TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TIỂU LUẬN MÔN CẤU TRÚC RỜI RẠC**

**NGHIÊN CỨU VỀ MODULO NGHỊCH ĐẢO BẰNG THUẬT TOÁN EXTENDED EUCLIDEAN VÀ HỆ THỐNG MÃ HÓA RSA**

*Người hướng dẫn*: **ThS Mai Duy Tân**

*Người thực hiện*: **NGUYỄN MINH KHANG – 52100040**

Lớp **: 21050201**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TIỂU LUẬN MÔN CẤU TRÚC RỜI RẠC**

**NGHIÊN CỨU VỀ MODULO NGHỊCH ĐẢO BẰNG THUẬT TOÁN EXTENDED EUCLIDEAN VÀ HỆ THỐNG MÃ HÓA RSA**

*Người hướng dẫn*: **ThS Mai Duy Tân**

*Người thực hiện*: **NGUYỄN MINH KHANG – 52100040**

Lớp **: 21050201**

Khoá  **: 25**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2022**

LỜI CẢM ƠN

Đầu tiên,em xin gửi lời cảm ơn chân thành đến Trường Đại học Tôn Đức Thắng đã đưa môn học “Cấu trúc rời rạc” vào trương trình giảng dạy. Đặc biệt,em xin gửi lời cảm ơn sâu sắc đến giảng viên bộ môn – Thầy Mai Duy Tân đã dạy dỗ, truyền đạt những kiến thức quý báu cho em trong suốt thời gian học tập vừa qua.Trong thời gian tham gia lớp học của thầy,em đã có thêm cho mình nhiều kiến thức bổ ích.Đây chắc chắn sẽ là những kiến thức quý báu, là hành trang để em có thể vững bước sau này.

Tuy nhiên, do bề dày kinh nghiệm còn nhiều hạn chế và khả năng tiếp thu thực tế còn nhiều bỡ ngỡ. Mặc dù em đã cố gắng hết sức nhưng chắc chắn bài báo cáo khó có thể tránh khỏi những thiếu sót và nhiều chỗ còn chưa chính xác, kính mong quý thầy,cô xem xét và góp ý để bài báo cáo của em được hoàn thiện hơn.

Lời cuối cùng,em xin kính chúc thầy, cô nhiều sức khỏe, thành công và hạnh phúc.

**BÀI TIỂU LUẬN ĐƯỢC HOÀN THÀNH**

**TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng tôi và được sự hướng dẫn của TS Mai Duy Tân. Các nội dung nghiên cứu, kết quả trong đề tài này là trung thực và chưa công bố dưới bất kỳ hình thức nào trước đây. Những số liệu trong các bảng biểu phục vụ cho việc phân tích, nhận xét, đánh giá được chính tác giả thu thập từ các nguồn khác nhau có ghi rõ trong phần tài liệu tham khảo.

Ngoài ra, trong đồ án còn sử dụng một số nhận xét, đánh giá cũng như số liệu của các tác giả khác, cơ quan tổ chức khác đều có trích dẫn và chú thích nguồn gốc.

**Nếu phát hiện có bất kỳ sự gian lận nào tôi xin hoàn toàn chịu trách nhiệm về nội dung đồ án của mình.** Trường Đại Học Tôn Đức Thắng không liên quan đến những vi phạm tác quyền, bản quyền do tôi gây ra trong quá trình thực hiện (nếu có).

*TP. Hồ Chí Minh, ngày 6 tháng 4 năm 2022*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

*Nguyễn Minh Khang*

PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN

**Phần xác nhận của GV hướng dẫn**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

**Phần đánh giá của GV chấm bài**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Tp. Hồ Chí Minh, ngày tháng năm

(kí và ghi họ tên)

TÓM TẮT

Bài tiểu luận này nhằm nghiên cứu và tìm hiểu về cách sửa dụng của một thuật toán có tên là Euclid mở rộng(extended euclid) giúp xử lý những bài toán về tìm một số modulo nghịch đảo.Ngoài ra,nhằm cung cấp thêm cho người xem và em những kiến thức về hệ thống mật mã RSA.

Cho biết về các cách sử dụng, khái quát,định nghĩa về chức năng cũng như những vấn đề gặp phải trong quá trình vận dụng vào Công nghệ thông tin.

Cung cấp chi tiết về cách sử dụng thuật toán và hệ thống mật mã RSA thông qua những đoạn code ví dụ minh họa.

Tìm hiểu và thảo luận về tính bảo mật và những ứng dụng mà hệ thống mã hóa RSA mang lại và đưa ra ý kiến của bản thân.

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc70167592)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc70167593)

[TÓM TẮT iv](#_Toc70167594)

[MỤC LỤC 1](#_Toc70167595)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 4](#_Toc70167596)

PHẦN 1-CHƯƠNG 1 – TÌM NGHỊCH ĐẢO MODULO N BẰNG THUẬT TOÁN EUCLID MỞ RỘNG (FINDING AN INVERSE MODULO N USING THE EXTENDED EUCLIDEAN

ALGORITHM.) [5](#_Toc70167597)

[1.1 Khái niệm nghịch đảo modulo? 5](#_Toc70167599)

[1.2 Khái quát về thuật toán Euclid mở rộng : 5](#_Toc70167600)

[1.3 Ví dụ,công thức,kết quả,phân tích thuật toán và giải thích chi tiết thuật toán euclid mở rộng về tìm số modulo nghịch đảo? 5](#_Toc70167601)

[1.4 Hiện thực và chạy chương trình minh họa : 7](#_Toc70167602)

PHẦN 2-CHƯƠNG 2 –HỆ THỐNG MÃ HÓA RSA((RSA CRYPTOSYSTEM)

..................................................................................................................................7

[2.1 Khái quát về mã hóa RSA? 8](#_Toc70167603)

[2.1.1.Số nguyên tố(prime) 8](#_Toc70167604)

[2.1.2.Thuật toán Euclid mở rộng 8](#_Toc70167605)

[2.1.3.Thuật toán phân tích thừa số nguyên tố: 9](#_Toc70167606)

[2.1.4.Bài toán RSA:](#_Toc70167607) 9

[2.1.5.Những tính năng của hệ mã hóa RSA: 1](#_Toc70167608)0

[2.1.6 Chữ ký số: 1](#_Toc70167609)0

[2.2 Hiện thực chương trình và ví dụ minh họa,giải thích cách thức hoạt động: 1](#_Toc70167610)0

[2.2.1.Ví dụ minh họa về mã hóa RSA: 1](#_Toc70167611)0

[2.2.2.Giải thích ví dụ: 1](#_Toc70167612)2

[2.3 Hiệu quả và tính bảo mật của RSA: 1](#_Toc70167613)3

[2.3.1.Hiệu quả của RSA: 1](#_Toc70167614)3

[2.3.2.Tính bảo mật của RSA: 1](#_Toc70167615)3

[2.4 Các mối đe dọa tiềm ẩn và hạn chế của RSA: 1](#_Toc70167617)3

[2.5 Kết luận: 1](#_Toc70167618)3

TÀI LIỆU THAM KHẢO..............................................................................................14

TỰ ĐÁNH GIÁ..............................................................................................................15

PHỤ LỤC.......................................................................................................................17

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

**CÁC CHỮ VIẾT TẮT**

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

**DANH MỤC HÌNH**

**No table of figures entries found.**

**DANH MỤC BẢNG**

**No table of figures entries found.**

PHẦN 1-CHƯƠNG 1 – TÌM NGHỊCH ĐẢO MODULO N BẰNG THUẬT TOÁN EUCLID MỞ RỘNG (FINDING AN INVERSE MODULO N USING THE EXTENDED EUCLIDEAN

ALGORITHM.)

*Tổng quát*:

- Khảo sát về bài toán nghịch đảo modulo

- Nghiên cứu về thuật toán Euclid mở rộng

- Viết chương trình minh họa.

1.1 Khái niệm nghịch đảo modulo?

-Khái niệm nghịch đảo modulo:Cho a là số nguyên x,m là các số nguyên dương(x<m),nếu x\*a mod m=1 thì a là nghịch đảo của a mod n.

-Kí hiệu là : mod m.

-Điều kiện:(a, m) = 1, m > a > 0.Với a,m cùng là số nguyên tố.

1.2 Khái quát về thuật toán Euclid mở rộng :

-Khái niệm:Thuật toán Euclid mở rộng là một phương pháp dùng để xử lí bài toán tìm số nghịch đảo modulo.Đây còn được xem là một cách để giải một phương trình vô định nguyên(phương trình Đi-ô-phăng).

1.3 Ví dụ,công thức,kết quả,phân tích thuật toán và giải thích chi tiết thuật toán euclid mở rộng về tìm số modulo nghịch đảo?

\*Công thức:

;

;

;

;

\*Ví dụ:

-Tính mod với =11, =60

Áp dụng thuật toán euclid mở rộng để giải quyết bài toán,ta có bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Step |  |  |  |  |  |  |
| 0 | 11 | 0 | 60 | 11 | 1 | 0 |
| 1 | 60 | 5 | 11 | 5 | 0 | 1 |
| 2 | 11 | 2 | 5 | 1 | 1 | 0 |
| 3 | 5 | 5 | 1 | 0 | -5 | 1 |
| 4 |  |  |  |  | 11 | -2 |

\*Giải thích chi tiết:

Step 0:

*>*

Step 1:

=60,

Step 2:

=5,

Step 3:

=11,

=>

Step 4:

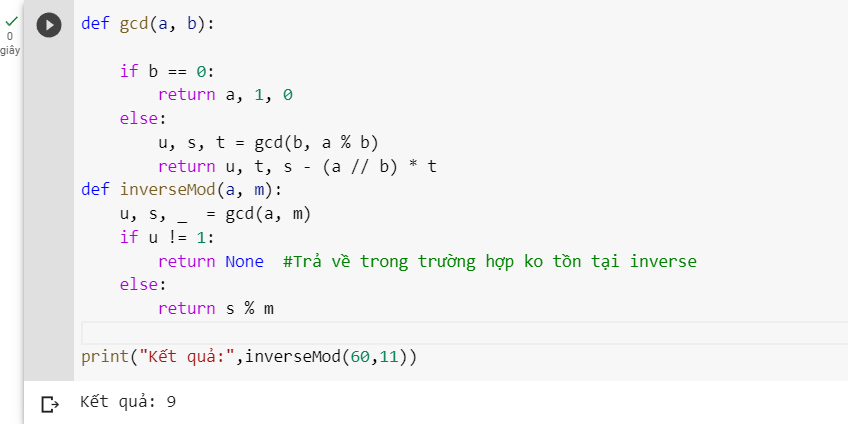
,

Từ bảng kết quả trên ta thấy được 11\*11+60\*(-2)=gcd(11,60)=1

=>s=11,t=-2

Vậy

1.4 Hiện thực và chạy chương trình minh họa :



Hình 1:Kết quả trả về của chương trình

\*Giải thích chương trình:

- Bước 1:Tìm ước chung lớn nhất

-Với hàm extended\_euclidean(a,b)

-Nếu b bằng 0 trả về a,1,0.Ngược lại thì trả về kết quả ước chung lớn nhất theo công thức trên.

- Bước 2:Tìm nghịch đảo modulo(a,m):

-Với ước chung lớn nhất bằng 1,áp dụng công thức của thuật toán Euclid mở rộng.Ngược lại,trả về trong trường hợp không tồn tại số modulo nghịch đảo.

\*Kết quả :Từ hình 1 ,có thể thấy kết quả của chương trình minh họa trùng khớp với kết quả ở ví dụ của bài toán =9.

CHƯƠNG 2 –HỆ THỐNG MÃ HÓA RSA(RSA CRYPTOSYSTEM)

2.1 Khái quát về mã hóa RSA?

-RSA là một mã hóa công khai.Thuật toán được Ron Rivest, Adi Shamir và Len Adleman phát minh 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.

-Hệ thống mã hóa RSA gồm 4 bước chính:key generation,key distribution,encryption và decryption.Nhằm đảm bảo tính bảo mật nên mỗi hệ thống khác nhau cần tạo ra các public và private key khác nhau.

-Public key:Được sử dụng để mã hóa những thông tin mà ta muốn chia sẻ với bất kỳ ai

-Private key:Ngược lại,được sử dụng để giải mã thông tin,chỉ riêng mình biết ,không được chia sẻ với người nào khác.

-Ngoài ra trapdoor function được xây dựng vào độ khó khăn của việc phân tích thừa số nguyên tố.

-Trước hết,để hiểu thêm về hệ thống mã hóa RSA em sẽ đưa ra những khái niệm toán học bao gồm:số nguyên tố,thuật toán eucluid mở rộng và phân tích thừa số nguyên tố cùng những ví dụ minh họa.

2.1.1.Số nguyên tố(prime)

Số nguyên tố là tập hợp số tự nhiên chia hết cho 1 và chính nó.

Ví dụ:2,3,5,…

2.1.2.Thuật toán Euclid mở rộng

Ví dụ :Tìm modulo nghịch đảo của 25 mod 101 với =101, = 25

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Step |  |  |  |  |  |  |
| 0 | 101 | 4 | 25 | 1 | 1 | 0 |
| 1 | 25 | 25 | 1 | 0 | 0 | 1 |
| 2 |  |  |  |  | 1 | -4 |

Kết luận: với( s=1 và t =-4)

2.1.3.Thuật toán phân tích thừa số nguyên tố:

-Phân tích thừa số nguyên tố là việc tách một số bất kỳ thành một tích các số nguyên nhỏ hơn.

Giả sử p<q thì p<

Chia n cho các số lẻ nhỏ hơn hoặc bằng để tìm p

Thuật toán này chỉ khả dụng với những số n nhỏ.

Ví dụ:Phân tích thừa số nguyên tố của 50:

50=2\*5\*5=2\*.

2.1.4.Bài toán RSA:

Cho một số nguyên dương:

n=p\*q(p,q là hai thừa số nguyên tố)

Một số nguyên dương b sao cho

gcd(b,(p-1)(q-1)=1 và một số nguyên c

=>Tìm số nguyên x sao cho

\*Cơ chế mã khóa công khai RSA:

-Chọn hai số nguyên tố p và q

-Tính n=p\*q φ(n)=(p-1)\*(q-1)

-Chọn số nguyên e, sao cho 1 < e < φ(n) và e là số nguyên tố cùng nhau với φ(n)

-Tìm số nguyên d, sao cho (d \* e) mod φ(n) = 1.

-Khóa công khai là cặp (e, n), khóa bí mật là cặp (d, n).

2.1.5.Những tính năng của hệ mã hóa RSA:

Cung cấp một mức cao về tính toán bảo mật,toàn vẹn,chống chối bỏ và xác thực.

-Tính bảo mật:Bảo mật thông tin cao.

-Tính toàn vẹn:Bảo đảm thông tin không bị thay đổi.

-Chống chối bỏ:Truyền tín hiệu đến người nào đó ngay cả khi họ từ chối.

-Tính xác thực: Xác thực,định danh người dùng hệ thống.

2.1.6 Chữ ký số:

-Chữ ký số là một dạng của chữ ký điện tử. Nó là một dạng dữ liệu dùng để chứng thực cho các dữ liệu khác

-Ưu điểm:Dễ dàng nhận biết được chữ ký giả.Do vậy người xác thực sẽ rất dễ phát hiện chữ ký nhanh chóng

2.2 Hiện thực chương trình và ví dụ minh họa,giải thích cách thức hoạt động:

2.2.1.Ví dụ minh họa về mã hóa RSA:

-Trước tiên ta cần xác định từng ký tự của đoạn text ứng với từng dạng số theo bảng sau:

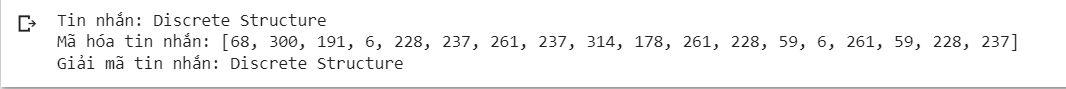
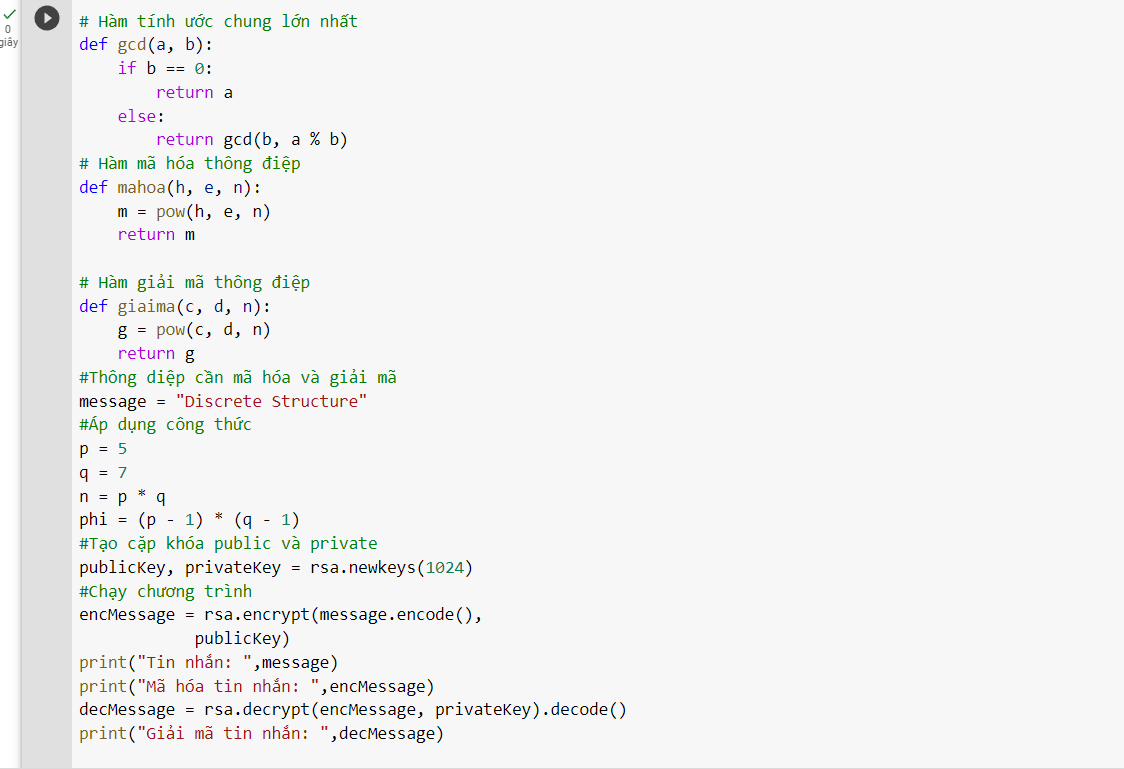
|  |  |  |  |
| --- | --- | --- | --- |
| a | 01 | n | 14 |
| b | 02 | o | 15 |
| c | 03 | p | 16 |
| d | 04 | q | 17 |
| e | 05 | r | 18 |
| f | 06 | s | 19 |
| g | 07 | t | 20 |
| h | 08 | u | 21 |
| i | 09 | v | 22 |
| j | 10 | w | 23 |
| k | 11 | x | 24 |
| l | 12 | y | 25 |
| m | 13 | z | 26 |
|  |  | space | 27 |

-Ví dụ cho một message:”Hello”

Sau khi mã hóa văn bản sẽ chuyển thành:”0805121215”

Tiếp theo sẽ đến với ví dụ có minh họa trên code:

-Mã hóa và giải mã về một đoạn tin nhắn "Discrete Structure"

 Hình 2.Kết quả sau khi mã hóa và giải mã từ tin nhắn

2.2.2.Giải thích:

Sau đây em sẽ trình bày các bước để có thể mã hóa và giải mã tin nhắn bằng RSA:

Bước 1:Viết cách hàm tính ước chung lớn nhất,hàm mã hóa,hàm giải mã,..

Bước 2:Chọn 2 số nguyên tố p và q để tạo ra một số nguyên khác n=p\*q

Bước 3:Khai báo cặp khóa public và private.

Bước 4:Để có thể chuyển đổi từ tin nhắn sang mã giả và giải mã ,em sử dụng đồng dư thức a=.

\*Công thức mã hóa:

c= với public key(e,n)

\*Công thức giải mã:

m= với private key(d,n)

2.3 Hiệu quả và tính bảo mật của RSA:

2.3.1.Hiệu quả:

-Thực tiễn cho thấy hệ mã hóa RSA có nhiều ứng dụng hiệu quả và độc đáo như :xác minh tính toàn vẹn của thông điệp bằng chữ ký số,mã hóa văn bản,…

-Mã hóa RSA cũng được sử dụng để phát triển nhiêu hệ thống như:OpenSSL,Cryptlit,…Ngoài ra RSA cũng được sử dụng một cách rộng rãi ngày nay như có thể thẩy ở các trình duyệt web,email,phương tiện truyền thông,…

-RSA cũng thường được sử dụng cho mục đích tạo ra kết nối an toàn giữa máy chủ và máy khách VPN.Có thể thấy RSA tiếp cận người dùng rất hiệu quả.

2.3.2.Bảo mật:

Hệ thống bảo mật của RSA rất cao.Vì độ bảo mật của RSA phụ thuộc vào 2 vấn đề củ bài toán:phân tích thừa số nguyên tố và bài toán RSA.Những số nguyên càng lớn, càng phức tạp thì bảo mật RSA lại càng cao.

2.4 Các mối đe dọa tiềm ẩn và hạn chế của RSA:

-Có nguy cơ bị lấy cắp thông tin vì công nghệ rất tinh vi.

-Có rất nhiều yếu tố xác thực.

-Tốc độ mã hóa chậm.

-Dễ bị tấn công.

2.5 Kết luận:

-Ngày nay, với sự phát triển của công nghệ thông tin đặt biệt là mạng internet thì việc truyền tải thông tin đã dể dàng và nhanh chóng hơn trong mọi lĩnh vực có nhu cầu trao đổi thông tin với nhau.Trong mật mã học,RSA là một thuật toán thú vị,nó đánh dấu sự tiến bộ vượt bậc của lĩnh vực mật mã học trong thời đại ngày nay.

**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

[1]RSA và những điều thú vị-Nguyễn Minh Thông-2020

[2] RSA là gì và cách thức hoạt động của mã hóa RSA-Nguyễn Hưng-2021

[3] Giáo trình lý thuyết cấu trúc rời rạc (2021-2022)-Trường Đại học Công nghiệp Thành phố Hồ Chí Minh

[4]Thuật toán RSA – mã hóa và giải mã thông tin-Lập trình python

[5] Code tham khảo task 1-TS Mai Duy Tân

**Tiếng Anh**

1. Cryptography Lab: RSA Encryption and Decryption.pdf
2. Discrete Structures Lecture Notes-Vladlen Koltun1 Winter 2008
3. More on Cryptography and Mathematical Induction-I¸sıl Dillig.
4. Public-key cryptography and RSA-Clemson university
5. The RSA Cryptosystem-Dunke university

**\*Tự đánh giá**

**Rubric**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Criteria** | **Scale** | **0 score** | **1/2 score** | **Full score** | **Self-evaluation** | **Reason** |
|  | **Theorical**  **research** | **1** | **Do**  **nothing**  **or**  **wrongly** | **Not**  **enough**  **details, no**  **example,**  **no**  **comment** | **Correct**  **calculation**  **s, detailed**  **explanatio**  **ns** | **1** | **Completed** |
| **Task 1** | **Implementation** | **2** | **Error** | **Correct but**  **bad**  **performance** | **Correct**  **and**  **good**  **performance** | **2** | **Completed** |
|  | **Test** | **1** | **No test** | **Test**  **without**  **verification** | **Test and**  **verification** | **1** | **Completed** |
|  | **Theorical**  **research** | **2** | **Do**  **nothing**  **or**  **wrongly** | **Not**  **enough**  **details, no**  **example,**  **no**  **comment** | **Correct**  **calculation**  **s, detailed**  **explanations** | **1** | **Completed** |
|  | **Implementation** | **1** | **Error** | **Correct but**  **bad**  **performance** | **Correct**  **and**  **good**  **performance** | **1** | **Completed** |
|  | **Test** | **1** | **No test** | **Test without**  **verification** | **Test and verification** | **1** | **Completed** |
| **Task 2** | **Analysis** | **0.5** | **Do**  **nothing**  **or**  **wrongly** | **Not**  **enough**  **details, no**  **example,**  **no comment** | **Correct,**  **detailed**  **explanations** | **0.5** | **Completed** |
|  | **Discussion** | **0.5** | **Do**  **nothing**  **or**  **wrongly** | **Not**  **enough**  **details, no**  **example,**  **no**  **comment** | **Correct,**  **detailed**  **explanatio**  **ns** | **0.5** | **Completed** |
|  | **Recommendation** | **0.5** | **Do**  **nothing**  **or**  **wrongly** | **Not**  **enough**  **details, no**  **example,**  **no**  **comment** | **Correct,**  **detailed**  **explanations** | **0.5** | **Completed** |
|  | **Reference** | **0.5** | **No reference** | **Wrong**  **format** | **Right**  **format** | **0.5** | **Completed** |
|  | **Total** | **10** | **Result** |  |  | **9** |  |

**PHỤ LỤC**