**TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI**



**KHOA CÔNG NGHỆ THÔNG TIN**

Logo

Description automatically generated

**BÁO CÁO BÀI TẬP**

AN TOÀN BẢO MẬT THÔNG TIN

**Giảng viên: Đỗ Văn Đức**

Sinh viên thực hiện: Nguyễn Thị Ngũ

Mã sinh viên: 191200758

Lớp: CNTT4 – K60

Hà Nội - 2022

Mục lục

[**I.** **Mật mã cổ điển** 3](#_Toc102600790)

[1. Mã hóa đơn chữ 3](#_Toc102600791)

[2. Mã hóa ceasar 4](#_Toc102600792)

[3. Mật mã hoán vị 5](#_Toc102600793)

[4. Mật mã ma trận playfair 6](#_Toc102600794)

[5. Mật mã vigenere 8](#_Toc102600795)

[6. Mật mã vigenere\_Autokey 10](#_Toc102600796)

[**II.** **Lý thuyết số** 11](#_Toc102600797)

[1. Tính lũy thừa modulo bằng hạ bậc 11](#_Toc102600798)

[2. Nghịch đảo modulo – thuật toán euclid mở rộng 11](#_Toc102600799)

[3. Tính lũy thừa modulo sử dụng định lý fermat 12](#_Toc102600800)

[4. Tính nhanh lũy thừa qua biểu diễn nhị phân 13](#_Toc102600801)

[5. Tính lũy thừa modulo bằng định lý euler 13](#_Toc102600802)

[6. Căn nguyên thủy 15](#_Toc102600803)

[7. Logarit rời rạc 15](#_Toc102600804)

[**III.** **Mã hóa hiện đại** 16](#_Toc102600805)

[1. DES 16](#_Toc102600806)

[2. AES 16](#_Toc102600807)

[**IV.** **Mã hóa công khai** 16](#_Toc102600808)

[1. Mã công khai RSA 16](#_Toc102600809)

[2. Trao đổi khóa Diffie-Hellman 17](#_Toc102600810)

1. **Mật mã cổ điển**
2. Mã hóa đơn chữ

Timeline

Description automatically generated

\* Ý tưởng:

- Chuyển đổi bảng chữ cái theo key

- Chuyển các từng ký tự của input sang ký tự mới theo bảng ký tự mới vừa tại ra.

- Giải mã thì làm ngược lại.

1. Mã hóa ceasar

Text

Description automatically generated

\* Ý tưởng:

- Mã hóa: Dịch từng ký tự của input sang phải key đơn vị.

- Giải mã: Dịch từng ký tự của input sang trái key đơn vị.

1. Mật mã hoán vị

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

\* Ý tưởng:

- Mã hóa: Duyệt chuỗi từ đầu đến cuối in ra các ký tự các nhau key lần. Sau mỗi lần lặp dịch vị trí lên 1 đơn vị.

- Giải mã: Tính độ rộng của mảng 2 chiều có độ sâu là key. Duyệt vòng for in ra ký tự của từng hàng.

1. Mật mã ma trận playfair

A picture containing text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

\* Ý tưởng:

- B1: Sử dụng 1 ma trận 5x5, các chữ cái được sắp xếp từ trái qua phải, từ trên xuống dưới.

- B2: Tách từng cặp của input

- B3: Chuyển hóa từng cặp đó dựa vào ma trân trên để tạo output.

1. Mật mã vigenere

Text

Description automatically generated

Text

Description automatically generated

\* Ý tưởng:

- Mã hóa: Tạo khóa bằng cách lặp key cho đến khi khóa có độ dài bằng input. So sánh key với bảng vừa tìm được ta được output.

- Giải mã: Làm ngược lại

1. Mật mã vigenere\_Autokey

Text

Description automatically generated

Text

Description automatically generated

\* Ý tưởng:

- Lấy thêm các ký tự ở input cho vào key để độ dài key bằng input.

Làm tương tự mật mã vigenere.

1. **Lý thuyết số**
2. Tính lũy thừa modulo bằng hạ bậc

Graphical user interface, text

Description automatically generated

\* Ý tưởng:

- Dùng đệ quy để hạ bậc dần bậc xuống mức ta có thể biết luôn được kết quả.

- Điều kiện kết thúc vòng lặp là khi hạ bậc về 1.

- Kết quả trả về là tích của bình phương bậc sau khi hạ và bậc lẻ.

1. Nghịch đảo modulo – thuật toán euclid mở rộng

Text

Description automatically generated

\* Ý tưởng: Euclid mở rộng luôn có dạng ri = Axi + Byi

- Áp dụng công thức sau:

Text

Description automatically generated

Lặp lại cho đến khi ri = 1 hoặc ri = 0.

- Kết quả là yi

1. Tính lũy thừa modulo sử dụng định lý fermat

Text

Description automatically generated with medium confidence

\* Ý tưởng:

- Kiểm tra n có là số nguyên tố không

+ Nếu phải thì kiểm tra xem a và n có là nguyên tố cùng nhau không. Nếu đúng là dạng 1: a^(n-1) mod n = 1 => hạ bậc rồi tính kết quả. Ngược lại là dạng 1: a^n mod n = 1 => hạ bậc rồi tính kết quả.

+ Ngược lại thì hạ bậc bình thường.

1. Tính nhanh lũy thừa qua biểu diễn nhị phân

Text

Description automatically generated

\* Ý tưởng:

- Chuyển hệ số mũ sang số nhị phân rồi lưu vào một mảng

- Tách lũy thừa cần tìm thành tích các lũy thừa có mũ là cơ số mới.

- Tính tích rồi trả về kết quả cần tìm.

1. Tính lũy thừa modulo bằng định lý euler

Text

Description automatically generated

Text

Description automatically generated

\* Ý tưởng:

- B1: Tính phi n

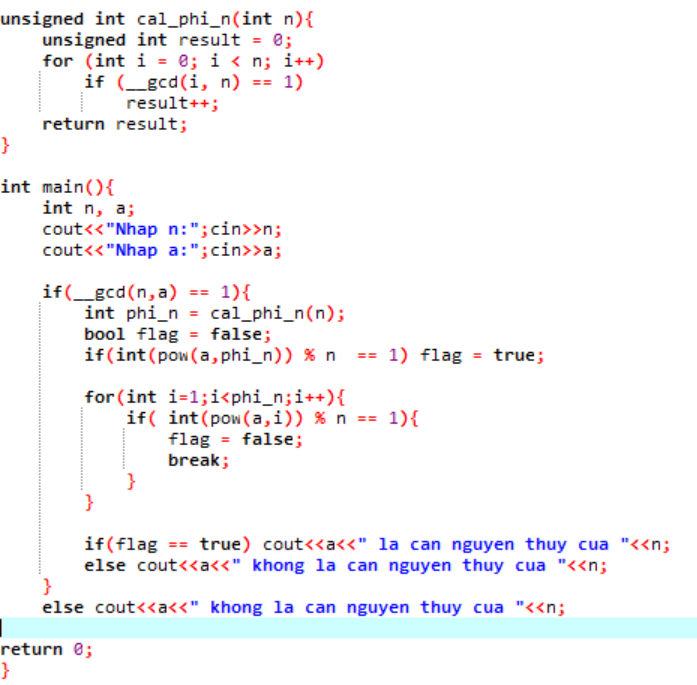
- B2: Kiểm tra xem số chia có phải là số nguyên tố không.

+ Nếu phải thì là dạng 1: hạ bậc mũ về tích của một số với phi-n và cộng phần dư. => Kết quả của bài toán được tính thông qua cách hạ bậc với mũ mới là mũ sau khi hạ.

+ Nếu không thì là dạng 2: hạ bậc mũ về tích của một số với (phi-n+1) và cộng phần dư. => Kết quả của bài toán được tính thông qua cách hạ bậc với mũ mới là mũ sau khi hạ.

B3: Nếu số chia không phải sô nguyên tốt thì hạ trực tiếp.

1. Căn nguyên thủy



\* Ý tưởng:

- Tính phi n. Tạo một biến cờ là false.

- Kiểm tra xem a mũ phi-n có phải là nguyên tố không. Nếu phải thì cờ bằng true.

- Kiểm tra a và các số nhỏ hơn phi-n có là nguyên tố cùng nhau không. Nếu một cái không là nguyên tố cùng nhau thì biến cờ bằng false và thoát vòng for.

- Nếu cờ = true là căn nguyên thủy và ngược lại.

1. Logarit rời rạc

Text

Description automatically generated

\* Ý tưởng:

- Duyệt vòng for kiểm tra xem a^i mod n có cái nào = b không. Nếu có thì in ra i, ngược lại in ra “Không có”.

1. **Mã hóa hiện đại**
2. DES

- Tài liệu sinh 16 khóa: https://www.youtube.com/watch?v=GHPyWDLP0kI

- Tài liệu mã hóa và giải mã: https://www.youtube.com/watch?v=ZQT15md1W5E

1. AES

- Tài liệu mã hóa: <https://www.youtube.com/watch?v=E6FlvjXAQHE>

- Tài liệu giải mã: https://www.youtube.com/watch?v=lGu4hNv9Tsg&t=0s

1. **Mã hóa công khai**
2. Mã công khai RSA

Text

Description automatically generated

\* Ý tưởng:

- Tính n = q \* p và tính phi-n

- Tính d = e ^ -1 mod phi-n

=> Khóa công khai là {e, n} Khóa bí mật là {d, n};

- Mã hóa: Tính c = M^e mod n.

- Giải mã: Tính g = C^d mod n.

1. Trao đổi khóa Diffie-Hellman

Text

Description automatically generated

\* Ý tưởng:

- ya = a ^ xa mod q

- yb = a^xb mod q

- khóa bí mật kAB = yb^xa mod q