

### 2.3. Tạo khoá bí mật, khoá công khai:

if (nudPNumber != nudQNumber)

{

int num, i, ctr;

int eNum = 0;

int bat\_dau = Convert.ToInt32(nudPNumber.Value);

int ket\_thuc = Convert.ToInt32(nudQNumber.Value);

List<int> mangso = new List<int>();

for (num = 1; num <= 1000; num++)

{

ctr = 0;

for (i = 2; i <= num / 2; i++)

{

if (num % i == 0)

{

ctr++;

break;

}

}

if (ctr == 0 && num != 1)

{

mangso.Add(num);

}

}

int NNum = bat\_dau \* ket\_thuc;

txtNNumber.Text = NNum.ToString();

int phiNum = (bat\_dau - 1) \* (ket\_thuc - 1);

txtPhiNumber.Text = phiNum.ToString();

foreach (int so in mangso.Reverse<int>())

{

if (GCD(so, phiNum) == 1)

{

eNum = so;

txtENumber.Text = eNum.ToString();

break;

}

}

double dNum = 0;

double res = 0;

for (dNum = 2; ; dNum++)

{

res = (dNum \* eNum) % phiNum;

if (res == 1)

{

txtDNumber.Text = dNum.ToString();

break;

}

}

string privateKey = "(" + dNum + "," + NNum + ")";

string publicKey = "(" + eNum + "," + NNum + ")";

}

else

{

MessageBox.Show("Nhập p và q khác nhau!");

}

- Đầu tiên, nhập 2 số p và q khác nhau.

- Sử dụng 1 danh sách các số nguyên tố từ 1 đến 1000 để tìm số nguyên tố phù hợp cho giá trị e.

- Tính toán N = p \* q, tính toán giá trị của hàm phi Euler Φ(N) = (p – 1) \* (q – 1)

- Tìm giá trị của e trong danh sách số nguyên tố ở trên sao cho GCD(e, Φ(N)) = 1.

- Tính giá trị của d bằng cách duyệt từ 2 đến vô cùng và tìm giá trị d thỏa mãn tính chất (d\*e) % Φ(N) = 1.

- Tạo khoá công khai: Public key = (e, n)

- Tạo khoá bí mật: Private key = (d, n)

## 3. Chức năng mã hoá:

txtVanBanMaHoa.Clear();

BigInteger number = 0;

string s = txtVanBanGoc.Text;

int eNum = Convert.ToInt32(txtENumber.Text);

int N = Convert.ToInt32(txtNNumber.Text);

foreach (char c in s)

{

number = BigInteger.Pow((int)c, eNum) % N;

encrypt += (char)number;

mang.Add(number);

}

string mh = "";

foreach (BigInteger c in mang)

{

mh += (char)c;

}

txtVanBanMaHoa.Text = mh;

- Duyệt qua từng kí tự trong văn bản gốc, chuyển từng kí tự về dạng số nguyên, tính toán (int) % n. Chuyển giá trị vừa tính được về dạng kí tự, thêm vào xâu mã hoá.

=> Thu được xâu mã hoá cần tìm.

## 4. Chức năng giải mã

int dNum = Convert.ToInt32(txtDNumber.Text);

int N = Convert.ToInt32(txtNNumber.Text);

txtVanBanGiaiMa.Clear();

string gm = "";

BigInteger number1 = 0;

foreach (BigInteger c in mang)

{

number1 = BigInteger.Pow(c, dNum) % N;

giaima.Add(number1);

}

foreach (BigInteger a in giaima)

{

gm += (char)a;

}

txtVanBanGiaiMa.Text = gm;

- Duyệt qua từng số nguyên lớn có trong mảng ở phần mã hoá, tính (int) % n, lưu giá trị vừa tính được vào trong list giải mã.

- Duyệt qua từng phần tử có trong list giải mã, chuyển các giá trị tính được về dạng kí tự, ta thu được văn bản ban đầu.

# CHƯƠNG 3. KẾT QUẢ THỬ NGHIỆM

A screenshot of a computer

Description automatically generated

Chọn p = 17, q = 11.

Ta tính ra được số mũ sinh mã e = 997, n = 187, phiN =160 và d = 13.

=> Khoá công khai = (997, 187)

=> Khoá bí mật = (13, 187).

- Mã hoá đoạn văn bản : abc

-> Văn bản mã hoá: %b¥

-> Văn bản giải mã: abc (trùng với văn bản gốc).