TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN CẤU TRÚC RỜI RẠC**

**FINDING AN INVERSE MODULO N**

**RSA CRYPTOSYSTEM**

*Người hướng dẫn*: **GV. MAI DUY TÂN**

*Người thực hiện*:

Lớp **:**

Khoá  **:**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÀI TẬP LỚN MÔN CẤU TRÚC RỜI RẠC**

**FINDING AN INVERSE MODULO N**

**RSA CRYPTOSYSTEM**

*Người hướng dẫn*: **GV. MAI DUY TÂN**

*Người thực hiện*:

Lớp **:**

Khoá  **:**

**THÀNH PHỐ HỒ CHÍ MINH, NĂM 2023**

LỜI CẢM ƠN

Lời đầu tiên, em xin gửi lời cảm ơn chân thành và sự tri ân sâu sắc đến với các thầy cô, giảng viên của khoa Công nghệ thông tin nói chung và các thầy cô giảng dạy môn Cấu trúc rời rạc nói riêng. Trong suốt quá trình học tập và rèn luyện, em đã nhận được rất nhiều sự giúp đỡ tận tình, sự quan tâm, chăm sóc của các thầy cô. Đặc biệt là thầy Mai Duy Tân đã cung cấp cho em các kiến thức bổ ích về môn học.

Bởi lượng kiến thức của em còn hạn hẹp và gặp nhiều vấn đề trong quá trình học nên báo cáo bài tập lớn này sẽ còn nhiều thiếu sót và cần được học hỏi thêm. Em rất mong em sẽ nhận được sự góp ý của quý thầy cô về bài báo cáo này của em để em rút kinh nghiệm trong những môn học sắp tới. Cuối cùng, em xin chân thành cảm ơn quý thầy cô.

TP Hồ Chí Minh, ngày tháng 04 năm 2023

**ĐỒ ÁN 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 GV. 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 tháng 04 năm 2023*

*Tác giả*

*(ký tên và ghi rõ họ tên)*

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 báo cáo tìm hiểu về hai nội dung chính sau đây:

* Phần 1: Finding an Inverse Modulo n
* Phần 2: RSA Cryptosystem

MỤC LỤC

[LỜI CẢM ƠN i](#_Toc132304024)

[PHẦN XÁC NHẬN VÀ ĐÁNH GIÁ CỦA GIẢNG VIÊN iii](#_Toc132304025)

[TÓM TẮT iv](#_Toc132304026)

[MỤC LỤC 1](#_Toc132304027)

[DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ 4](#_Toc132304028)

[1. Chapter 1: Finding an Inverse Modulo n 5](#_Toc132304029)

[1.1. Euclidean Algorithm 5](#_Toc132304030)

[1.1.1. Ý tưởng 5](#_Toc132304031)

[1.1.2. Ví dụ 5](#_Toc132304032)

[1.2. Extended Euclidean Algorithm 7](#_Toc132304033)

[1.2.1. Bổ đề Bézout 7](#_Toc132304034)

[1.2.2. Ý tưởng 7](#_Toc132304035)

[1.2.3. Ví dụ 7](#_Toc132304036)

[1.3. Finding an Inverse Modulo n 8](#_Toc132304037)

[1.3.1. Khái niệm 8](#_Toc132304038)

[1.3.2. Ý tưởng 8](#_Toc132304039)

[1.3.3. Ví dụ 8](#_Toc132304040)

[1.4. Test 9](#_Toc132304041)

[2. Chapter 2: RSA cryptosystem 11](#_Toc132304042)

[2.1. Tổng quan 11](#_Toc132304043)

[2.2. Cách thức hoạt động 11](#_Toc132304044)

[2.3. Thuật toán RSA 12](#_Toc132304045)

[2.3.1. Ý tưởng 12](#_Toc132304046)

[2.3.2. Ví dụ 12](#_Toc132304047)

[2.3.2.1 Key generation 13](#_Toc132304048)

[2.3.2.2 Encryption 14](#_Toc132304049)

[2.3.2.3 Decryption 14](#_Toc132304050)

[2.3. Phân tích 14](#_Toc132304051)

[2.3.1. Hiệu suất 14](#_Toc132304052)

[2.3.2. Bảo mật 14](#_Toc132304053)

[2.4. Các lỗ hổng bảo mật và hạn chế 14](#_Toc132304054)

[2.4.1. Nguy hiểm khi để lộ private key 14](#_Toc132304055)

[2.4.2. Độ dài khóa ngắn 14](#_Toc132304056)

[2.5. Đề xuất giải pháp để cải thiện 14](#_Toc132304057)

[2.5.1. Bảo quản private key cẩn thận 14](#_Toc132304058)

[2.5.2. Tạo khóa có độ dài lớn 15](#_Toc132304059)

[2.6. Test 15](#_Toc132304060)

[SELF-EVALUATION FORM 18](#_Toc132304061)

**DANH MỤC KÍ HIỆU VÀ CHỮ VIẾT TẮT**

**CÁC KÝ HIỆU**

**CÁC CHỮ VIẾT TẮT**

DANH MỤC CÁC BẢNG BIỂU, HÌNH VẼ, ĐỒ THỊ

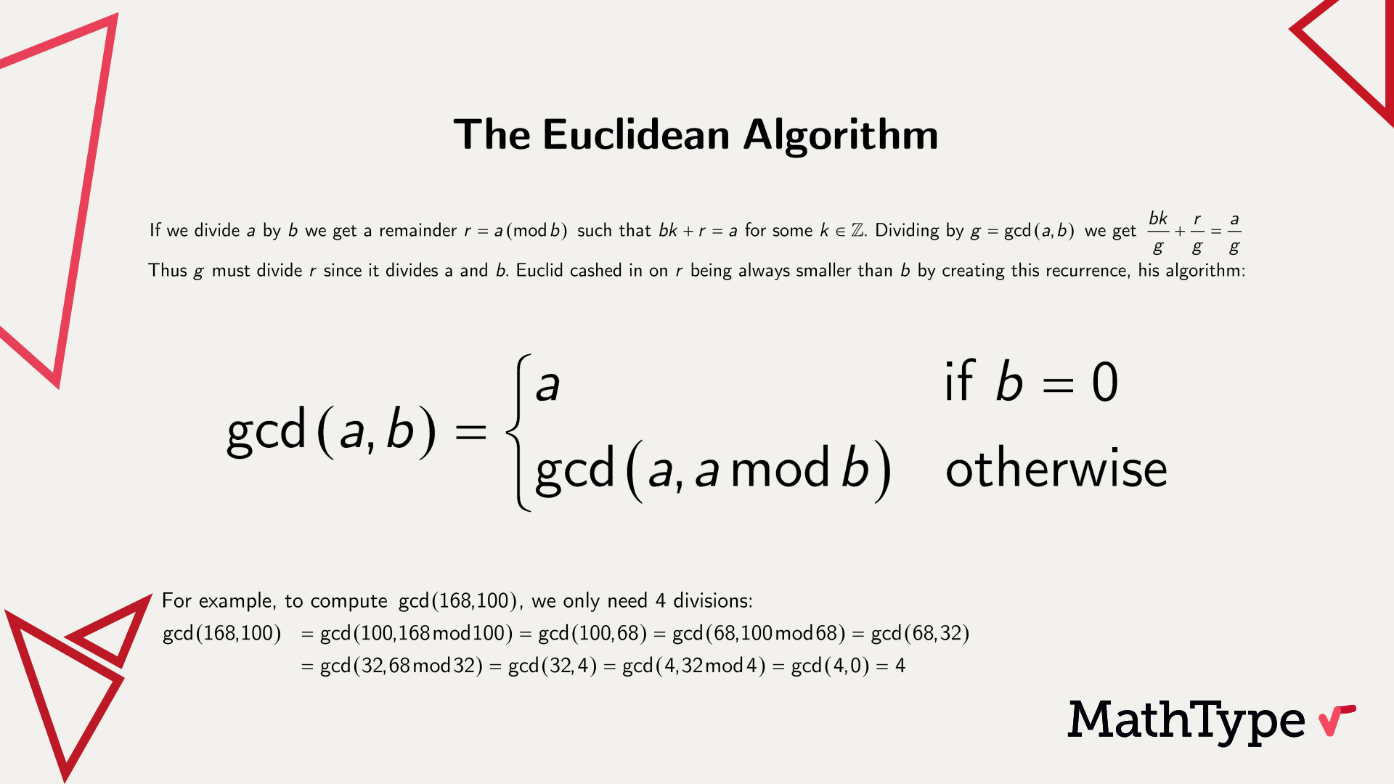
**DANH MỤC HÌNH**

**No table of figures entries found.**

**DANH MỤC BẢNG**

**No table of figures entries found.**

1. Chapter 1: Finding an Inverse Modulo n
   1. Euclidean Algorithm
      1. Ý tưởng



Để tìm ước chung lớn nhất của hai số nguyên a, b theo thuật toán Euclidean:

* Tìm ước chung lớn nhất của số nguyên a và phần dư của số nguyên a chia cho số nguyên b
* Tiếp tục tìm cho đến khi phần dư của số nguyên a chia cho số nguyên b bằng 0. Số nguyên a lúc này là ước chung lớn nhất của hai số nguyên a và b
  + 1. Ví dụ

Cho số nguyên a và số nguyên dương b bất kì, tồn tại số nguyên q và r sao cho a = bq + r và 0 <= r < b

(trong đó r là phần dư của số nguyên a chia cho số nguyên b, q là phần thương của số nguyên a chia cho số nguyên b)

Tìm ước chung lớn nhất của 326 và 78 theo thuật toán Euclidean

gcd(326, 78)

326 = 78 \* 4 + 14 ← gcd(78, 14)

78 = 14 \* 5 + 8 ← gcd(14, 8)

14 = 8 \* 1 + 6 ← gcd(8, 6)

8 = 6 \* 1 + 2 ← gcd(6, 2)

6 = 2 \* 3 + 0 ← gcd(2, 0)

Vậy ước chung lớn nhất của 326 và 78 là 2

* 1. Extended Euclidean Algorithm

Thuật toán Extended Euclidean Algorithm là thuật toán mở rộng của thuật toán Euclidean Algorithm trong đó ngoài việc tìm ước chung lớn nhất của hai số nguyên a, b thuật toán còn tìm hệ số Bézout

* + 1. Bổ đề Bézout

Cho hai số nguyên a, b không đồng thời bằng 0 và d là ước chung lớn nhất của a và b. Lúc này tồn tại một cặp x, y sao cho:

ax + by = d

* + 1. Ý tưởng

Thực thi thuật toán Euclidean tìm UCLN d của 2 số nguyên a, b

Khi tìm được UCLN d thì đi ngược lại và biểu diễn d ở dạng d = ax + by theo phần thương và số dư ở dòng trước cho đến khi đạt đến 2 số nguyên a, b ban đầu

* + 1. Ví dụ

gcd(326, 78)

326 = 78 \* 4 + 14 ← gcd(78, 14)

78 = 14 \* 5 + 8 ← gcd(14, 8)

14 = 8 \* 1 + 6 ← gcd(8, 6)

8 = 6 \* 1 + 2 ← gcd(6, 2)

6 = 2 \* 3 + 0 ← gcd(2, 0)

2 = 8 – 6

2 = 8 – (14 – 8) (Thay 6 = 14 - 8)

2 = -14 + 8 \* 2

2 = -14 + (78 – 14 \* 5) \* 2 (Thay 8 = 78 – 14 \* 5)

2 = 78 \* 2 + 14 \* (-11)

2 = 78 \* 2 + (326 – 78 \* 4) \* (-11) (Thay 14 = 326 – 78 \* 4)

2 = 326 \* (-11) + 78 \* (46)

Vậy x = -11, y = 46

* 1. Finding an Inverse Modulo n
     1. Khái niệm

**Congruence modulo**

Cho 2 số nguyên m, n và d là số nguyên dương.

m được gọi là đồng dư với n modulo d và viết ở dạng m ≡ n (mod d) nếu và chỉ nếu d | (m – n) hay m – n = k \* d

**Multiplicative inverse modulo n**

Cho bất kì số nguyên a, n với n > 1, nếu tồn tại số nguyên s sao cho as ≡ 1 (mod n) thì s được gọi là multiplicative inverse modulo n.

a-1a ≡ 1 (mod n) tương đương với as ≡ 1 (mod n)

Nghịch đảo của a theo modulo n tồn tại khi a và n nguyên tố cùng nhau tức là gcd(a, n) = 1

* + 1. Ý tưởng

Nếu gcd(a, n) = 1 thì có a-1

Áp dụng thuật toán Extended Euclidean để tìm x, y trong ax + ny = gcd(a, n) = 1

Trong đó x tìm được chính là inverse of a modulo n

* + 1. Ví dụ

Tìm nghịch đảo của 8 theo modulo 11

8 \* x ≡ 1 (mod 11)

gcd(8, 11)

11 = 8 \* 1 + 3 ← gcd(8, 3)

8 = 3 \* 2 + 2 ← gcd(3, 2)

3 = 2 \* 1 + 1 ← gcd(2, 1)

2 = 1 \*1 + 1 ← gcd(1, 1)

1 = 1 \* 1 + 0 ← gcd(1, 0)

Vậy gcd(8, 11) = 1

1 = 2 – 1

1 = 2 – (3 – 2) (Thay 1 = 3 – 2)

1 = -3 + 2 \* 2

1 = -3 + (8 – 3 \* 2) \* 2 (Thay 2 = 8 – 3 \* 2)

1 = 8 \* 2 – 3 \* 5

1 = 8 \* 2 – (11 – 8) \* 5 (Thay 3 = 11 – 8)

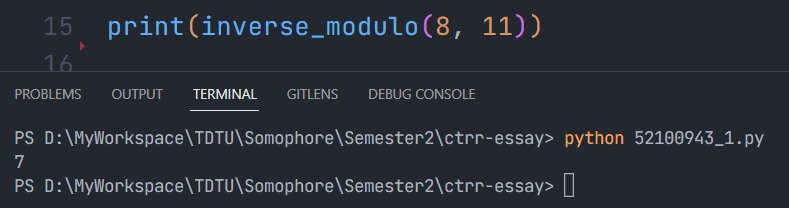
1 = 11 \* (-5) + 8 \* 7 (1 = n \* y + a \* x)

Vậy x = 7, y = -5

Vậy nghịch đảo của 8 theo modulo 11 là 7

8 \* 7 ≡ 1 (mod 11)

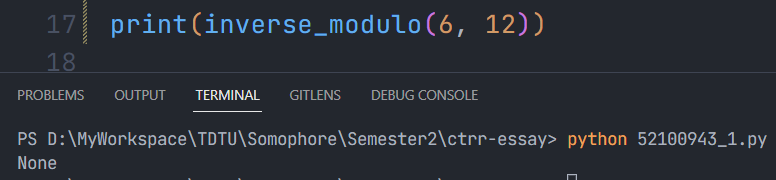
* 1. Test



Đầu tiên hàm inverse\_modulo sẽ tìm gcd(8, 11) và hệ số x trong 8 \* x + 11 \* y = gcd(8, 11) bằng thuật toán Extended Euclidean.

gcd(8, 11) = 1 nên có tồn tại nghịch đảo của 8 theo modulo 11.

Để nghịch đảo của 8 theo modulo của 11 luôn dương và không vượt quá 11 hàm sẽ lấy hệ số x modulo cho 11.

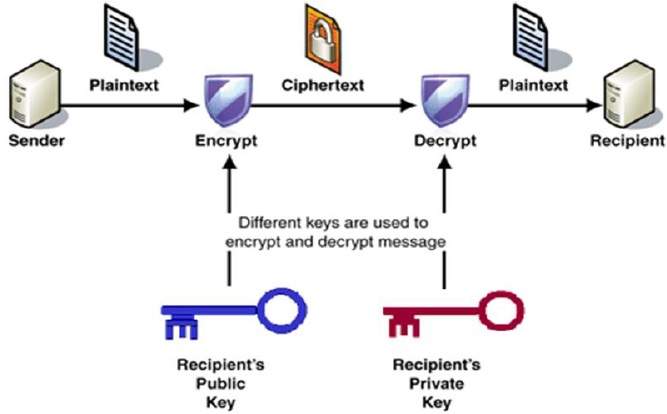


Vì gcd(6, 12) khác 1 cho nên không tồn tại nghịch đảo của 6 theo modulo 12.

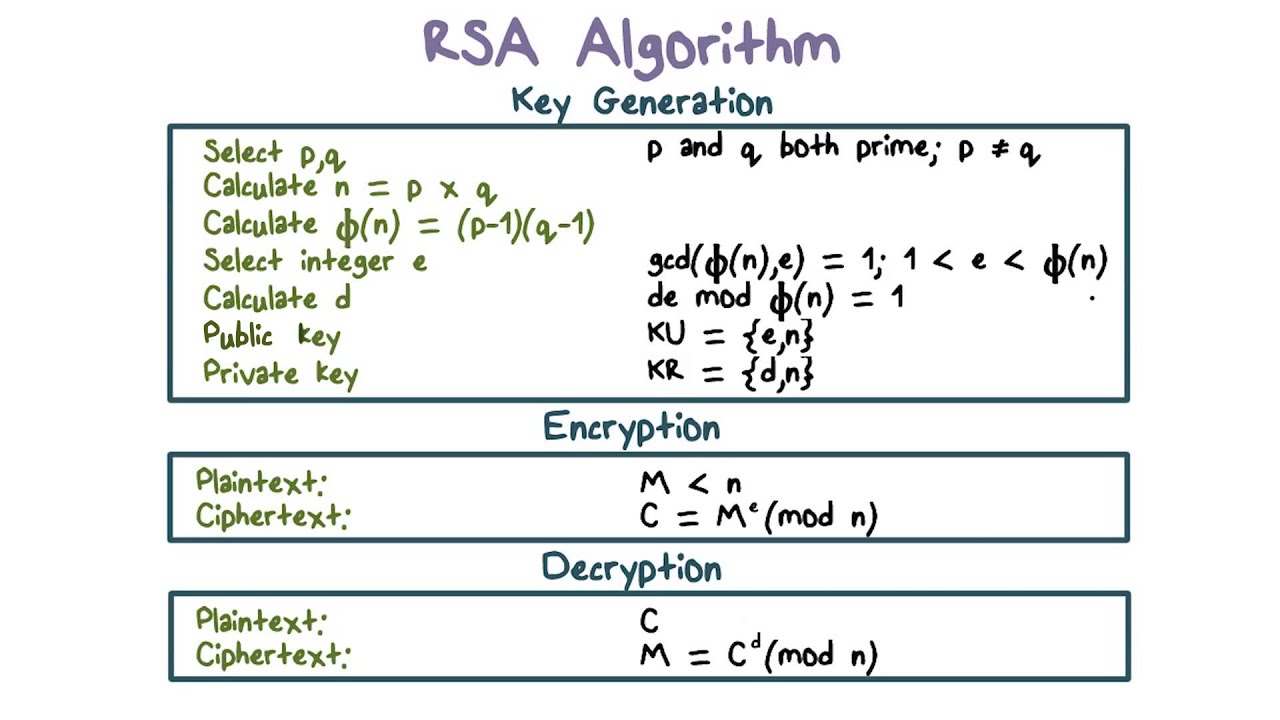
1. Chapter 2: RSA cryptosystem
   1. Tổng quan

RSA cryptosystem là thuật toán mã hóa sử dụng public key. Thuật toán được đặt theo tên 3 nhà nghiên cứu Ron Rivest, Adi Shamir và Leonard Adleman.

* 1. Cách thức hoạt động



* Người gửi gửi văn bản cho người nhận. Nội dung văn bản được mã hóa với public key của người nhận thành văn bản đã được mã hóa.
* Văn bản mã hóa sau khi được truyền đến người nhận sẽ được giải mã bởi private key của người nhận thành nội dung văn bản ban đầu người gửi gửi.
  1. Thuật toán RSA
     1. Ý tưởng



* Tạo khóa:
  + Chọn 2 số nguyên tố lớn khác nhau, một trong những cách để có được 2 số nguyên tố lớn khác nhau là chọn số nguyên ngẫu nhiên trong khoảng (2n-1 + 1, 2n – 1) với n là số bits
  + Tính modulus n = p \* q
  + Tính hàm phi Euler Φ(n) = (p - 1) \* (q - 1)
  + Chọn e sao cho gcd(Φ(n), e) = 1 và 1 < e < Φ(n)
  + Tính d bằng cách sử dụng thuật toán Extended Euclidean.
* Mã hóa
  + Sử dụng toán tử modulo để mã hóa văn bản bằng public key
* Giải mã
  + Sử dụng toán tử modulo để giải mã văn bản bằng private key
    1. Ví dụ
       1. Key generation

Chọn 2 số nguyên tố p = 5, q = 11 (trong ví dụ này, em chọn 2 số nguyên tố nhỏ để thuận lợi cho việc tính toán)

n = p \* q = 5 \* 11 = 55

Φ(n) = (p - 1) \* (q - 1) = (5 - 1) \* (11 - 1) = 40

Chọn 1 số e, sao cho gcd(40, e) = 1 và 1 < e < 40

e = 2 => Loại do gcd(40, 2) = 2

e = 3 => Nhận do gcd(40, 3) = 1

Vậy e = 3

de mod Φ(n) = 1 tương đương de ≡ 1 (mod Φ(n)) => Tính d bằng thuật toán

Extended Euclidean

3 \* d ≡ 1 (mod 40)

gcd(3, 40)

40 = 3 \* 13 + 1 ← gcd(3, 1)

3 = 1 \* 3 + 0 ← gcd(1, 0)

Vậy gcd(3, 40) = 1

1 = 40 – 3 \* 13

1 = 3 \* (-13) + 40 (1 = a \* x + n \* y)

Vậy x = -13, y = 1

Lấy nghịch đảo của 3 theo modulo 40 là số dương

x = -13 + 40 = 27

Vậy nghịch đảo của 3 theo modulo 40 là 27

3 \* 27 ≡ 1 (mod 40)

=> Public key = {3, 55}, Private key = {27, 55}

* + - 1. Encryption

Giả sử nội dung văn bản là M = 5

C = Me (mod n) = 53 (mod 55) = 125 mod 55 = 15

* + - 1. Decryption

Giải mã nội dung văn bản thông qua private key

M = Cd (mod n) = 1527 (mod 55) = 177147 mod 55 = 5

* 1. Phân tích
     1. Hiệu suất
* Thư viện cryptography được sử dụng rộng rãi, được tối ưu tốt và thường xuyên được cập nhật.
  + 1. Bảo mật
* Sử dụng key có độ dài 2048 bits
* Hàm hash SHA256 có tính bảo mật cao
  1. Các lỗ hổng bảo mật và hạn chế
     1. Nguy hiểm khi để lộ private key

Nếu private key bị lộ thì nội dung message hoàn toàn có thể được giải mã => Lộ thông tin cần bảo mật

* + 1. Độ dài khóa ngắn

Nếu độ dài khóa quá ngắn thì hacker có thể dùng kỹ thuật vét cạn (brute-force attack) để tìm khóa

* 1. Đề xuất giải pháp để cải thiện
     1. Bảo quản private key cẩn thận
* Sử dụng thiết bị lưu trữ key bảo mật
  + 1. Tạo khóa có độ dài lớn
* Sử dụng key có độ dài tối thiểu 2048 bits

* 1. Test

private\_key = rsa.generate\_private\_key(public\_exponent=65537, key\_size=2048)

public\_key = private\_key.public\_key()

Tạo khóa

msg = b"From T with Love"

Nội dung văn bản

ciphertext = public\_key.encrypt(

    msg,

    padding.OAEP(

        mgf=padding.MGF1(algorithm=hashes.SHA256()),

        algorithm=hashes.SHA256(),

        label=None

    )

)

Nội dung văn bản được mã hóa với public key

plaintext = private\_key.decrypt(

    ciphertext,

    padding.OAEP(

        mgf=padding.MGF1(algorithm=hashes.SHA256()),

        algorithm=hashes.SHA256(),

        label=None

    )

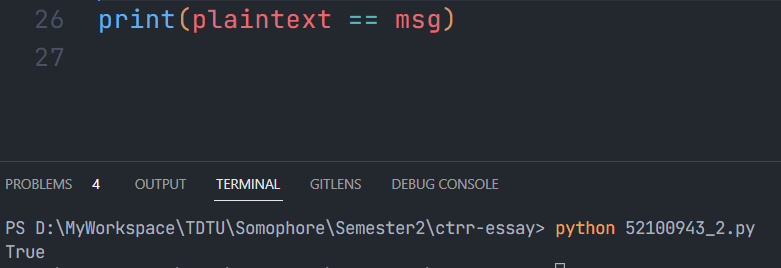
)

Giải mã văn bản được mã hóa với private key

Nếu giải mã văn bản với private key khác (không phải private key ban đầu tạo) thì chương trình sẽ báo lỗi.

print(plaintext == msg)

Kiểm tra xem nội dung văn bản có giống văn bản gốc không?



**TÀI LIỆU THAM KHẢO**

**Tiếng Việt**

[Modular multiplicative inverse – Tính nghịch đảo theo modulo | Nhan Nguyen (wordpress.com)](https://nhannguyen95.wordpress.com/2017/03/16/modular-multiplicative-inverse-tinh-nghich-dao-theo-phep-nhan-modulo/)

**Tiếng Anh**

Slide Discrete Structures Number Theory - TS Nguyễn Thị Huỳnh Trâm

SELF-EVALUATION FORM

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