**ĐẠI HỌC BÁCH KHOA HÀ NỘI**

TRƯỜNG CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

**BÁO CÁO BÀI TẬP NHẬP MÔN AN TOÀN THÔNG TIN**

**Programming Assigment 2 : Lập trình mô phỏng   
TRIVIUM STREAM CIPHER**

**NGUYỄN HỮU DŨNG**

Mã số sinh viên: 20215545

**Mã lớp: 149480**

|  |  |
| --- | --- |
| **Giảng viên :** | TS. Trần Vĩnh Đức |
|  |  |
|  |  |
| **HÀ NỘI, 3/2024** | |

1. **Tóm tắt đề bài:**
2. **Cấu tạo:**

**Ảnh có chứa biểu đồ, Bản vẽ kỹ thuật, Kế hoạch, hàng

Mô tả được tạo tự động**

Trivium là hệ mã dòng với kích thước khoá 80 bit. Dựa trên việc kết hợp ba thanh ghi dịch có phản hồi, và kết hợp với thành phầnn phi tuyến. Ba thanh ghi A, B, C với kích thước mỗi thanh ghi chứa được lần lượt 93 bits, 84 bits, 111 bits.

Ban đầu, người dùng đưa vào 2 input là IV (80 bit) và key (80 bit). Trạng thái của từng thanh ghi như sau:

* 80 bit IV ­được đưa vào 80 bit trái nhất của thanh ghi A.
* 80 bit khoá được đưa vào 80 bit trái nhất của thanh ghi B.
* Mọi bit thanh ghi C có giá trị 0 ngoại trừ ba bit phải nhất :

c109 = c110 = c111 = 1

1. **Hoạt động:**

* Pha khởi động:

Trong pha ­đầu tiên này, hệ mã ­được chạy 4 x (93 + 84 + 111) = 1152 lần, nhưng không tạo ra bit ­đầu ra nào. Pha này cần để tạo cho hệ mã ­đủ ngẫu nhiên, ­đảm bảo key stream phụ thuộc vào cả key và IV.

* Pha sinh khóa:

Dãy bit sau ­đó bắt đầu từ chu kỳ 1153, được sử dụng như dòng khoá si của hệ mã dòng.

1. **Mô phỏng chương trình:**

Ngôn ngữ lập trình: C++

Tên file chương trình: Trivium.cpp

1. Khởi tạo:

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, hàng

Mô tả được tạo tự động

Ba thanh ghi được mô phỏng bằng 3 deque, thuận tiện mô phỏng việc thêm bit mới (khi thêm 1 bit mới vào đầu là push\_front(), và pop\_back() nếu thừa bit).

Mỗi phần tử trong thanh ghi có giá trị 0 hoặc 1 (để kiểu char cho tiết kiệm bộ nhớ).

Input là IV và key là 2 đầu vào có kích thước 80 bit.

1. Pha khởi động:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

1. Sinh Stream Key:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

**Ảnh có chứa biểu đồ, Bản vẽ kỹ thuật, Kế hoạch, hàng

Mô tả được tạo tự động**

1. Mã hóa file:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Trong đó:

* Hàm chuyển text sang chuỗi bit theo bảng mã ASCII:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

* Hàm XOR 2 dãy bit:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, hàng

Mô tả được tạo tự động

* Hàm chuyển dãy bit sang text:

Ảnh có chứa văn bản, Phông chữ, hàng, số

Mô tả được tạo tự động

1. **Kết quả:**

Khai báo mảng động chứa tên các file đọc và ghi tương ứng:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

Hàm main() sẽ tiến hành mã hóa từng file:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Giả sử tất cả các IV và key để mã hóa đều như nhau:

IV="10101010110011001111000011110000111100001111000011110000111100001111000011110000";

key="11001100011110000011110000111100001111000011110000111100001111000011110000111100";

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Kết quả:

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ

Mô tả được tạo tự động

