**TRƯỜNG ĐẠI HỌC BÁCH KHOA HÀ NỘI**

**BÁO CÁO BÀI 2 – IT4015  
Đề tài: Cài đặt hệ mã dòng Trivium.**

**NGUYỄN TRUNG HIẾU - 20215578**

|  |  |
| --- | --- |
| **Giảng viên hướng dẫn:** | Thầy Trần Vĩnh Đức  Chữ ký của GVHD |
| **Mã học phần:** | 149480 |
| **Bộ Môn:**  **Trường/Viện:** | Nhập môn An Toàn Thông Tin  Trường CNTT & TT. |
| **HÀ NỘI, 3/2024** | |

# I. Đề bài:

A close up of black text

Description automatically generated

1. Mục tiêu:

* Xây dựng hệ mã dòng Trivium, sau đó mã hóa các file sử dụng 1 key và 1 IV. (initial value – giá trị ban đầu) được chọn ngẫu nhiên.

2. Phương pháp:

Trivium là hệ thống mã dòng sử dụng 3 thanh ghi LFSR (Linear Feedback Shift Register) với độ dài lần lượt là 80, 80 và 128 bit. Hệ thống này hoạt động theo các bước sau:

Khởi tạo:

* + Khóa (key) và giá trị khởi tạo (IV) được chọn ngẫu nhiên với độ dài 80 bit mỗi giá trị.
  + Trạng thái ban đầu của 3 thanh ghi được tính toán dựa trên key và IV.

Tạo khóa dòng:

* + Mỗi bit của khóa dòng được tạo ra bằng cách kết hợp các bit từ 3 thanh ghi LFSR.
  + Quá trình này được lặp lại để tạo ra khóa dòng có độ dài bằng với độ dài của bản rõ.

Mã hóa:

* Chọn ngẫu nhiên key và IV với độ dài 80 bit mỗi giá trị.
* Khởi tạo hệ thống Trivium với key và IV.
* Đọc file cần mã hóa từng byte.
* Mã hóa mỗi byte bằng cách XOR với bit tương ứng của khóa dòng.
* Ghi byte mã hóa vào file đầu ra.
* Lặp lại bước 3 đến 5 cho đến khi toàn bộ file được mã hóa.

Giải mã:

* + Quá trình giải mã được thực hiện tương tự như quá trình mã hóa, nhưng sử dụng cùng một key và IV.

3. Yêu cầu:

* Gửi về file trivium được mã hóa và cho vào thư mục output.

# II. Phương pháp giải:

1. Khởi tạo 3 thanh ghi:

A close-up of a text

Description automatically generated

2.Cho Key, IV vào trong thanh ghi 1, 2:

A white paper with text and numbers

Description automatically generated

3. Tính toán output theo 3 thanh ghi:

A screenshot of a computer code

Description automatically generated

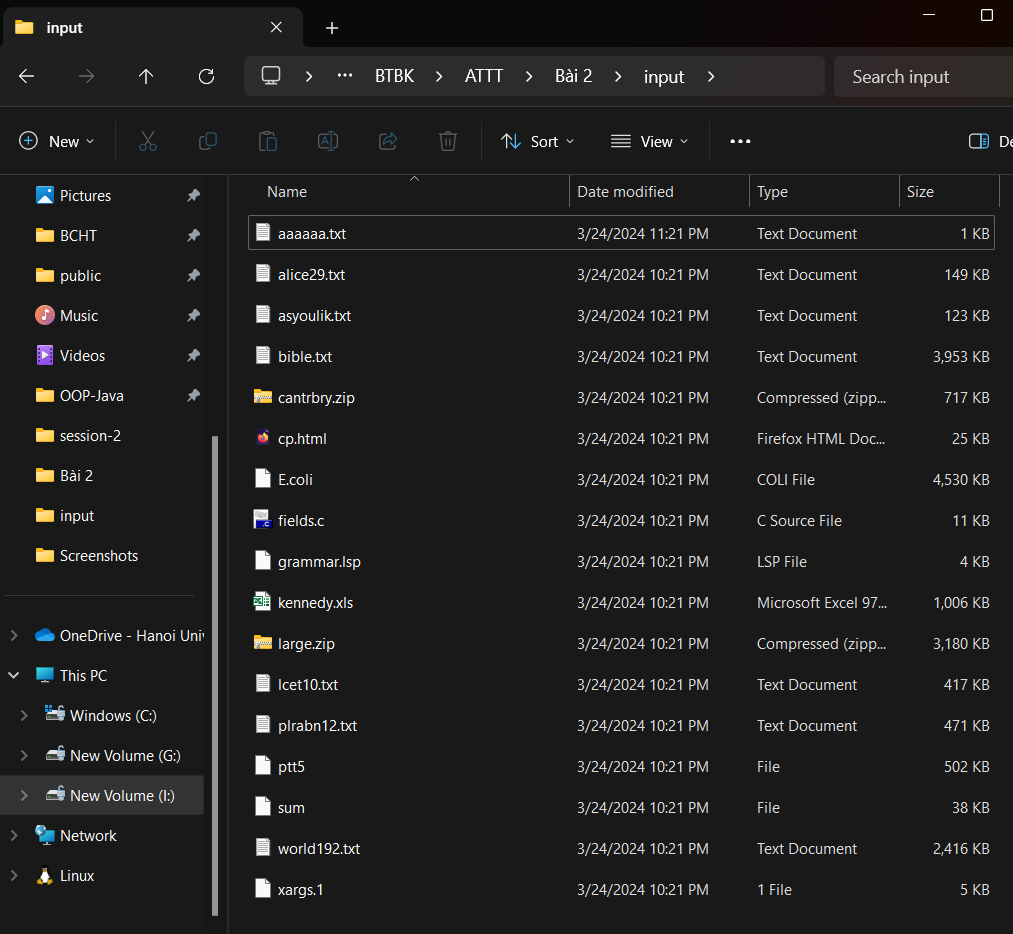
4. Đọc các file ở trong tệp input và tạo giá trị ban đầu:  
A screen shot of a computer

Description automatically generated  
5.Mã hóa các kĩ tự trong input và đưa ra output:  
A computer code with text

Description automatically generated  
6. Kết thúc và trả về thời gian mã hóa:

A white background with black and red text

Description automatically generated  
III. Kết quả chạy chương trình:

1. Tệp tin input:  
  
2. Khóa của chương trình:   
A black background with white numbers

Description automatically generated  
3.Kết quả chạy chương trình: A black and white screen with white lines

Description automatically generated  
4. Kiểm tra mã hóa:  
A screenshot of a computer screen

Description automatically generated

IV. Source code và các tài liệu tham khảo:

* Trivium Specifications – Christophe De Canni`ere and Bart Preneel:  
  https://www.ecrypt.eu.org/stream/p3ciphers/trivium/trivium\_p3.pdf
* Link GitHub chứa source code:   
  <https://github.com/HieuNT-2306/SecurityAssignment/tree/bai2/B%C3%A0i%202>
* Cách sử dụng:
  + Clone git repo về folder.
  + Chỉnh sửa file key.txt tùy theo ý muốn.
  + Đưa các file muốn mã hóa vào trong tập tin input.
  + Chạy chương trình, sau đó lấy các file được mã hóa trong tập tin output.