TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**BÁO CÁO CUỐI KỲ**

**BÁO CÁO CUỐI KỲ**

**MÔN CẤU TRÚC RỜI RẠC**

*Người hướng dẫn*: **TS. NGUYỄN THỊ HUỲNH TRÂM**

*Người thực hiện*:

**HUỲNH HOÀNG TIẾN ĐẠT – 52200023**

**NGUYỄN THỊ HUYỀN DIỆU – 52200090**

**PHẠM THỊ THANH BÌNH – 52200104**

Lớp **: 22050201**

Khoá  **: 26**

**THÀNH PHỐ HỒ CHÍ MINH, THÁNG 4 NĂM 2024**

TỔNG LIÊN ĐOÀN LAO ĐỘNG VIỆT NAM

**TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

**KHOA CÔNG NGHỆ THÔNG TIN**



**TIỂU LUẬN GIỮA KỲ**

**TIỂU LUẬN GIỮA KỲ**

**MÔN CẤU TRÚC RỜI RẠC**

*Người hướng dẫn*: **TS. NGUYỄN THỊ HUỲNH TRÂM**

*Người thực hiện*:

**HUỲNH HOÀNG TIẾN ĐẠT – 52200023**

**NGUYỂN THỊ HUYỀN DIỆU – 52200090**

**PHẠM THỊ THANH BÌNH – 52200104**

Lớp **: 22050201**

Khoá  **: 26**

**THÀNH PHỐ HỒ CHÍ MINH, THÁNG 4 NĂM** **2024**

# **LỜI CẢM ƠN**

Để hoàn thành bài Báo cáo Cuối kỳ II năm học 2023 - 2024 môn Cấu trúc rời rạc lần này,

Lời đầu tiên, nhóm chúng em xin gửi lời cảm ơn chân thành của mình đến với Ban giám hiệu trường Đại học Tôn Đức Thắng, quý thầy cô giáo giảng viên của khoa Công nghệ thông tin vì đã tạo điều kiện tốt nhất giúp nhóm chúng em có thể trau đồi kiến thức để hoàn thành bài Báo cáo cuối kỳ lần này. Đây thực sự là một cơ hội tuyệt vời giúp cho nghề nghiệp của tụi em trong tương lai rộng mở hơn khi được tiếp xúc với sự hiện đại và nhiều kiến thức.

Với lòng biết ơn sâu sắc và vô cùng đặc biệt của mình, nhóm chúng em xin gửi lời cảm ơn sâu sắc đến TS. Nguyễn Thị Huỳnh Trâm – Giảng viên lý thuyết và thực hành môn Cấu trúc rời rạc, người đã luôn đồng hành, dẫn dắt và giúp đỡ chúng em trong việc hoàn thành bài Báo cáo Cuối kỳ lần này. Từ những kiến thức cô đã giảng dạy trên những giờ học để tụi em có thể áp dụng những kiến thức đó vào bài. Một lần nữa nhóm chúng em xin chân thành cảm ơn cô vì sự hỗ trợ của cô ạ.

Vì kiến thức bản thân tụi em còn hạn chế nên trong quá trình giải quyết vấn đề nên khi hoàn thành bài báo cáo lần này thì nhóm chúng em cũng không tránh khỏi những sai sót, chúng em kính mong nhận được những lời nhận xét, đóng góp ý kiến từ cô ạ.

Lời cuối cùng, nhóm chúng em xin gửi lời cảm ơn chân thành và gửi ngàn lời chúc tốt đẹp đến với quý thầy cô khi đã tạo cơ hội cho chúng em nâng cấp kiến thức trong môn học này.

Chúng em xin chân thành cảm ơn!

Tp. Hồ Chí Minh, ngày 22 tháng 05 năm 2024

Sinh viên

Huỳnh Hoàng Tiến Đạt

Nguyễn Thị Huyền Diệu

Phạm Thị Thanh Bình

# **ĐỒ ÁN ĐƯỢC HOÀN THÀNH**

# **TẠI TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**

Tôi xin cam đoan đây là sản phẩm đồ án của riêng chúng tôi và được sự hướng dẫn của TS.Nguyễn Thị Huỳnh Trâm;. 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 22 tháng 05 năm 2024*

*Tác giả*

*Huỳnh Hoàng Tiến Đạt*

*Nguyễn Thị Huyền Diệu*

*Phạm Thị Thanh Bình*

# **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 này được chia thành **04 chương**: Trước hết ta sẽ tìm hiểu về các nguyên tắc, các quy luật trong môn học Cấu trúc rời rạc. Phần tiếp theo thì ta sẽ giải quyết các vấn đề được đưa ra.

**Chương 1: Tổng quan đề bài**

**Chương 2: Part 1**

**Chương 3: Part 2**

**Chương 4: Part 3**

Hướng tiếp cận:

* Đầu tiên ta sẽ phải ngồi đọc lấy hết toàn bộ slide bài giảng trên lớp, highlight và rút ra những ý chính cần thiết phù hợp để giải quyết các bài tập được giao.
* Đối với phần tiếp theo: Ta sẽ phân tích đề bài thật kỹ lưỡng, làm thử bài tập ra giấy để dễ dàng chỉnh sửa cho hợp lý rồi mới đưa vào bài tiểu luận giữa kỳ để hạn chế sai sót.

Kết quả nhận được: Sau khi hoàn thành bài tiểu luận lần này thì em có thêm nhiều kiến thức mới và bổ ích hơn.

# **MỤC LỤC**

# **DANH SÁCH CÁC HÌNH ẢNH**

# **DANH SÁCH CÁC BẢNG BIỂU**

# **BẢNG ĐÓNG GÓP CỦA TỪNG THÀNH VIÊN TRONG NHÓM**

| **STT** | **Họ và tên** | **MSSV** | **Công việc được giao** | **Mức độ hoàn thành công việc (%)** | **Nhận xét** | **Chữ ký** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | Huỳnh Hoàng Tiến Đạt | 52200023 | Câu 2, 7, 9 | 100 | Hoàn thành tốt | A picture containing linedrawing  Description automatically generated |
| 2 | Nguyễn Thị Huyền Diệu | 52200090 | Câu 1, 4, 6 | 100 | Hoàn thành tốt | *A signature on a white background  Description automatically generated* |
| 3 | Phạm Thị Thanh Bình | 52200104 | Câu 3, 5, 8 | 100 | Hoàn thành tốt | **A close-up of a signature  Description automatically generated** |

# **LỜI MỞ ĐẦU**

Trong thời đại mạnh mẽ của Công nghệ Thông tin và Internet, nhu cầu và đời sống của con người ngày càng được cải thiện. Con người có xu hướng trải nghiệm, tìm kiếm những điều mới mẻ, tận hưởng cuộc sống hiện đại, ứng dụng những công nghệ hiện đại như robot, trí tuệ nhân tạo, AI... Điều này dẫn đến việc ứng dụng, sử dụng ngôn ngữ lập trình để tạo ra các trang web, trò chơi, ứng dụng là điều không thể tránh khỏi. Thậm chí là các loại AI chatbot để tư vấn những thắc mắc của con người chúng ta.

Môn học "Cấu trúc rời rạc" không chỉ là nền tảng lý thuyết mà còn mang đến cái nhìn sâu sắc, những tư duy logic về cách chúng ta có thể áp dụng những nguyên lý này vào thực tế.

Môn học mang đến những khám phá mới mẻ từ nhiều khía cạnh quan trọng trong lĩnh vực công nghệ thông tin. Mục tiêu là không chỉ là hiểu biết về các khái niệm lý thuyết, các tư duy logic mà còn là khả năng áp dụng chúng để giải quyết những thách thức cụ thể trong lĩnh vực Công nghệ Thông tin ngày nay.

# **CHƯƠNG 1: TỔNG QUAN ĐỀ BÀI**

## **Question 1: Euclid’s algorithm and Bezout’s identity**

a. Using Euclid’s algorithm to calculate *gcd*(2024, 1000 + *m*) and *lcm*(2024, 1000 + m), where *m* is the last 3 digits of your student ID. For example, if your student ID is 52200**123** then you need to calculate *gcd*(2024, 1123) and *lcm*(2024, 1123).

b. Apply above result(s) in to find 5 integer solution pairs (x,y) of this equation:

2024x + (1000 + *m*)y = *gcd*(2024, 1000 + *m*)

For example, if your student ID is 52000**123** then your equation is:

2024x + 1123y = *gcd*(2024, 1123)

## **Question 2: Recurrence relation**

Solve this recurrence relation.

*an = 8.an−1 – 15.an−2*

with *a0 = 5* and *a1 = m,*

where *m* is the last 2 digits of your student ID. For example, if your student ID is 522001**23** then *a1 = 23*.

## **Question 3: Set**

a. Create a set Γ of characters from your case-insensitive non-diacritical full name. For example, the set corresponding with “Tôn Đức Thắng” is Δ = {A, C, D, G, H, N, O, T, U}.

b. Find the union, intersect, non-symmetric difference, and symmetric difference of Γ and Δ, where Γ and Δ are from question 3a.

## **Question 4: Relations**

Let ℜ be a binary relation defined on 2 integers as follow:

where  is the last 2 digits of your student ID.

For example, if your student ID is 522001**23** then the valid binary relation is

Is R reflexive, symetric, anti-symetric, transitive? Prove your answer.

## **Question 5: Kruskal’s algorithm**

Propose a solution for circuit-checking in Kruskal's algorithm. Give an example.

## **Question 6: Eulerian** **circuit**

a. Does the following graph have an Eulerian circuit or Eulerian path? Why?

A grid with letters and numbers

Description automatically generated

b. Study and present your knowledge about Hierholzer’s algorithm to find an Eulerian circuit.

c. If the graph has an Eulerian circuit, use Hierholzer's algorithm to find an Eulerian circuit of that graph when the initial circuit R1 is:

i. If % 4 = 0 then R1 is EINME

ii. If % 4 = 1 then R1 is abhga

iii. If % 4 = 2 then R1 is UVbaU

iv. If % 4 = 3 then R1 is XCdX

Where is the 4-digit number combined by the last 4 digits in your StudentID*.* For example, Student ID 52201234 has = 1234.

## **Question 7: Map coloring**

Given this map:

A map of india with white text

Description automatically generated

a. Modeling this map by a graph.

b. Color the map (graph) with a minimum number of colors. Present your solution step by step.

Let be the 4-digit number combined by the last 4 digits in your StudentID*.* For example, StudentID 52201234 has = 1234.

i. If % 4 = 0 then start from Bihar.

ii. If % 4 = 1 then start from Orissa.

iii. If % 4 = 2 then start from Rajasthan.

iv. If % 4 = 3 then start from Meghalaya.

## **Question 8: Finding an Inverse Modulo *n***

* Conduct research on Finding an Inverse Modulo *n* using the extended Euclidean algorithm. Give your own examples.
* Implement a Python program to find an Inverse Modulo *n* using the extended Euclidean algorithm. Related libraries are NOT allowed.
* Test the implemented program using sample data and verify the results. Capture your screen results and explain them in your report document.

## **Question 9: RSA cryptosystem**

* Conduct research on RSA cryptosystem. Understand the mathematical concepts behind the RSA cryptosystem, including prime number generation, modular arithmetic, extended Euclidean algorithm, prime factorization, etc. Give your own examples.
* Implement a Python program to encrypt and decrypt a message with the RSA cryptosystem. Cryptography libraries are allowed.
* Test the implemented RSA cryptosystem using sample messages and verify the results. Capture your screen results and explain them in your report document.
* Analyze the efficiency and security of the implemented RSA cryptosystem.
* Discuss the potential security threats and limitations of the RSA cryptosystem.
* Conclude with recommendations for improving the RSA cryptosystem implementation.

# **CHƯƠNG 2: THỰC HIỆN GIẢI ĐỀ BÀI**

## **Câu 1: Euclid’s Algorithm and Bezout’s Identity**

### **Euclid’s Algorithm**

* Vì theo yêu cầu của đề bài là chọn MSSV nhỏ nhất trong 3 thành viên của nhóm nên nhóm chúng em xác định MSSV là 52200023. Nên m = 023
* Từ đó đề bài sẽ trở thành:

1. *gcd*(2024, 1000 + *023*) = *gcd*(2024, 1023)
2. *lcm*(2024, 1000 + *023*) = *lcm*(2024, 1023)
3. ***gcd*(2024, 1023)**

* Theo thuật toán Euclide, chúng ta giả sử a = 2024, b = 1023. Bắt đầu tiến hành việc a/b. Trong khi phần dư của việc a/b khác 0 thì ta gán giá trị của b cho a, giá trị của phép dư a/b sẽ được gán cho b. Và điều đó được lặp đi lặp lại, tiếp tục cho đến khi giá trị dư của phép chia a/b bằng 0. Cuối cùng, giá trị của b ở bước cuối cùng chính là GCD của a và b.

Bảng 1.1: Phép chia a/b

|  |  |  |  |
| --- | --- | --- | --- |
| **a** | **b** | **Kết quả** | **Phần dư** |
| 2024 | 1023 | 1 | 1001 |
| 1023 | 1001 | 1 | 22 |
| 1001 | 22 | 45 | 11 |
| 22 | **11** | 2 | 0 |

* Sau 4 lần chia thì ta nhận được kết quả cuối cùng của b là 11 khi phép chia đã dư 0.
* Vì vậy, kết quả của ***gcd*(2024, 1023) = 11.**

1. ***lcm*(2024, 1023)**

* Để tiến hành tính lcm(2024, 1023) của hai số a và b mà ta giả sử ở trên, ta có thể tính được chúng thông qua *gcd*(2024, 1023). Bằng cách lấy trị tuyệt đối tích a và b chia cho *gcd*(2024, 1023) thì ta sẽ nhận được giá trị của *lcm*(2024, 1023).
* *gcd*(2024, 1023) = 11 (giá trị đã được tính tại câu 1a ở trên)
* *Ta có:*

*a* x *b =gcd(a, b)* x *lcm(a, b)*

⬄ 2024 x 1023 = gcd(2024, 1023) x lcm(2024, 1023)

⬄ 2070552 = 11 x lcm(2024, 1023)

* lcm(2024, 1023) = = **188232**

1. **Bezout’s Identity**

**2024x + (1000 + *m*)y = *gcd*(2024, 1000 + *m*)**

* m = 023
* 2024x + (1000 + *023*)y = *gcd*(2024, 1000 + *023*)

⬄ 2024x + 1023y = *gcd*(2024, 1023) = 11 (đã thực hiện phép tính tại câu 1a)

* Ta sẽ biểu diễn 11 dưới dạng tổ hợp tuyến tính của 2024 và 1023, bằng cách truy ngược lại từ thuật toán Euclid ở câu trên:
* Ta có:
  + 11 = 1001 – 22 x 45

Tiếp tục thay 22 bằng tổ hợp của 1023 và 1001 như bước trên:

* + 11 = 1001 – (1023 – 1001) x 45 = 1001 x 46 – 1023 x 45

Thay 1001 bằng tổ hợp của 2024 và 1023 từ bước đầu tiên:

* + 11 = (2024 – 1023) x 46 – 1023 x 45 = 2024 x 46 – 1023 x 91

**Từ đó**, chúng ta có 2024 x 46 – 1023 x 91 = 11

Để tìm nghiệm của phương trình 2024x + 1023y = 1, ta chia cả hai vế của phương trình 2024x + 1023y = 1 cho 11:

⬄ 2024 x ( + 1023 x ( = 1

Vì 2 số 46 và 91 đều không chia hết cho 11, do đó ta không thể chia một cách trực tiếp. Ta phải đi tìm nghiệm phù hợp cho phương trình 2024x + 1023y = 1.

Giả sử một nghiệm cơ bản là (x0, y0). Khi đó các nghiệm tổng quát của phương trình 2024x + 1023y = 1 có dạng là:

* x = x0 + 1023k
* y = y0 – 2024k

Với k là một số nguyên bất kỳ. Thay x0 = 46 và y0 = - 91 vào thì ta có nghiệm tổng quát của phương trình là:

* x = 46 + 1023k
* y = -91 – 2024k

Với k là các giá trị nguyên, từ đó ta có thể tạo ra các cặp nghiệm khác nhau:

* k = 0 : (46, -91)
* k = 1 : (1069, -2115)
* k = 2 : (2092, -4139)
* k = 3 : (3115, -6163)
* k = 4 : (4138, -8187)

Vậy các nghiệm của phương trình 2024x + 1023y = 1 là tất cả các cặp số nguyên có dạng: (x,y) = (46 + 1023k, -91 – 2024k) với k∈Z.

## **Câu 2: Recurrence relation**

* **Student ID: 52200023 → m = 23**
* *an = 8.an−1 – 15.an−2*
* Với *a0 = 5* and *a1 = 23*
* Phương trình đặc trưng của chuỗi đệ quy là:
* Giải phương trình Đặc trưng để tìm ra các giá trị của t:

Phương trình được phân tích thành: (t – 3)(t – 5) = 0

Do đó, các giá trị của t là: t = 3 hoặc t = 5

→ *an =*

Ta có:

*=*

*=*

⬄ *=*

⬄ *=*

⬄ C = 1 và D = 4

**Vì vậy**, ***an =***

## **Câu 3: Set**

### **Tạo tập hợp**

* Họ và tên đầy đủ và in hoa là: HUYNH HOANG TIEN DAT
* 11 ký tự được sử dụng để tạo ra được tên, vì vậy độ dài của Γ là 11
* Γ={A,D,E,G,H,I,N,O,T,U,Y}

### **Tìm Union, intersect, non-symmetric difference, and symmetric**

1. Γ∪Δ={A,D,E,G,H,I,N,O,T,U,Y}∪{A,C,D,G,H,L,N,Q,R,U}

={A,C,D,E,G,H,I,L,N,O,Q,R,T,U,Y}

1. Γ∩Δ={A,D,E,G,H,I,N,O,T,U,Y}∩{A,C,D,G,H,L,N,Q,R,U}

={A,D,G,H,N,U}

1. ΓΔΔ=({A,D,E,G,H,I,N,O,T,U,Y}∖{A,C,D,G,H,L,N,Q,R,U})∪({A,C,D,G,H,L,N,Q,R,U}∖{A,D,E,G,H,I,N,O,T,U,Y})

=({E,I,O,T,Y})∪({C,L,Q,R})

={C,E,I,L,O,Q,R,T,Y}

1. ΓΔΔ=({A,D,E,G,H,I,N,O,T,U,Y}∖{A,C,D,G,H,L,N,Q,R,U})∪({A,C,D,G,H,L,N,Q,R,U}∖{A,D,E,G,H,I,N,O,T,U,Y})

=({E,I,O,T,Y})∪({C,L,Q,R})

={C,E,I,L,O,Q,R,T,Y}

## **Câu 4: Relation**

* **Student ID: 52200023 => m = 23**
* ∀a, b ∈ N (aRb↔23| (a.b))

1. **R phản xạ:** Để chứng minh R phản xạ, cần chứng minh rằng:

Với mọi 𝑎 ∈N, aRa

Theo định nghĩa của R, điều này có nghĩa là:

Với mọi 𝑎 ∈N, 23| (a.a)

⬄Với mọi 𝑎 ∈N, 23| ()

điều này sai vì:

"∀a ∈" "N,nếu 23 ∤ a thì 23 ∤ " )

"Ví dụ: nếu 23 ∤ 1 thì 23 ∤ ")

**Do đó R có không tính phản xạ.**

1. **R đối xứng:** Để chứng minh R đối xứng, cần chứng minh rằng:

Với mọi a, b ∈ Z, nếu a R b thì b R a

Theo định nghĩa của R, điều này có nghĩa là:

Với mọi a,b Z , nếu 23 |(a.b) thì 23| (b.a)

Điều này đúng vì a.b = b.a theo commutative law of multiplication F1(A-1 Epp)

**Do đó R đối xứng.**

1. **R phản đối xứng:** Để R phản đối xứng có nghĩa là:

Với mọi số nguyên a và b thuộc N, nếu 23|(a.b) và 23|(b. a) thì a = b.

Phản ví dụ sau đây cho thấy điều này là sai.

**R không phản đối xứng.**

1. **R mang tính bắc cầu:** R mang tính bắc cầu khi và chỉ khi câu lệnh sau đúng:

Với mọi x, y, z R, nếu xRy và yRz thì xRz.

Theo định nghĩa của R, điều này có nghĩa là:

Với mọi x, y, z R, nếu 23 |(a.b) và 23 |(b.a) thì 23 |(a.c).

* 23 ∤ (ac) => **R không có tính bắc cầu.**

Example: a = 1, b = 23, c = 24 =>

## **Câu 5: Kruskal’s algorithm**

## **Câu 6: Eulerian circuit**

Đồ thị có chu trình Euler khi:

• Tất cả các đỉnh có bậc khác 0 đều được kết nối.

• Tất cả các đỉnh đều có bậc chẵn.

Đồ thị có đường đi Euler khi:

• Tất cả các đỉnh có bậc khác 0 đều được kết nối.

• Có 0 hoặc 2 đỉnh có thể có bậc chẵn.

Đồ thị sau có chu trình Euler vì:

• Tất cả các đỉnh đều được kết nối.

• {A,B,C,D} có 6 độ.

• {E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, a, b, c, d, e, f, g, h, i, j, k, l, m, n} có 4 độ.

b. Nghiên cứu và trình bày kiến ​​thức về thuật toán Hierholzer để tìm chu trình Euler.

**Bước 1**: Đảm bảo rằng đồ thị được kết nối và chứa chính xác 0 hoặc 2 đỉnh bậc lẻ.

**Bước 2:** Khởi tạo 2 ngăn xếp

+ cpath: sẽ lưu trữ đường dẫn Euler Path tạm thời.

+ epath: sẽ lưu giữ đường dẫn Euler cuối cùng.

**Bước 3**: Gọi v là đỉnh bắt đầu rồi đẩy v tới cpath.

+ Nếu có 2 đỉnh bậc lẻ thì một trong số đó phải là v.

+ Nếu mọi đỉnh đều có bậc chẵn thì mọi đỉnh đều có thể là v.

**Bước 4**: Giả sử u là phần tử top-cpath.

**Bước 5**: Nếu tất cả các cạnh của u đã được thăm, đẩy u từ cpath tới epath. Khác: chọn bất kỳ cạnh ngẫu nhiên nào (u, x). Sau đó đẩy x vào cpath và xóa (u,x) khỏi G.

Bước 6: Lặp lại cho đến khi cpath trống.

\*Lưu ý rằng: Đường đi có thể bao gồm hoặc không bao gồm tất cả các cạnh. Do đó, nếu điểm đầu cũng là điểm cuối thì ta có được chu trình Euler bằng cpath nghịch đảo.

1. **Eulerian circuit.**

**Link :** [**https://drive.google.com/file/d/1PvCu8pcPx3Ic41E-8BWsq5zn3caa8c8k/view?usp=sharing**](https://drive.google.com/file/d/1PvCu8pcPx3Ic41E-8BWsq5zn3caa8c8k/view?usp=sharing)

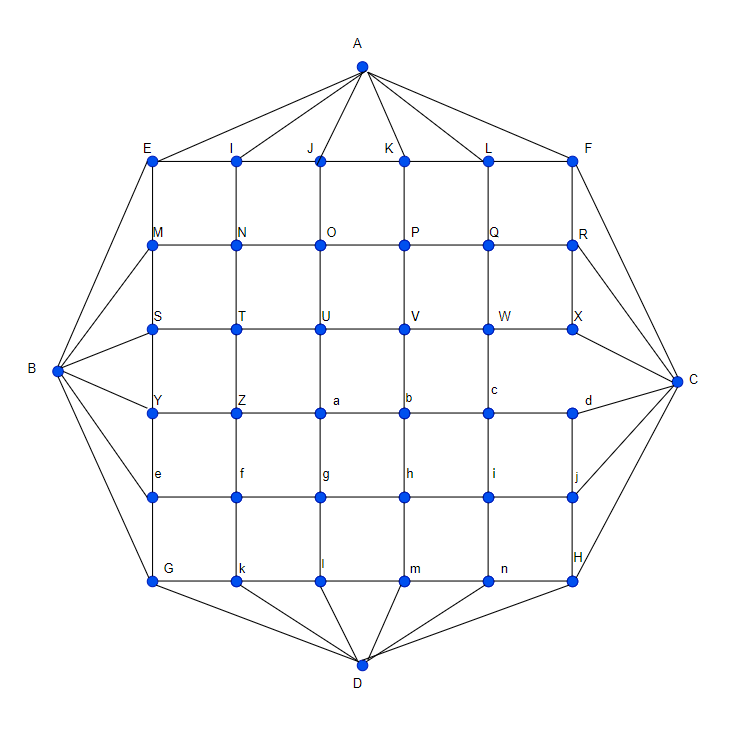
Bốn chữ số cuối cùng của ID sinh viên là 0023 thì abcd % 4 = 23 % 4 = 3

⇒ thì R1 là XCdX

Mạch ban đầu có 3 cạnh XC, Cd, dX. Do đó, để rõ ràng, tôi sẽ xóa

3 cạnh này của đồ thị. Mạch Euler bắt đầu bằng X và sử dụng

Thuật toán Hierholzer’s để xây dựng nó



**Giai đoạn 1: Bắt đầu với các cạnh bên ngoài**

Để làm cho quá trình có thể theo dõi được, tôi sẽ bắt đầu từ các đỉnh bên ngoài và đi ngang qua các đỉnh bên trong những cái sau. Bắt đầu 2 ngăn xếp cpath và epath. Vertex X là điểm khởi đầu :

**cpath = [], epath = []**

**Giai đoạn 1- Phần 1**

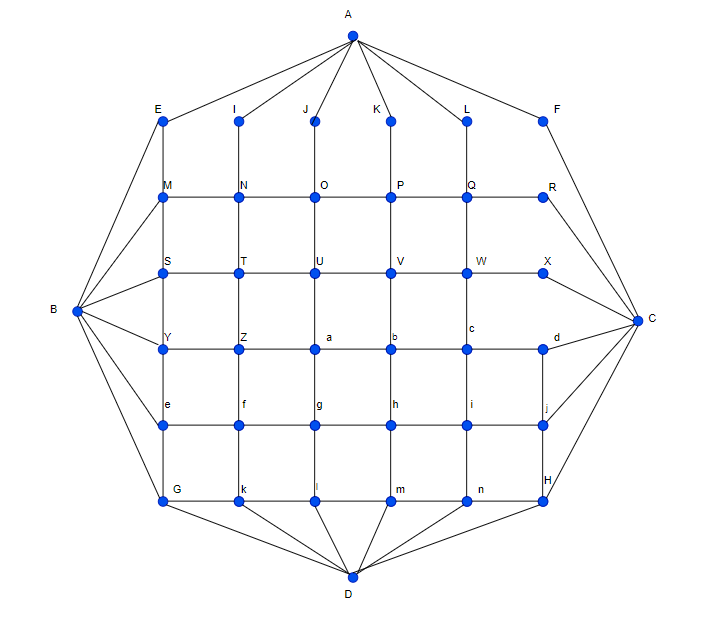
* Về phía bắc của X, đẩy X, R, F tới cpath và lần lượt xóa các cạnh XR và FR.

cpath = [X, R, F]

* Quay về bên trái đỉnh F, đẩy thẳng 5 đỉnh L, K, J, I, E liên tiếp vào cpath. Xóa 5 cạnh tương ứng FL, LK, KJ, JI, IE

cpath = [X, R, F, L, K, J, I, E]

Kết quả được thể hiện trong Capture 6c.1



Capture 6c.1

**Giai đoạn 1- Phần 2**

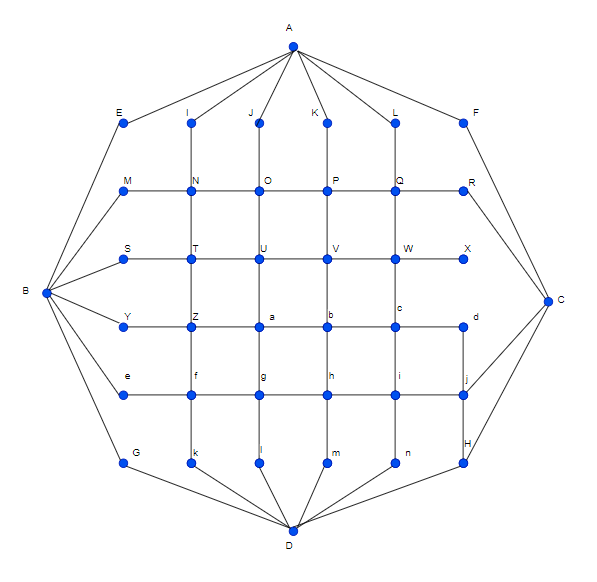
* Tương tự, di chuyển xuống G, lặp lại thao tác tương tự cho các đỉnh M đến đường thẳng đứng. Đẩy 5 đỉnh vào cpath và xóa 5 cạnh

cpath = [X, R, F, L, K, J, I, E, **M, S, Y, e, G**]

* Tiếp theo, đi bên phải G, dọc theo đường thẳng cho đến khi gặp H. Vì hình dạng của đường đi là không khác gì các đỉnh trước nên 5 đỉnh k,l,m,n,H sẽ bị đẩy lên cpath và loại bỏ 5 cạnh giữa chúng.

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, **k, l, m, n, H**]

Kết quả được thể hiện trong Capture 6c.2.

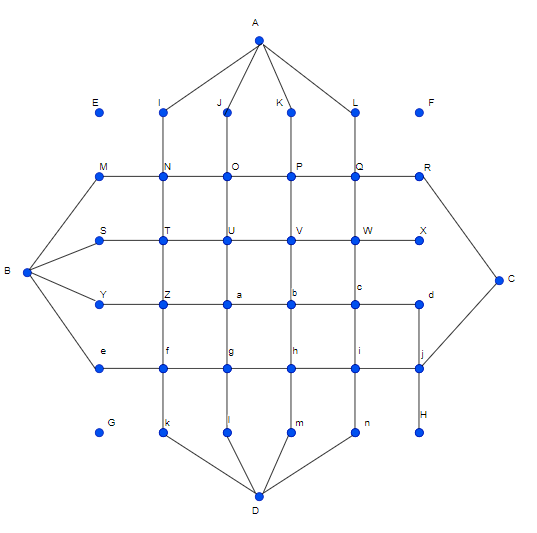
****

## Capture 6c.2

**Giai đoạn 1- Phần 3**

Như đã đề cập ở trên, giai đoạn này sẽ bao phủ các cạnh ngoài trước khi chạm tới các đỉnh bên trong. Rõ ràng, đối với ngoại vi bên ngoài, ta thấy một vòng bát giác được tạo bởi các đỉnh H, C, F, A, E, B, G, D. Đây là lộ trình được chỉ định cho phần cuối của chặng 1. Bằng cách đẩy 8 con đường nào đỉnh (H là điểm cuối) thành cpath và xóa 8 cạnh của vòng, chúng ta nhận được nhiều. Biểu đồ “mỏng hơn” được hiển thị bên dưới qua Capture 7c.3.

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H**, C, F, A, E, B, G , Đ, H**]



**Giai đoạn 2: Lớp đầu tiên của đường dẫn bên trong**

Ở giai đoạn này, các đường đi ngang trông giống như 2 hình lục giác, được minh họa trước bằng nổi bật với màu đỏ và hồng. Chụp 7c.4

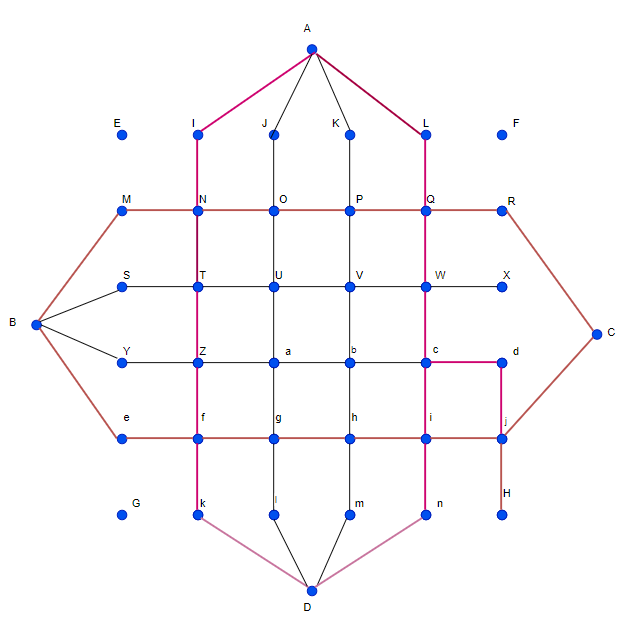
**Giai đoạn 2- Phần 1**

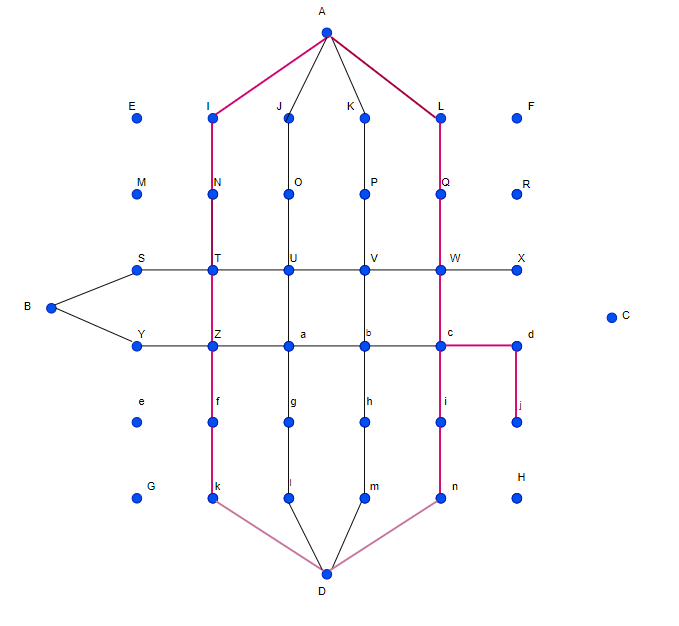
Trước đây chúng ta dừng lại ở đỉnh H. Sau đó, chúng ta sẽ di chuyển dọc theo đường màu đỏ trước tiên. Con đường duy nhất còn lại để bắt đầu từ H là đi lên. ⇒ Đẩy j vào cpath, loại bỏ cạnh Hj.

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H**, j]**

Vì vậy, quy trình cho đường “hình lục giác” nằm ngang màu đỏ là 14 đoạn và chúng ta sẽ di chuyển qua 14 đỉnh, theo chiều kim đồng hồ hoặc ngược chiều kim đồng hồ đều được chấp nhận. Tại thời điểm, đỉnh j là điểm bắt đầu và tôi chọn di chuyển ngược chiều kim đồng hồ. Sau đó mười hai các đỉnh theo thứ tự sẽ là C, R, Q, P, O, N ,M ,B, e, f, g, h, i, j. Và xóa 14 cạnh “đỏ” giữa chúng.

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H, j, C, **R, Q, P, O, N ,M,B, e, f, g, h, i, j**]

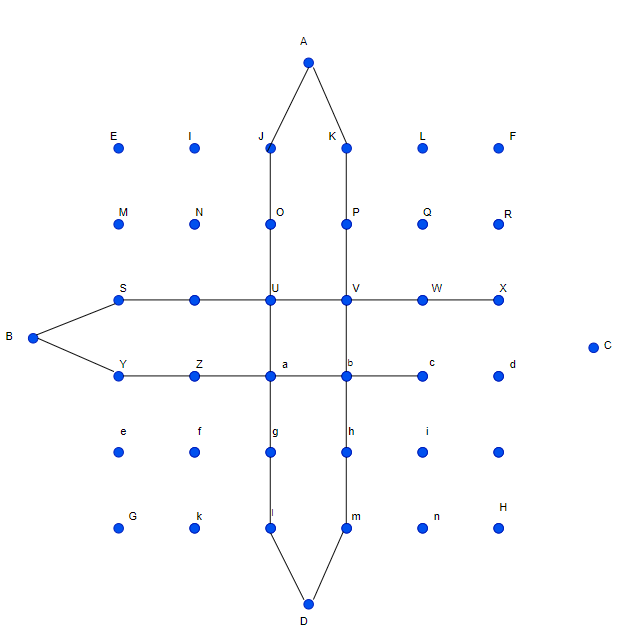




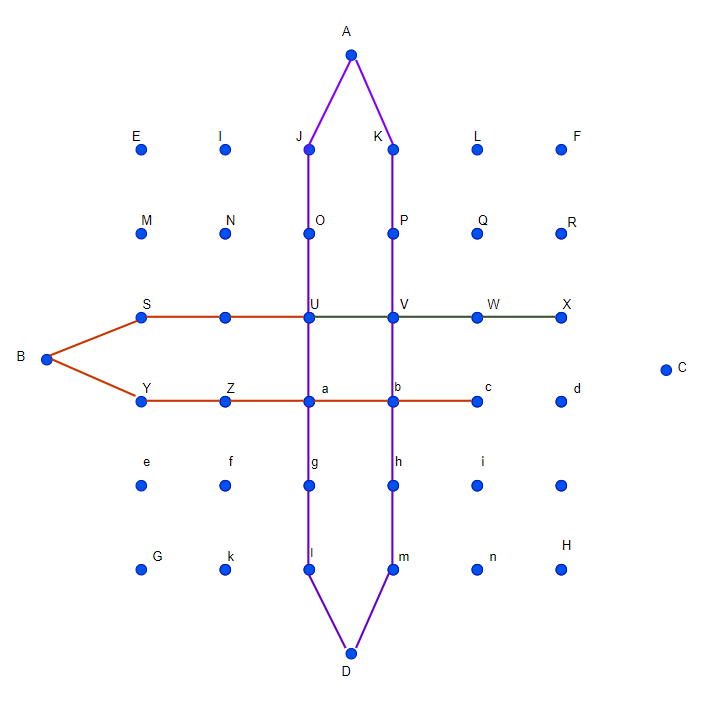
**Giai đoạn 2- Phần 2**

Chỉ cần đi ngang theo đường lục giác màu hồng. Tuyến đường có tổng cộng 14 cạnh + 2 cạnh. Đẩy d và c đến cpath trước. Lần này cũng di chuyển ngược chiều kim đồng hồ. Tóm lại, 16 đỉnh được đẩy để xếp chồng lên nhau.

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H, j, C, R, Q, P, O, N ,M ,B, e, f, g, h, i, j, **d, c, W, Q, L, A, I, N, T, Z, f, k, D, n, i, c**]



**Giai đoạn 3: Con đường cuối cùng**



Đây là bước cuối cùng trong số các bước cuối cùng, hiện ở đỉnh c, để đến X, chỉ cần làm theo 3 phần của tuyến đường theo thứ tự cam, tím và xanh lục

Sau con đường màu cam

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H, j, C, R, Q, P, O, N ,M ,B, e, f, g, h, i, j, d, c, W, Q, L, A, I, N, T, Z, f, k, D, n, i, c**, b, a, Z, Y, B, S, T, U**]

Sau con đường màu tím

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H, j, C, R, Q,P, O, N ,M ,B, e, f, g, h, i, j, d, c, W, Q, L, A, I, N, T, Z, f, k, D, n, i, c, b, a, Z, Y, B, S, T, U, **a, g, l, D, m, h, b, V, P, K, A, J, O, U**]

Sau con đường xanh

cpath = [X, R, F, L, K, J, I, E, M, S, Y, e, G, k, l, m, n, H, C, F, A, E, B, G , D, H, j, C, R, Q, P, O, N ,M ,B, e, f, g, h, i, j, d, c, W, Q, L, A, I, N, T, Z, f, k, D, n, i, c, b, a, Z, Y, B, S, T, U, a, g, l, D, m, h, b, V, P, K, A, J, O, U, **V, W, X]**

Lúc này X không còn con đường nào để di chuyển. Chúng tôi bắt đầu pop cpath và đẩy từng cái một đến đường dẫn.

epath = [X, W, V, U, O, J, A, K, P, V, b, h, m, D, l, g, a, U, T, S, B, Y, Z, a , b, c, i, n, D, k, f, Z, T, N, I, A, L, Q, W, c, d, j, i, h, g, f, e, B, M, N, O, P, Q, R, C, j, H, D, G, B, E, A, F, C, H, n, m, l,k, G, e, Y, S, M, E, I, J, K, L, F, R, X]

Đường epath là một chu trình Euler trong đồ thị đã cho.

## **Câu 7: Map coloring**

* Đường dẫn cho đồ thị được vẽ và tô màu: [*https://drive.google.com/file/d/1eTVNapT1wiCUm8hdNKN9WDpPLgdVxY28/view?usp=sharing*](https://drive.google.com/file/d/1eTVNapT1wiCUm8hdNKN9WDpPLgdVxY28/view?usp=sharing)

### **Vẽ đồ thị**

A map of a network

Description automatically generated

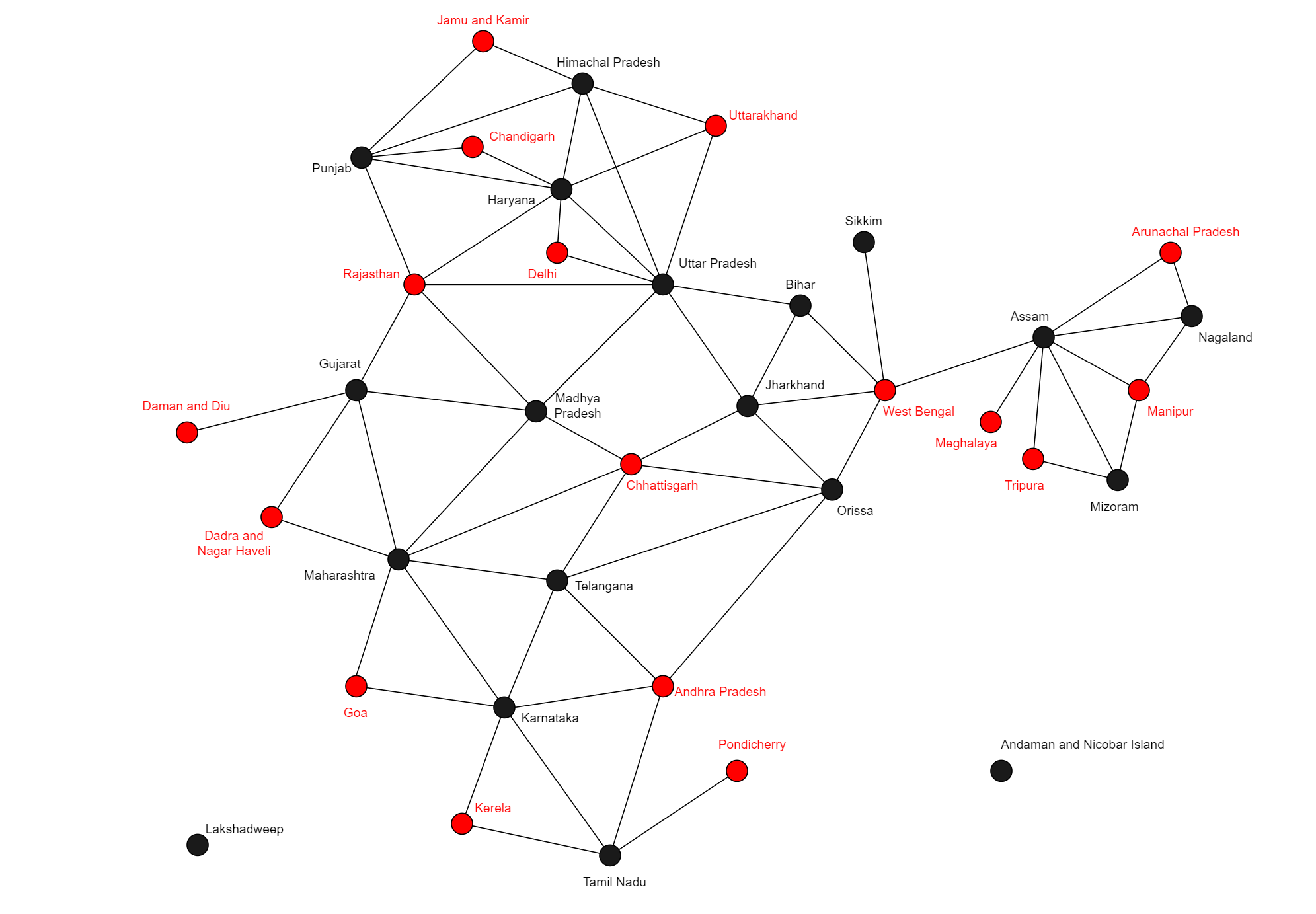
*Hình 1.0.1: Đồ thị Graph Map*

### **Tô màu đồ thị**

* + Giai đoạn 1: Tô màu với màu thứ nhất là màu Đỏ
  + Giai đoạn 2: Tô màu với màu thứ hai là màu Xanh dương
  + Giai đoạn 3: Tô màu với màu thứ ba là màu Xanh lá cây (Xanh lục)
  + Giai đoạn 4: Tô màu với màu thứ tư là màu Tím

*Giải thích:*

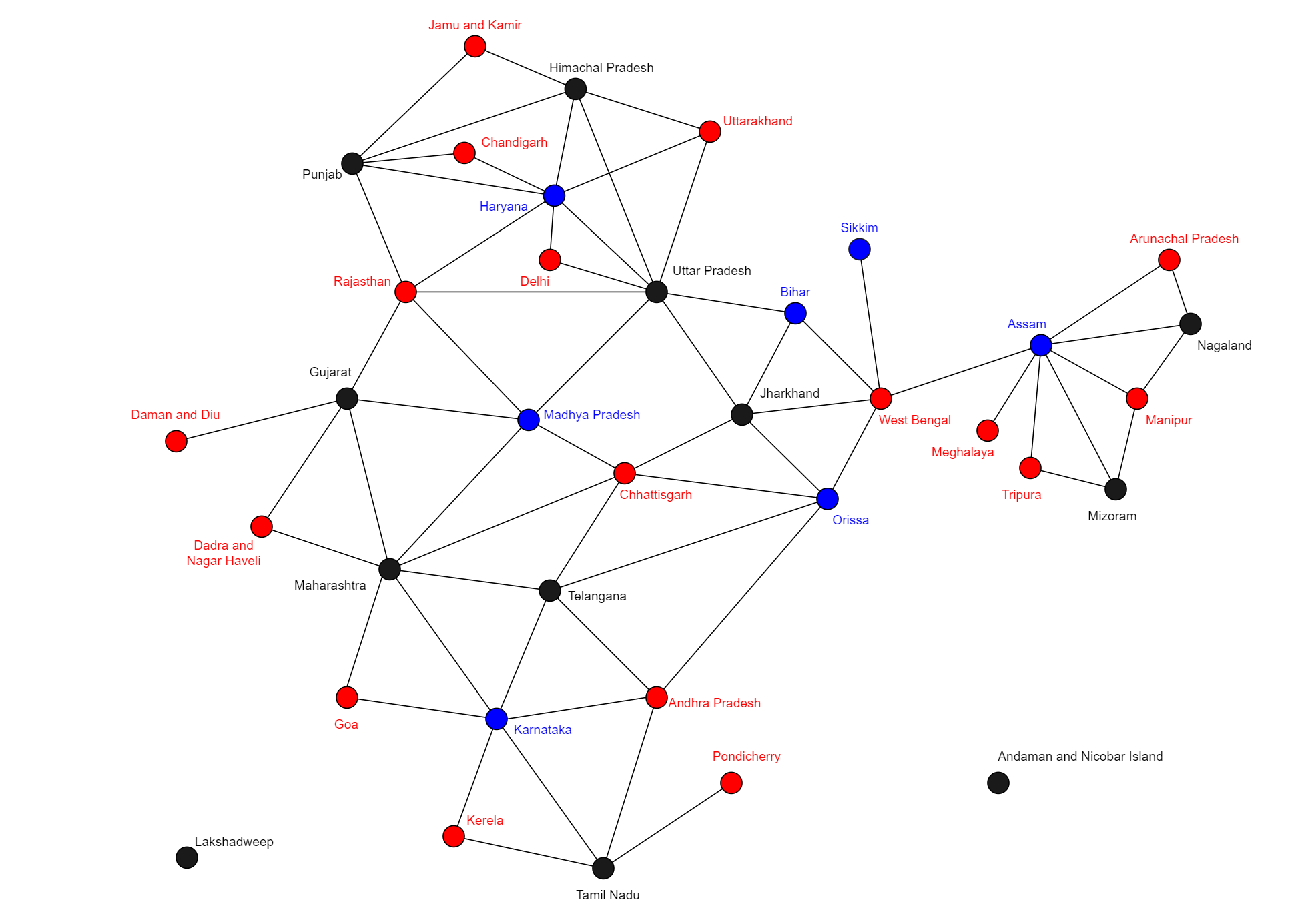
**Giai đoạn 1: Màu được tô là màu đỏ, bắt đầu từ Meghalaya**



*Hình 1.0.2: Đồ thị được tô màu Đỏ tại 17 bang*

* Có 17 bang được tô màu đỏ là: Meghalaya, Arunachal Pradesh, Manipur, Tripura, West Bengal, Chhattisgarh, Andhra Pradesh, Pondicherry, Kerala, Goa, Daman and Diu, Dadra and Nagar Haveli, Rajasthan, Delhi, Chandigarh, Jammu and Kashmir, Uttarakhand.
* Vì Mã số sinh viên là 52200023 với bốn chữ số cuối ID sinh viên là 0023 thì abcd % 4 = 23 % 4 = 3. Vì thế sẽ bắt đầu từ Meghalaya.
* Bắt đầu từ Meghalaya, em sẽ lần lượt đi từ Đông sang Tây. Quy tắc là các vùng nào có chung ranh giới thì sẽ không cùng màu. Nói cách khác, đặc biệt với bối cảnh của đồ thị thì những đỉnh có chung một cạnh với nhau sẽ không được sử dụng cùng một màu.
* Đầu tiên, ta sẽ bắt đầu với phía Đông của bản đồ thị, một khi Meghalaya đã là điểm bắt đầu thì Assam sẽ không thể tô cùng màu. Vì vậy, ta sẽ chọn Arunachal Pradesh, Manipur và Tripura để sơn cho chúng màu đỏ vì chúng cách nhau một đỉnh. Ngoài ra, Tây Bengal là hàng xóm, nằm sát bên của Assam, vậy nên nó cũng có thể có màu đỏ.
* Tiếp theo, chúng ta đã có 5 màu đỏ rồi, và West Bengal có màu đỏ, do đó có bang Bihar, Jharkhand, Orissa sẽ bị bỏ qua trong màu tiếp theo. Em chọn Chhattisgarh và Andhra Pradesh sẽ là hai vùng được tô màu đỏ tiếp theo ở phía Nam, nơi tạo ra nền tảng rào cản cho những quyết định tiếp theo.
* Tiếp theo là Pondicherry, Kerala, Goa, Daman and Diu, Dadra and Nagar Haveli là năm khu vực tiếp theo được tô màu đỏ vì Gujarat, Maharashtra, Karnataka, Tamil Nadu kết nối với Chhattisgarh và Andhra Pradesh.
* Cuối cùng, ở phía trên của biểu đồ, Rajasthan, Delhi, Chandigarh, Jammu and Kashmir và Uttarakhand lần lượt được chọn để tô cùng một màu.

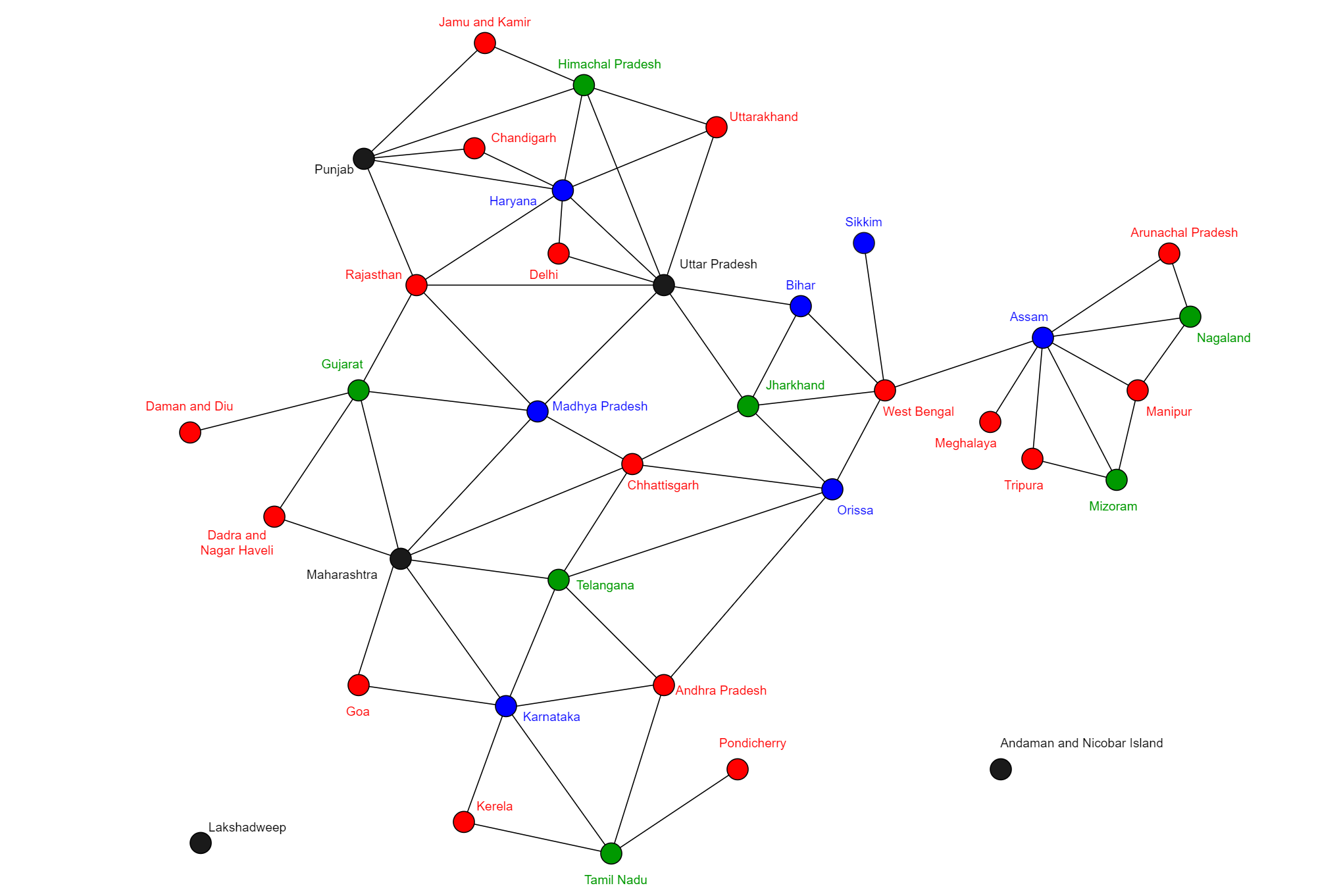
**Giai đoạn 2: Màu được tô là màu Xanh dương**



*Hình 1.0.3: Đồ thị được tô màu Xanh dương tại 7 bang tiếp theo*

* 7 bang được tô màu Xanh dương là: Assam, Sikkim, Bihar, Orissa, Karnataka, Madhya Pradesh, Haryana.
* Lần này, em sẽ bắt đầu tô màu Xanh dương cho cái tên mà đã rơi ra từ lần trước đó là Assam. Ngoài ra, hàng xóm của West Bengal chưa có màu nên 3 bang Sikkim, Bihar, Orissa vẫn là màu Xanh dương tiếp theo.
* Trong khi đó ở phía giữa chỉ có 2 bang là Karnataka, Madhya Pradesh có khả năng cũng sẽ nhận được màu xanh.
* Kết thúc giai đoạn 2 thì Haryana sẽ là người cuối cùng mang màu Xanh dương.

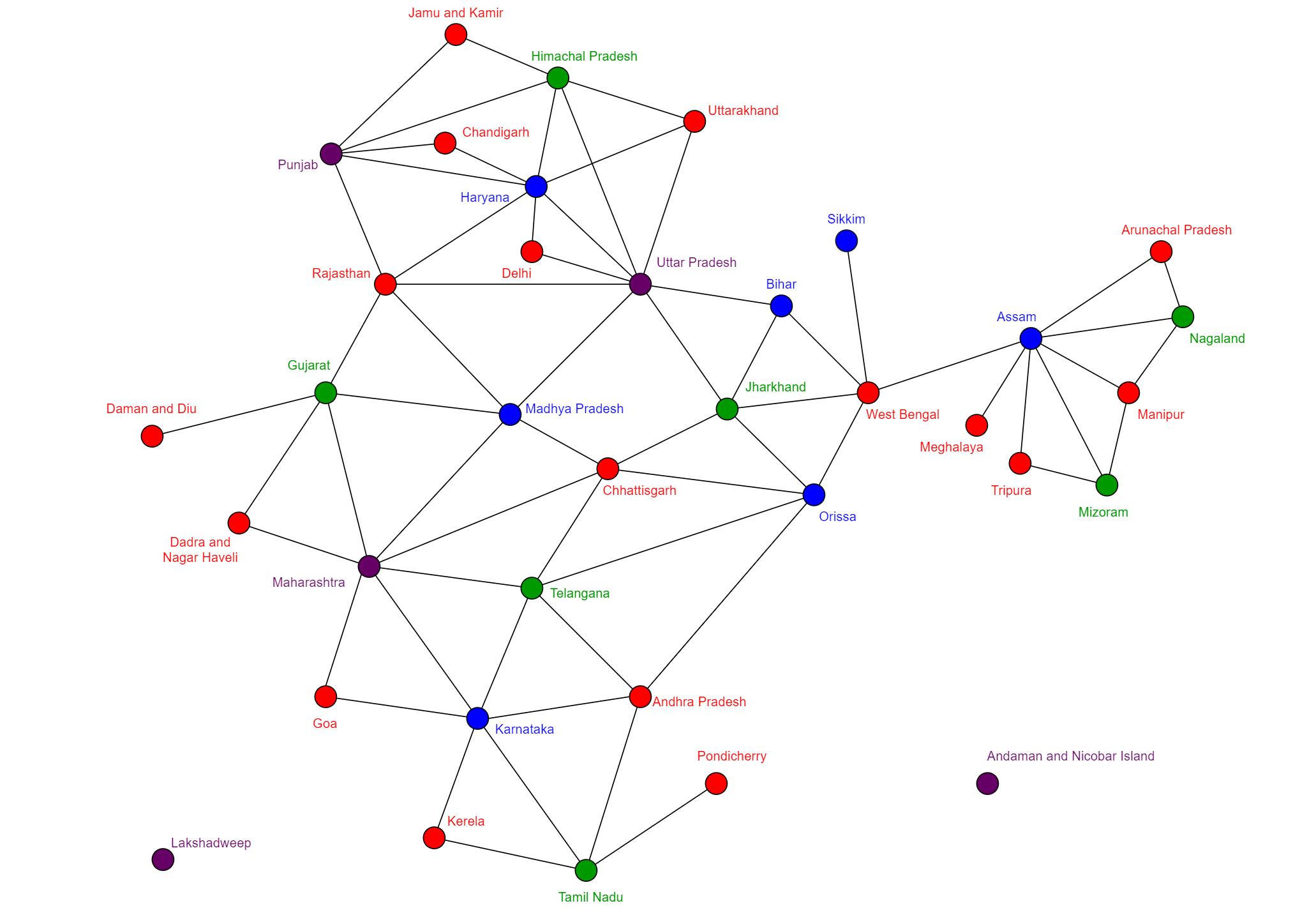
**Giai đoạn 3: Màu được tô là màu Xanh lá cây (Xanh lục)**



*Hình 1.0.4: Đồ thị được tô màu Xanh lá cây tại 7 bang tiếp theo*

* 7 bang được tô màu Xanh lá cây (Xanh lục): Nagaland, Mizoram, Jharkhand, Himachal Pradesh, Gujarat, Telangana,Tamil Nadu
* Nhìn chung, phía Đông đã được dán nhãn màu Xanh dương và Đỏ, nhưng 2 bang Nagaland và Mizoram để lại không có màu. Ngoài ra, chúng cũng không có chung bất kỳ lợi thế nào. Chính vì vậy, 2 bang này sẽ được đánh dấu bằng việc tô màu Xanh lá cây.
* Dường như người hàng xóm cuối cùng của West Bengal là Jharkhand cũng chưa có màu sắc. Vì thế sẽ có thêm 1 màu Xanh lá cây cho bang này.
* Ở giữa bản đồ thị, Gujarat, Telangana và Tamil Nadu vẫn tối và chưa có màu. Tuy nhiên, Maharashtra là một lựa chọn khả thi nhưng nó nằm giữa Gujarat và Telangana. Vì vậy chỉ có ba cái đầu tiên được chuyển sang màu Xanh lá cây.
* Ở phía Bắc thì em chọn Himachal Pradesh là bang cuối cùng có màu Xanh lá cây, bỏ đi Punjab cho màu cuối cùng.

**Giai đoạn 4: Màu được tô là màu Tím**



*Hình 1.5: Đồ thị được tô màu Tím tại 5 bang còn lại*

* 5 bang được tô màu Tím: Punjab, Uttar Pradesh, Maharashtra, Đảo Andaman and Nicobar, Lakshadweep.
* Với tỉ lệ này thì 2 nhóm đảo không được kết nối với biểu đồ. Vì lý do này, nên chúng có thể nhận được màu Tím.
* Ở phía giữa biểu đồ, Uttar Pradesh, Maharashtra là những đỉnh chưa được chạm tới, cộng với đó là chúng không liền kề với cái kia. Nên hai đỉnh này là thực sự phù hợp để có màu Tím.
* Đỉnh cuối cùng chắc chắn được dán nhãn là màu Tím.

## **Câu 8: Finding an Inverse Modulo *n***

**Câu 9: RSA Cryptosystem**

**9.1 Giới thiệu về Hệ mã hóa Bất đối xứng RSA:**

Hệ mã hóa RSA là một trong những cột mốc quan trọng trong lịch sử an ninh thông tin và truyền thông an toàn. Được biết đến với tên viết tắt của ba nhà khoa học máy tính nổi tiếng, Ron Rivest, Adi Shamir và Leonard Adleman, hệ mã hóa này đã mở ra một thế giới mới của tính bảo mật và đáng tin cậy trong việc truyền tải thông tin trên Internet.

Tính chất bất đối xứng của RSA, nơi có một cặp khóa công khai và khóa bí mật, đã giúp nó trở thành một tiêu chuẩn cho việc bảo vệ dữ liệu, xác thực danh tính và tạo chữ ký điện tử.

Bằng cách sử dụng các số nguyên tố lớn và các phép toán modulô, RSA tạo ra các khóa mật mã mạnh mẽ, khó bị phá hủy. Việc sử dụng khóa công khai và khóa bí mật cho phép truyền thông tin một cách an toàn mà không cần phải chia sẻ khóa bí mật giữa hai bên giao tiếp.

Từ các ứng dụng trong thương mại điện tử đến việc bảo vệ thông tin cá nhân trực tuyến, RSA đã chứng minh mình là một công cụ quan trọng trong việc đảm bảo an toàn thông tin trên mạng. Sự phát triển và sự phổ biến của nó thúc đẩy sự tiến bộ trong lĩnh vực an ninh mạng và đảm bảo rằng dữ liệu của chúng ta được bảo vệ một cách hiệu quả và đáng tin cậy.

**Các Khái Niệm Toán Học Cơ Bản**

**Số Nguyên Tố:** Trong RSA, việc chọn hai số nguyên tố lớn, ký hiệu là p và q, là bước đầu tiên và quan trọng nhất. Hai số này phải đủ lớn để đảm bảo độ an toàn của hệ thống. Chúng ta có thể sử dụng bài kiểm tra Miller – Rabin để kiểm tra một số có phải nguyên tố hay không và mức độ tin cậy của số đó có cao hay không.

Giả sử chúng ta chọn hai số nguyên tố lớn là p = 673 và q = 787. Độ lớn của hai con số này đủ để đảm bảo tính an toàn của hệ thống RSA.

**Số Học Mô-đun**: Số học mô-đun là một ngành toán học xử lý các số dư sau phép chia. Các phép toán trong RSA được thực hiện theo mô-đun của một số n, là tích của hai số nguyên tố p và,q. Số này rất quan trọng vì nó được sử dụng trong cả quá trình mã hóa và giải mã.

Ký hiệu của sự đồng dư là a ≡ b(mod m), có nghĩa là a và b có cùng số dư khi chia cho m. Trong RSA, các phép toán mô-đun đảm bảo rằng các giá trị trung gian không trở nên quá lớn và có thể quản lý được trong thực tế tính toán.

Giả sử ta tính n là tích của hai số p và q:

n = p x q = 673 x 787 = 529951

Từ đó số n này sẽ được sử dụng trong quá trình mã hóa và giải mã.

**Thuật Toán Euclide Mở Rộng:** Thuật toán Euclide mở rộng không chỉ tìm ước số chung lớn nhất (GCD) của hai số mà còn tính toán các hệ số Bézout x và y thỏa mãn phương trình ax+by=gcd(a,b). Các hệ số này đóng vai trò quan trọng trong việc giải mã và các ứng dụng mật mã khác.

Trong hệ mật mã RSA, thuật toán Euclide mở rộng được sử dụng để tìm nghịch đảo mô-đun, một yếu tố then chốt trong việc tạo khóa bí mật. Để tìm nghịch đảo của

e theo mô-đun ϕ(n), ta cần tìm d sao cho e⋅d≡1(modϕ(n)). Đây là một trường hợp đặc biệt của phương trình Bézout khi gcd(e,ϕ(n))=1.

Do đó, thuật toán Euclide mở rộng giúp giải quyết phương trình ax+by=GCD(a,b) và tìm nghịch đảo mô-đun d của e, đóng vai trò quan trọng trong việc tạo khóa bí mật RSA.

Giả sử chúng ta muốn tìm nghịch đảo của 𝑒 =17 theo modulo ϕ(n), trong đó ϕ(n) = (p−1)(q−1). Ta sẽ giải phương trình

17x+ϕ(n)y=gcd(17,ϕ(n)):

17x+660y = gcd(17,660)

Sử dụng thuật toán Euclide mở rộng, chúng ta có thể tìm được nghịch đảo của

e=17 là d=389.

**Phân Tích Số Nguyên Tố:** Tính bảo mật của RSA dựa trên độ khó của việc phân tích n (tích của hai số nguyên tố lớn) thành các thừa số nguyên tố của nó. Với các số đủ lớn, việc này hầu như không thể thực hiện được trong thời gian hợp lý bằng các phương pháp hiện tại.

Ví dụ: Với số nguyên tố n=529951, việc phân tích nó thành các thừa số nguyên tố sẽ trở nên rất khó khăn. Đây chính là điểm mạnh của RSA, bởi việc phá vỡ n thành các thừa số nguyên tố là một nhiệm vụ rất khó đối với các phương pháp hiện tại, đặc biệt khi n rất lớn.

**Quá Trình Hoạt Động của RSA**

**Sinh Khóa (Tạo khóa):**

* Chọn hai số nguyên tố lớn p và q.
* Tính toán giá trị n: n = p × q.
* Tính hàm số Euler : ϕ(n) = (p−1)(q−1).
* Chọn số mũ mã hóa e sao cho 1<e<ϕ(n) và gcd(e,ϕ(n)) = 1.
* Tính số mũ giải mã d: d là nghịch đảo mô-đun của e theo mô-đun ϕ(n), tức là d⋅e≡1 (mod ϕ(n)).

**Các thành phần của một Hệ thống khóa trong RSA:**

Hệ mật mã RSA sử dụng hai loại khóa chính là khóa công khai và khóa bí mật. Mỗi loại khóa bao gồm các thành phần khác nhau và có vai trò quan trọng trong quá trình mã hóa và giải mã.

**Khóa Công Khai**

Khóa công khai được chia sẻ rộng rãi và bao gồm hai thành phần chính:

* **n, mô-đun:**
  + n là tích của hai số nguyên tố lớn p và q. Nó được tính bằng cách n=p×q. Mô-đun n là thành phần quan trọng trong cả quá trình mã hóa và giải mã, đảm bảo rằng các giá trị trung gian không trở nên quá lớn.
* **e, số mũ công khai (số mũ mã hóa):**
  + e là số nguyên dương được chọn sao cho nó nguyên tố cùng nhau với ϕ(n) (hàm số Euler của n). Thường thì e sẽ được chọn là các giá trị phổ biến như 3, 17, hoặc 65537 vì chúng đảm bảo hiệu quả tính toán và an toàn. e được sử dụng trong quá trình mã hóa thông điệp.

**Khóa Bí Mật**

Khóa bí mật được giữ kín và chỉ người nhận mới có quyền truy cập. Khóa bí mật bao gồm:

* **n, mô-đun:**
  + n xuất hiện cả trong khóa công khai và khóa bí mật. Nó là thành phần chung, đóng vai trò quyết định trong các phép toán mã hóa và giải mã.
* **d, số mũ bí mật (số mũ giải mã):**
  + d là số nguyên được tính sao cho d×e≡1(modϕ(n)). Nói cách khác, d là nghịch đảo mô-đun của e theo mô-đun ϕ(n). d được sử dụng trong quá trình giải mã thông điệp.

**Chia Sẻ Khóa:**

* Khóa công khai (e,n) được chia sẻ công khai và có thể được bất kỳ ai sử dụng để mã hóa thông điệp.
* Khóa bí mật (d,n) được giữ kín và chỉ người nhận mới có quyền truy cập.

**Mã Hóa:**

* Thông điệp gốc M được chuyển đổi thành một số nguyên m sao cho 0≤m<n.
* Ciphertext c được tính bằng cách: 𝑐=𝑚^e (mod n).

**Giải Mã:**

* Ciphertext c được giải mã bằng khóa bí mật: 𝑚=𝑐^𝑑 (mod n).
* Sau khi giải mã, m được chuyển đổi trở lại thành thông điệp gốc M.

Ví Dụ Cụ Thể:

Giả sử Diệu và Bình muốn gửi một thông điệp là “42” đến cho Đạt sử dụng hệ thống RSA với các tham số đã chọn thì chúng ta sẽ đi qua các bước để minh họa quá trình này như thế này:

1. Chọn số Nguyên Tố:

* Chọn 2 số nguyên tố là p = 61 và q = 53

1. Tính n và ϕ(n):

n = p x q = 61 x 53 = 3233

ϕ(n) = (p – 1) x (q – 1) = (61 – 1) x (53 – 1) = 60 x 52 = 3120

1. Chọn e

* Chọn e = 17 (vì ta có thể tính được gcd(17,3120) = 1)

1. Tính d

* Sử dụng thuật toán Euclide mở rộng để tìm số d sao cho:

d x 17 ≡ 1 (mod 3120)

Chúng ta sẽ thực hiện các bước của một thuật toán Euclide mở rộng:

3120 = 17 x 183 + 9

17 = 9 x 1 + 8

9 = 8 x 1 + 1

8 = 8 x 1 + 0

Từ đó, ta ngược lại để tìm số d:

1 = 9 – 1 x 8

8 = 17 – 1 x 9

1 = 9 – 1 x (17 – 1 x 9) = 2 x 9 – 17

9 = 3120 – 183 x 17

1 = 2 x (3120 – 183 x 17) – 17 = 2 x 3120 – 367 x 17

Do đó, ta có thể suy ra được **d = 2753**

1. Mã hóa:

* Ta đã biết thông điệp gốc là m = 42, ta sẽ tính ciphertext c

c = mod 3233

Quá trình diễn ra phép tính:

≡ 1764 mod 3233 ≡ 1764

≡ mod 3233 ≡ 3111696 mod 3233 ≡ 1550

≡ mod 3233 ≡ 2402500 mod 3233 ≡ 1730

≡ mod 3233 ≡ 2992900 mod 3233 ≡ 2256

≡ 2256 x 42 mod 3233 ≡ 94752 mod 3233 ≡ 256

1. Giải Mã

* Sử dụng khóa bí mật d = 2753, Đạt sẽ tính toán lại thông diệp gốc m:

m = mod 3233

Quá trình tính toán (sử dụng phân rã lũy thừa):

≡ 81796 mod 3233 ≡ 1997

≡ mod 3233 ≡ 3988009 mod 3233 ≡ 717

≡ mod 3233 ≡ 514089 mod 3233 ≡ 1733

≡ mod 3233 ≡ 3000289 mod 3233 ≡ 201

≡ 201 x 1733 x 717 x 1997 x 286 mod 3233 ≡ 42 mod 3233

Vậy thông điệp gốc được khôi phục thành công là: m = 42

Thông qua ví dụ trên. chúng ta đã minh họa chi tiết cách mà hệ thống RSA hoạt động để mã hóa và giải mã một thông điệp, đảm bảo tính bảo mật và tính toàn vẹn của thông tin truyền tải giữa Đạt, Diệu và Bình.

**Một vài Thông Báo Mẫu để Kiểm tra:**

* Message: “Hello, World!”
* Message: “Dat”
* Message: “Dieu”
* Message: “Binh”

**Xác minh kết quả của hệ thống RSA thông qua code Python:**

* Thông điệp mẫu: “Hello, World!”
* Thông điệp mã hóa: [3000, 1313, 745, 745, 2185, 678, 1992, 604, 2185, 2412, 745, 1773, 1853]
* Thông điệp giải mã: “Hello, World!”

A screenshot of a computer

Description automatically generated

Hình 1: Kết quả mã hóa của Message “Hello, World!”

**Giải thích kết quả:**

* Với các số nguyên tố mà ta đã giả sử cố định trong đoạn code: p = 61 và q = 53

1. **Tạo khóa RSA:**

* n = p x q = 61 x 53 = 3233
* ϕ = (p – 1) x (q – 1) = 60 x 52 = 3120
* Và ta cũng đã chọn số nguyên tố cố định cùng nhau với ϕ là e = 65537
* Sau đó, tính d là nghịch đảo của modulo ϕ.
* d = e-1 mod ϕ và khi đó giá trị của d = 2753
* Từ đó, ta có khóa công khai là (ϕ, e) = (65537,3233) và khóa riêng tư là (d, n) = (2753, 3233).

1. **Mã hóa:**

* Đối với mỗi ký tự trong message “Hello, World!” thì nhận thấy:
  + ASCII của ‘H’ là 72, ‘e’ là 101, ‘l’ là 108, ...
  + Mã hóa từng ký tự theo công thức là c = mod n

Phép tính khi mã hóa từng ký tự để cho ra kết quả:

“H” → mã ASCII là 72

* + c1 = mod 3233 = 3000

“e” → mã ASCII là 101

* + c2 = mod 3233 = 1313

“l” → mã ASCII là 108

* + c3 = mod 3233 = 745

“l” → mã ASCII là 108

* + c4 = mod 3233 = 745

“o” → mã ASCII là 111

* + c5 = mod 3233 = 2185

“,” → mã ASCII là 44

* + c6 = mod 3233 = 678

“ ” → mã ASCII là 32

* + c7 = mod 3233 = 1992

“W” → mã ASCII là 87

* + c8 = mod 3233 = 604

“o” → mã ASCII là 111

* + c9 = mod 3233 = 2185

“r” → mã ASCII là 114

* + c10 = mod 3233 = 2412

“l” → mã ASCII là 108

* + c11 = mod 3233 = 745

“d” → mã ASCII là 100

* + c12 = mod 3233 = 1773

“!” → mã ASCII là 33

* + c13 = mod 3233 = 1853

1. **Giải mã**

* Mỗi số trong danh sách được giải mã bằng cách sử dụng khóa riêng tư để tính toán được số nguyên tương ứng.
  + m1 = mod 3233 = 72 → “H”
  + m2 = mod 3233 = 101 → “e”
  + m3 = mod 3233 = 108 → “l”
  + m4 = mod 3233 = 108 → “l”
  + m5 = mod 3233 = 111 → “o”
  + m6 = mod 3233 = 44 → “H”
  + m7 = mod 3233 = 32 → “H”
  + m8 = mod 3233 = 87 → “H”
  + m9 = mod 3233 = 111 → “H”
  + m10 = mod 3233 = 114 → “H”
  + m11 = mod 3233 = 108 → “H”
  + m12 = mod 3233 = 100 → “H”
  + m13 = mod 3233 = 33 → “H”
* Kết quà cuối cùng của cả quá trình giải mã là thông điệp gốc xuất hiện “Hello, World!”
* Thông điệp mẫu: “Dat”
* Thông điệp mã hóa: [1759, 1632, 884]
* Thông điệp giải mã: “Dat”

A screenshot of a computer program

Description automatically generated

Hình 2: Kết quả mã hóa của Message “Dat”

**Giải thích kết quả:**

* Với các số nguyên tố mà ta đã giả sử cố định trong đoạn code: p = 61 và q = 53

1. **Tạo khóa RSA:**

* n = p x q = 61 x 53 = 3233
* ϕ = (p – 1) x (q – 1) = 60 x 52 = 3120
* Và ta cũng đã chọn số nguyên tố cố định cùng nhau với ϕ là e = 65537
* Sau đó, tính d là nghịch đảo của modulo ϕ.
* d = e-1 mod ϕ và khi đó giá trị của d = 2753
* Từ đó, ta có khóa công khai là (ϕ, e) = (65537,3233) và khóa riêng tư là (d, n) = (2753, 3233).

1. **Mã hóa:**

* Đối với mỗi ký tự trong message “Dat” thì nhận thấy:
  + ASCII của ‘D’ là 68, ‘a’ là 97, ‘t’ là 116.
  + Mã hóa từng ký tự theo công thức là c = mod n

Phép tính khi mã hóa từng ký tự để cho ra kết quả:

“D” → mã ASCII là 68

* + c1 = mod 3233 = 1759

“a” → mã ASCII là 97

* + c2 = mod 3233 = 1632

“t” → mã ASCII là 116

* + c3 = mod 3233 = 884

1. **Giải mã**

* Mỗi số trong danh sách được giải mã bằng cách sử dụng khóa riêng tư để tính toán được số nguyên tương ứng.
  + m1 = mod 3233 = 68 → “D”
  + m2 = mod 3233 = 97 → “a”
  + m3 = mod 3233 = 116 → “t”
* Kết quà cuối cùng của cả quá trình giải mã là thông điệp gốc xuất hiện “Dat”
* Thông điệp mẫu: “Dieu”
* Thông điệp mã hóa: [1759, 3179, 1313, 2160]
* Thông điệp giải mã: “Dieu”

A computer screen shot of a number

Description automatically generated

Hình 3: Kết quả mã hóa của Message “Dieu”

**Giải thích kết quả:**

* Với các số nguyên tố mà ta đã giả sử cố định trong đoạn code: p = 61 và q = 53

1. **Tạo khóa RSA:**

* n = p x q = 61 x 53 = 3233
* ϕ = (p – 1) x (q – 1) = 60 x 52 = 3120
* Và ta cũng đã chọn số nguyên tố cố định cùng nhau với ϕ là e = 65537
* Sau đó, tính d là nghịch đảo của modulo ϕ.
* d = e-1 mod ϕ và khi đó giá trị của d = 2753
* Từ đó, ta có khóa công khai là (ϕ, e) = (65537,3233) và khóa riêng tư là (d, n) = (2753, 3233).

1. **Mã hóa:**

* Đối với mỗi ký tự trong message “Dieu” thì nhận thấy:
  + ASCII của ‘D’ là 68, ‘i’ là 105, ‘e’ là 101, ‘u’ là 117
  + Mã hóa từng ký tự theo công thức là c = mod n

Phép tính khi mã hóa từng ký tự để cho ra kết quả:

“D” → mã ASCII là 68

* + c1 = mod 3233 = 1759

“a” → mã ASCII là 105

* + c2 = mod 3233 = 3179

“t” → mã ASCII là 101

* + c3 = mod 3233 = 1313

“t” → mã ASCII là 117

* + c4 = mod 3233 = 2160

1. **Giải mã**

* Mỗi số trong danh sách được giải mã bằng cách sử dụng khóa riêng tư để tính toán được số nguyên tương ứng.
  + m1 = mod 3233 = 68 → “D”
  + m2 = mod 3233 = 105 → “i”
  + m3 = mod 3233 = 101 → “e”
  + m4 = mod 3233 = 117 → “u”
* Kết quà cuối cùng của cả quá trình giải mã là thông điệp gốc xuất hiện “Dieu”
* Thông điệp mẫu: “Binh”
* Thông điệp mã hóa: [524, 3179, 2235, 2170]
* Thông điệp giải mã: “Binh”

A screenshot of a computer

Description automatically generated

Hình 4: Kết quả của mã hóa Message “Binh”

**Giải thích kết quả:**

* Với các số nguyên tố mà ta đã giả sử cố định trong đoạn code: p = 61 và q = 53

1. **Tạo khóa RSA:**

* n = p x q = 61 x 53 = 3233
* ϕ = (p – 1) x (q – 1) = 60 x 52 = 3120
* Và ta cũng đã chọn số nguyên tố cố định cùng nhau với ϕ là e = 65537
* Sau đó, tính d là nghịch đảo của modulo ϕ.
* d = e-1 mod ϕ và khi đó giá trị của d = 2753
* Từ đó, ta có khóa công khai là (ϕ, e) = (65537,3233) và khóa riêng tư là (d, n) = (2753, 3233).

1. **Mã hóa:**

* Đối với mỗi ký tự trong message “Binh” thì nhận thấy:
  + ASCII của ‘B’ là 66, ‘i’ là 105, ‘n’ là 110, ‘h’ là 104
  + Mã hóa từng ký tự theo công thức là c = mod n

Phép tính khi mã hóa từng ký tự để cho ra kết quả:

“D” → mã ASCII là 66

* + c1 = mod 3233 = 524

“a” → mã ASCII là 105

* + c2 = mod 3233 = 3179

“t” → mã ASCII là 110

* + c3 = mod 3233 = 2235

“t” → mã ASCII là 104

* + c4 = mod 3233 = 2170

1. **Giải mã**

* Mỗi số trong danh sách được giải mã bằng cách sử dụng khóa riêng tư để tính toán được số nguyên tương ứng.
  + m1 = mod 3233 = 66 → “B”
  + m2 = mod 3233 = 105 → “i”
  + m3 = mod 3233 = 110 → “n”
  + m4 = mod 3233 = 104 → “h”
* Kết quà cuối cùng của cả quá trình giải mã là thông điệp gốc xuất hiện “Binh”

**Phân tích Hiệu quả và Tính bảo mật của hệ thống RSA:**

**Hiệu quả**

1. **Kích thước khóa**:

* Trong các thông điệp mẫu này, chúng ta sử dụng các số nguyên tố nhỏ (p = 61, q = 53) và khóa có độ dài 8 bit để đơn giản hóa tính toán và minh họa.
* Trong thực tế, RSA thường sử dụng các số nguyên tố lớn (2048 bit hoặc lớn hơn) để đảm bảo an toàn, điều này làm tăng đáng kể thời gian tính toán cho cả mã hóa và giải mã.

1. **Hiệu suất mã hóa và giải mã:**

* Mã hóa bằng RSA thường nhanh hơn giải mã vì số mũ e (thường là 65537) nhỏ hơn nhiều so với d.
* Giải mã chậm hơn vì d thường rất lớn (trong ví dụ này, d = 2753), đòi hỏi nhiều phép tính mô đun hơn.

1. **Quá trình mã hóa và giải mã với các thông điệp mẫu:**

* Thông điệp mẫu "Binh" và các thông điệp khác đã được mã hóa và giải mã đúng cách.
* Các bước mã hóa và giải mã sử dụng phép tính số mũ mô đun, có thể thực hiện hiệu quả với các thuật toán tối ưu như Thuật toán Bình phương và Nhân.

Qua đó cho thấy hệ thống RSA hoạt động hiệu quả trong việc mã hóa và giải mã các thông điệp nhỏ. Các phép toán mã hóa và giải mã của RSA chủ yếu dựa vào phép lũy thừa modulo, đây là các phép toán tương đối nhanh với các số nguyên nhỏ và trung bình. Trong các ví dụ trên, việc mã hóa và giải mã các thông điệp mẫu như “Hello, World!”, "Dat", "Dieu", và "Binh" được thực hiện khá nhanh chóng.

Tuy nhiên, khi kích thước của khóa (cặp số nguyên tố p và q) tăng lên để đảm bảo an toàn, các phép toán này trở nên phức tạp và tốn thời gian hơn. Ví dụ, việc mã hóa và giải mã với các khóa 2048 bit hoặc 4096 bit sẽ tốn nhiều thời gian và tài nguyên hơn.

**Tính Bảo Mật**

1. **Kích thước khóa và số nguyên tố**:

* Với p = 61 và q = 53, n = 3233, các số này quá nhỏ để đảm bảo an toàn.
* Trong thực tế, sử dụng các số nguyên tố lớn hơn (2048 bit hoặc lớn hơn) để đảm bảo an toàn.

1. **Khóa công khai và khóa riêng tư**:

* Khóa công khai (e = 65537, n = 3233) và khóa riêng tư (d = 2753, n = 3233) được tạo ra chính xác.
* Số e thường được chọn là 65537 vì nó là số nguyên tố nhỏ, giúp tăng hiệu quả mã hóa mà không ảnh hưởng đến bảo mật.

1. **Khả năng tấn công**:

* **Tấn công thô bạo (Brute-force)**: Với kích thước khóa nhỏ, kẻ tấn công có thể thử tất cả các cặp số nguyên tố có thể để tìm p và q, từ đó tính toán d. Điều này không thực tế với kích thước khóa lớn (2048 bit hoặc lớn hơn).
* **Tấn công phân tích nhân tử (Factoring Attack)**: Bảo mật RSA dựa trên tính khó khăn của việc phân tích nhân tử số lớn n. Với n nhỏ như trong ví dụ này, việc phân tích nhân tử khá đơn giản. Tuy nhiên, với các giá trị n lớn, việc này trở nên rất khó khăn.
* **Tấn công dựa trên khóa công khai (Public Key Attack)**: Kẻ tấn công có thể sử dụng khóa công khai để mã hóa và giải mã thử cho đến khi tìm được khóa riêng tư. Điều này trở nên khó khăn với các khóa công khai lớn.

1. **Tính bảo mật với thông điệp mẫu**:

* Các thông điệp mẫu "Dat", "Dieu", và "Binh" đã được mã hóa và giải mã chính xác.
* Tuy nhiên, với khóa nhỏ như đã sử dụng, hệ thống không an toàn trước các tấn công thô bạo và phân tích nhân tử.

**Mối đe dọa bảo mật tiềm ẩn**

**Tấn công nhân tử (Factoring Attack):**

Bảo mật của RSA phụ thuộc vào tính khó khăn của việc phân tích một số lớn n thành hai số nguyên tố p và q. Nếu kẻ tấn công có thể phân tích n, họ có thể tính được ϕ (n) và khóa riêng tư d, từ đó giải mã mọi thông điệp mã hóa bằng khóa công khai. Các thuật toán như Quadratic Sieve và General Number Field Sieve (GNFS) là các phương pháp hiệu quả nhất hiện nay để phân tích nhân tử.

**Tấn công thời gian (Timing Attack):**

Các tấn công dựa trên thời gian phân tích thời gian cần thiết để thực hiện các phép toán mã hóa hoặc giải mã. Kẻ tấn công có thể đo thời gian xử lý và từ đó suy luận ra các bit của khóa riêng. Các tấn công này thường yêu cầu kẻ tấn công có quyền truy cập vật lý hoặc theo dõi từ xa thiết bị thực hiện mã hóa.

**Tấn công kênh bên (Side-Channel Attack):**

Bao gồm các tấn công dựa trên quan sát các yếu tố vật lý như thời gian, điện năng tiêu thụ, bức xạ điện từ, hoặc âm thanh để thu thập thông tin về khóa riêng. Ví dụ, bằng cách đo lường điện năng tiêu thụ trong quá trình mã hóa, kẻ tấn công có thể tái tạo lại các giá trị khóa.

**Tấn công Padding Oracle:**

Xảy ra khi hệ thống RSA không xử lý đúng cách các khối đệm (padding) trong quá trình mã hóa. Kẻ tấn công có thể gửi các khối mã hóa và nhận phản hồi về tính hợp lệ của chúng, từ đó suy luận ra thông tin về khối dữ liệu gốc.

**Tấn công RSA thô bạo (Brute-force RSA Attack):**

Thử tất cả các cặp số nguyên tố có thể để tìm ra p và q. Điều này không thực tế với các khóa lớn nhưng khả thi với các khóa nhỏ. Tấn công thô bạo là phương pháp không khả thi đối với các khóa có kích thước đủ lớn, vì số lượng các cặp số nguyên tố có thể trở nên khổng lồ.

**Tấn công bằng chữ ký giả (Forged Signature Attack):**

Nếu không sử dụng các hàm băm an toàn và giao thức chữ ký số, kẻ tấn công có thể giả mạo chữ ký số. Điều này đòi hỏi sử dụng các hàm băm mật mã an toàn như SHA-256 và các giao thức chữ ký số chuẩn như PKCS#1.

**Những hạn chế của hệ thống mật mã RSA**

**Tính chậm trong giải mã:**

Giải mã bằng RSA thường chậm hơn mã hóa do d lớn hơn nhiều so với e, dẫn đến nhiều phép toán hơn. Điều này ảnh hưởng đến hiệu suất của các hệ thống cần thực hiện nhiều phép giải mã, như các máy chủ web phục vụ HTTPS.

**Yêu cầu về khóa lớn:**

Để đảm bảo an toàn, RSA cần sử dụng các số nguyên tố rất lớn (2048 bit hoặc lớn hơn), làm tăng độ phức tạp và thời gian tính toán. Việc tạo ra và quản lý các khóa lớn cũng đòi hỏi nhiều tài nguyên hơn.

**Không an toàn với dữ liệu lớn:**

RSA không phù hợp để mã hóa trực tiếp các khối dữ liệu lớn. Thay vào đó, RSA thường được sử dụng để mã hóa khóa phiên (session key) của các thuật toán mã hóa đối xứng, như AES. Việc sử dụng RSA trực tiếp để mã hóa dữ liệu lớn có thể dẫn đến vấn đề về hiệu suất và bảo mật.

**Phụ thuộc vào nguồn ngẫu nhiên:**

Quá trình tạo ra các số nguyên tố lớn cần các nguồn ngẫu nhiên chất lượng cao để đảm bảo tính an toàn. Nếu các số nguyên tố không thực sự ngẫu nhiên, RSA có thể bị phá vỡ. Điều này đòi hỏi các hệ thống phải có các bộ tạo số ngẫu nhiên mạnh mẽ và đáng tin cậy.

**Tấn công bởi các tiến bộ trong toán học và điện toán:**

Các tiến bộ trong toán học (ví dụ như thuật toán phân tích nhân tử mới) hoặc sự phát triển của máy tính lượng tử có thể làm suy yếu hoặc phá vỡ RSA. Máy tính lượng tử có khả năng chạy các thuật toán như Shor’s Algorithm, có thể phân tích nhân tử rất nhanh và phá vỡ RSA.

**Khuyến nghị nhằm cải thiện việc triển khai hệ thống mật mã RSA**

**Sử dụng khóa lớn:**

Nên sử dụng các số nguyên tố có kích thước tối thiểu 2048 bit, và tốt hơn là 3072 bit hoặc lớn hơn để đảm bảo an toàn trước các tấn công hiện tại và tương lai. Khóa lớn hơn làm tăng độ khó của việc phân tích nhân tử, nhưng đồng thời cũng tăng yêu cầu về tính toán.

**Sử dụng nguồn ngẫu nhiên chất lượng cao:**

Đảm bảo rằng các số nguyên tố được tạo ra từ các nguồn ngẫu nhiên chất lượng cao để tránh bị tấn công do tính ngẫu nhiên kém. Các bộ tạo số ngẫu nhiên nên tuân thủ các tiêu chuẩn như NIST SP 800-90A/B/C.

**Áp dụng các biện pháp bảo vệ kênh bên:**

Thực hiện các biện pháp bảo vệ kênh bên, bao gồm làm nhiễu điện năng tiêu thụ, thời gian xử lý, và các bức xạ điện từ. Sử dụng các kỹ thuật bảo vệ như thêm nhiễu giả (random noise), che giấu các dấu hiệu thời gian, và kiểm soát kỹ thuật điện năng tiêu thụ để giảm thiểu nguy cơ bị tấn công.

**Sử dụng Padding an toàn:**

Áp dụng các lược đồ padding an toàn như OAEP (Optimal Asymmetric Encryption Padding) để đảm bảo tính an toàn của quá trình mã hóa. OAEP là một kỹ thuật chuẩn bảo vệ chống lại các tấn công padding oracle và làm cho hệ thống RSA an toàn hơn khi sử dụng trong thực tế.

**Kết hợp với mật mã đối xứng:**

Sử dụng RSA để mã hóa khóa phiên của các thuật toán mật mã đối xứng như AES thay vì mã hóa trực tiếp dữ liệu lớn. AES hoặc các thuật toán đối xứng khác hiệu quả hơn trong việc mã hóa các khối dữ liệu lớn, đồng thời tận dụng tính an toàn của RSA để bảo vệ khóa phiên.

**Cập nhật và giám sát định kỳ:**

Thường xuyên kiểm tra và cập nhật các thuật toán bảo mật, phần mềm, và phần cứng để đảm bảo rằng hệ thống luôn sử dụng các tiêu chuẩn bảo mật mới nhất. Điều này giúp ngăn chặn các lỗ hổng bảo mật tiềm ẩn và giảm nguy cơ bị tấn công.

**Sử dụng chữ ký số và chứng thực:**

Áp dụng các giao thức chữ ký số và chứng thực để đảm bảo tính toàn vẹn và xác thực của dữ liệu. Chữ ký số giúp bảo vệ chống lại các tấn công giả mạo và bảo vệ tính toàn vẹn của thông điệp.

**Nâng cao nhận thức và đào tạo bảo mật:**

Đào tạo người dùng và các chuyên gia bảo mật về các nguy cơ bảo mật và các biện pháp phòng ngừa. Nhận thức và kỹ năng về bảo mật là yếu tố quan trọng trong việc duy trì tính an toàn của hệ thống mật mã.

**Chuẩn bị cho sự xuất hiện của máy tính lượng tử:**

Nghiên cứu và chuẩn bị cho các giải pháp mật mã hậu lượng tử (post-quantum cryptography). Các hệ thống mật mã hiện tại, bao gồm RSA, có thể bị phá vỡ bởi máy tính lượng tử trong tương lai. Việc chuẩn bị trước và triển khai các thuật toán mật mã hậu lượng tử sẽ giúp hệ thống duy trì tính an toàn khi máy tính lượng tử trở nên phổ biến.

# **TÀI LIỆU THAM KHẢO**