

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**HỌC PHẦN: KỸ THUẬT GIẤU TIN
MÃ HỌC PHẦN: INT14102**

LAB: stclab-2

Sinh viên thực hiện: Nguyễn Quốc Việt

Mã sinh viên: B21DCAT220

Tên lớp: 04

Giảng viên hướng dẫn: Đỗ Xuân Chơ

HÀ NỘI 2025

LAB: stclab-2

1. Mục đích

Giúp sinh viên hiểu được thuật toán giấu tin sử dụng phương pháp dựa trên tính phản xạ đối xứng của ký tự biết cách sử dụng công cụ để thực hiện giấu và tách tin.

2. Yêu cầu đối với sinh viên

Sử dụng thuần thục hệ điều hành Linux và có kiến thức về kỹ thuật giấu tin.

3. Nội dung lý thuyết

Trong hầu hết các thuật toán giấu tin, thông điệp bí mật được ẩn giấu bằng cách thay đổi cấu trúc của văn bản chứa do đó khả năng bị nghi ngờ hay mất mát dữ liệu khi gõ lại văn bản theo cấu trúc chính xác là có thể xảy ra. Để tránh xảy ra khả năng này cũng như tăng cường tính bảo mật, thay vì giấu các bit bí mật bằng cách thay đổi cấu trúc của văn bản chứa, phương pháp này sẽ giấu các thông điệp bí mật bằng cách tạo ra một văn bản tóm tắt thu thập từ các bài báo hay bất kỳ một phương tiện văn bản thông tin đại chúng. Quá trình tạo ra văn bản tóm tắt phụ thuộc vào tính phản xạ đối xứng của bảng chữ cái tiếng Anh. Dựa vào tính chất này, bảng chữ cái được chia thành các bộ khác nhau, mỗi bộ đại diện cho một cặp bit. Để thực hiện điều này cần phân tích tính phản xạ đối xứng của bảng chữ cái tiếng Anh và phân loại chúng để thể hiện các bit.

Thuật toán giấu tin

Đầu vào:

Thông điệp bí mật

Bất kỳ văn bản bằng ngôn ngữ tiếng Anh

Các bước thực hiện:

Bước 1: Biến đổi thông điệp bí mật thành chuỗi bit nhị phân

Bước 2: Kiểm tra xem tổng độ dài của chuỗi bit là chẵn hay lẻ. Nếu lẻ, phải thêm 1 bit '0' vào cuối chuỗi bit nhị phân. Bây giờ có thể chia chuỗi bit tổng thành các cặp bit liên tiếp.

Bước 3: Chuyển đổi toàn bộ các ký tự của văn bản đầu vào thành các chữ cái viết hoa.

Bước 4: Với từng cặp bit, xem xét chữ cái đầu tiên của từ đầu tiên trong câu:

✓ Nếu chữ cái đó nằm trong nhóm đại diện cho cặp bit đang xem xét, chọn câu này và đưa vào văn bản chứa.

✓ Nếu chữ cái đó không nằm trong nhóm đại diện cho cặp bit đang xem xét, bỏ qua câu này và chọn câu tiếp theo

Bước 5: Quá trình tiếp diễn cho đến khi toàn bộ chuỗi bit của thông điệp bí mật được thực thi hết

Bước 6: Văn bản mã hóa thu được là bản tóm tắt của văn bản đầu vào và được gửi đến người nhận

Đầu ra:

Văn bản chứa thông điệp bí mật, hay chính là văn bản tóm lược của văn bản đầu vào

Thuật toán tách tin:

Đầu vào:

Văn bản chứa thông điệp bí mật (đầu ra của thuật toán giấu tin) Các bước thực hiện:

Bước 1: Lấy các chữ cái đầu tiên của các từ đầu tiên trong từng câu.

Bước 2: Dựa vào bảng để lấy ra các cặp bit từ những chữ cái thu được và đưa ra một file.

Bước 3: Chuyển đổi chuỗi bit nhị phân thành dạng chữ cái tương ứng.

Bước 4: Toàn bộ thông điệp dưới dạng chữ cái thu được chính là thông điệp ẩn giấu
Đầu ra:

Thông điệp bí mật

4. Nội dung thực hành

Add module file lab:

Imodule <https://github.com/kokushibouz/Labtainer-Lab/raw/refs/heads/main/stclab-2.tar>

Khởi động bài lab:

Vào terminal, gõ :

```
labtainer -r stclab-2
```

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người

thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Nhiệm vụ 1: Làm quen với công cụ

- Trước khi thực hiện giấu tin ta sẽ tiến hành mở công cụ lên và làm quen với công cụ bằng lệnh:

```
./steganography.py
```
- Công cụ cung cấp cho chúng ta 2 chế độ chọn là giấu tin (mã hoá) và tách tin (giải mã)
- Để thực hiện giấu tin ta cần chọn file chứa thông điệp (tức là văn bản cần được giấu tin) và văn bản nền (tức là văn bản để ta giấu thông điệp vào)
- Để thực hiện tách tin ta cần chọn file chứa thông điệp được giấu

Nhiệm vụ 2: Thực hiện giấu tin

- Sau khi đã làm quen với công cụ ta sẽ tiến hành giấu tin

- Ta tiến hành chọn file message.txt là file chứa thông điệp cần giấu và file text.txt là file chứa văn bản để ta giấu thông điệp vào
- Sau khi giấu tin thành công sẽ xuất hiện file encrypt.txt
- Tiến hành đọc file và so sánh xem khả năng giấu tin của thuật toán?

Nhiệm vụ 3: Thực hiện giải mã và xem nội dung thông điệp

- Nhận thấy rằng trên máy user có một file flag.zip và cần mật khẩu để unzip file
- Ta sẽ tiến hành lấy mật khẩu bằng cách tách thông điệp từ file passwd.txt
- Sau khi thu được thông điệp ta tiến hành giải nén file flag.zip bằng lệnh
Unip flag.zip
- Sau khi giải nén thành công ta tiến hành đọc nội dung file trong thư mục đã được giải nén

Kết thúc bài lab:

o Kiểm tra checkwork:

checkwork

o Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

stoplab

Khởi động lại bài lab:

labtainer -r stclab-2