Lê Ngọc Kiều Anh

MSSV: 22520047

**BÀI TẬP AN TOÀN MẠNG BUỔI 5**

1. **Tìm khóa công khai 3 trang web (tên trang web, kích thước khóa, nhà cung cấp chứng thực cho trang, một phần đầu của chuỗi khóa).**

**Trang web 1:**

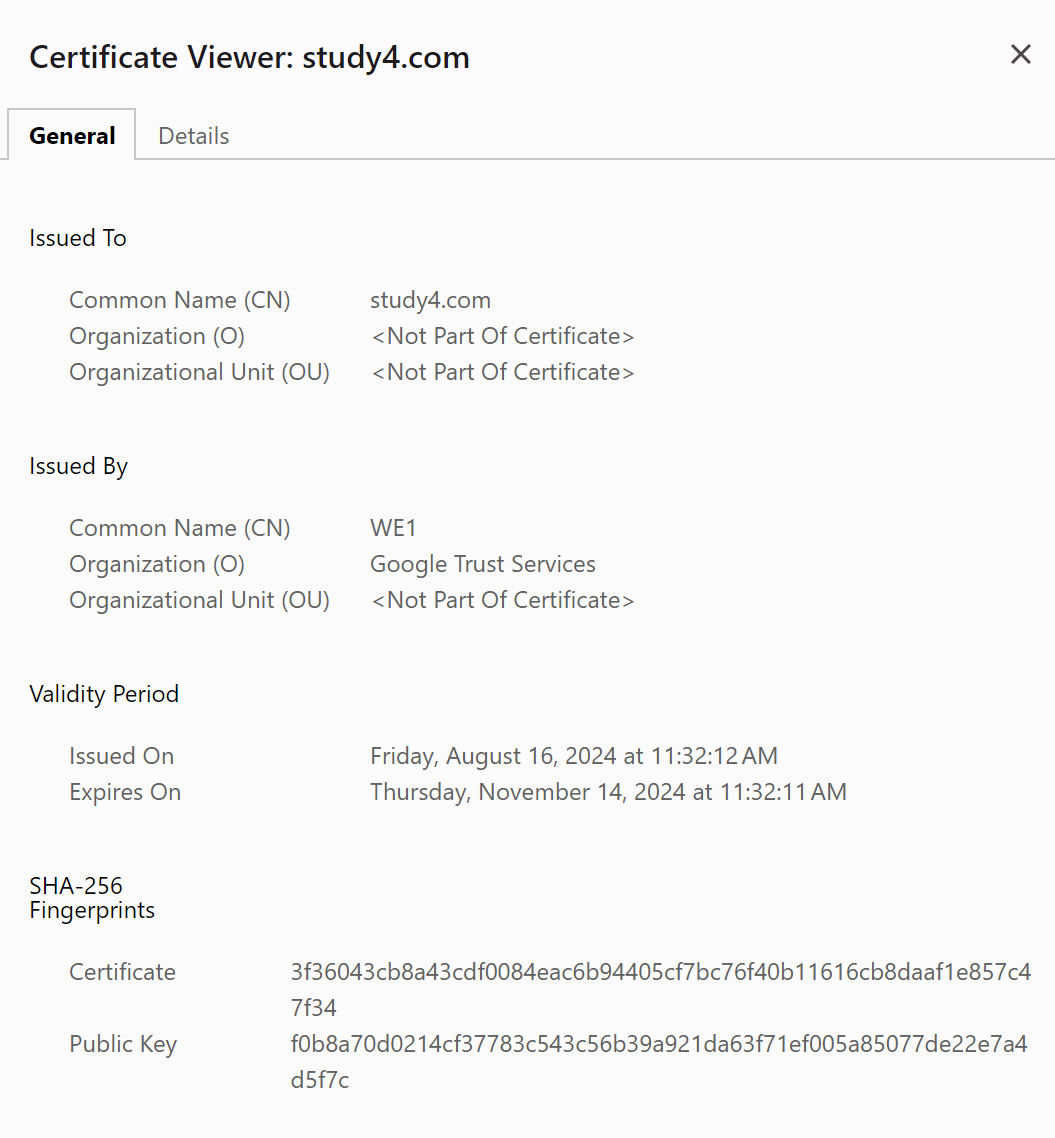
**-** Tên trang web: study4.com

- Kích thước khóa: 4096 bit

- Nhà cung cấp chứng thực: Google Trust Services

- Một phần đầu của chuỗi khóa:

f0b8a70d0214cf37783c543c56b39a921da63f71ef005a85077de22e7a4d5f7c

****

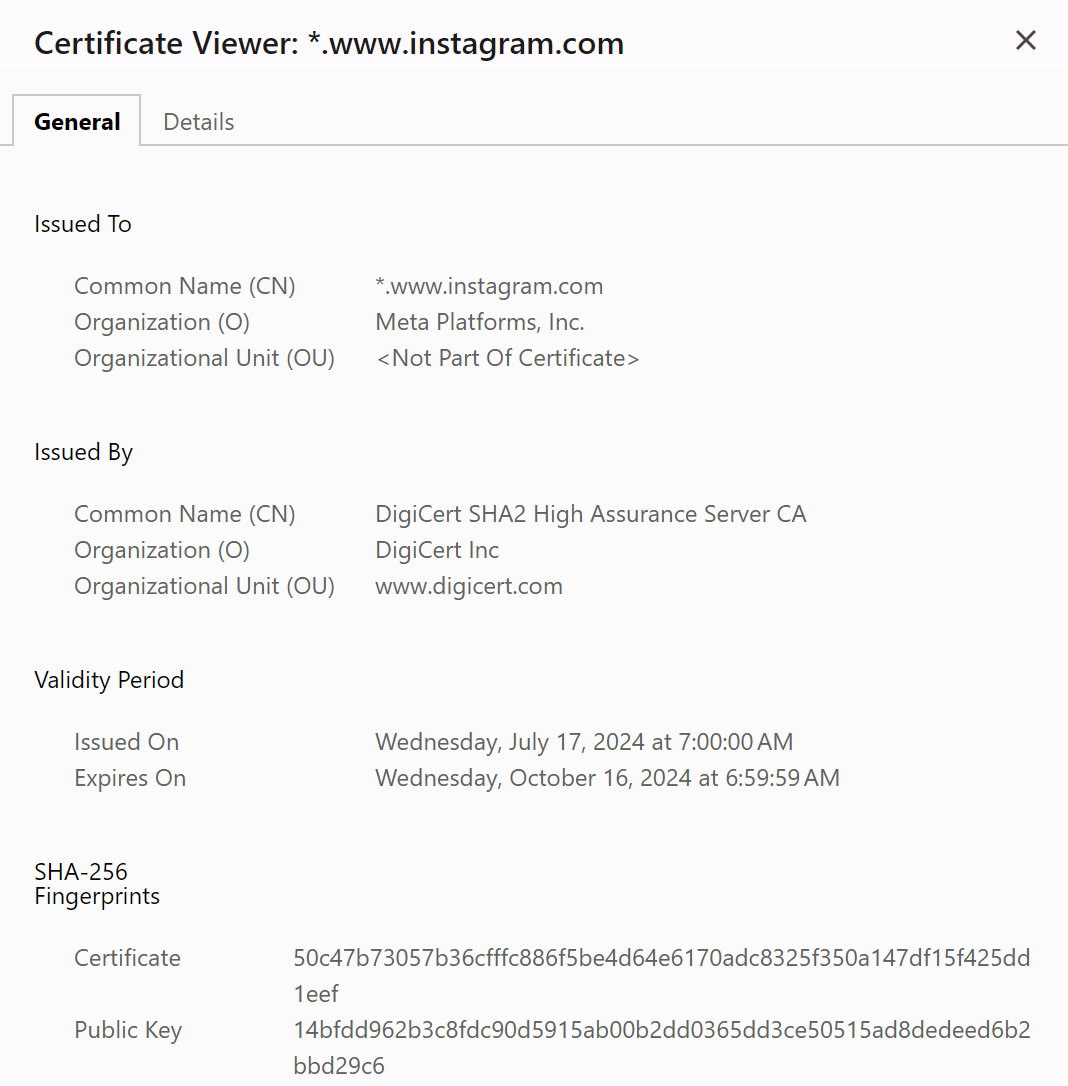
**Trang web2:**

**-** Tên trang web: instagram.com

- Kích thước khóa: 2048 bit

- Nhà cung cấp chứng thực: DigiCert Inc

- Một phần đầu của chuỗi khóa: 14bfdd962b3c8fdc90d5915ab00b2dd0365dd3ce50515ad8dedeed6b2bbd29c6

****

**Trang web 3:**

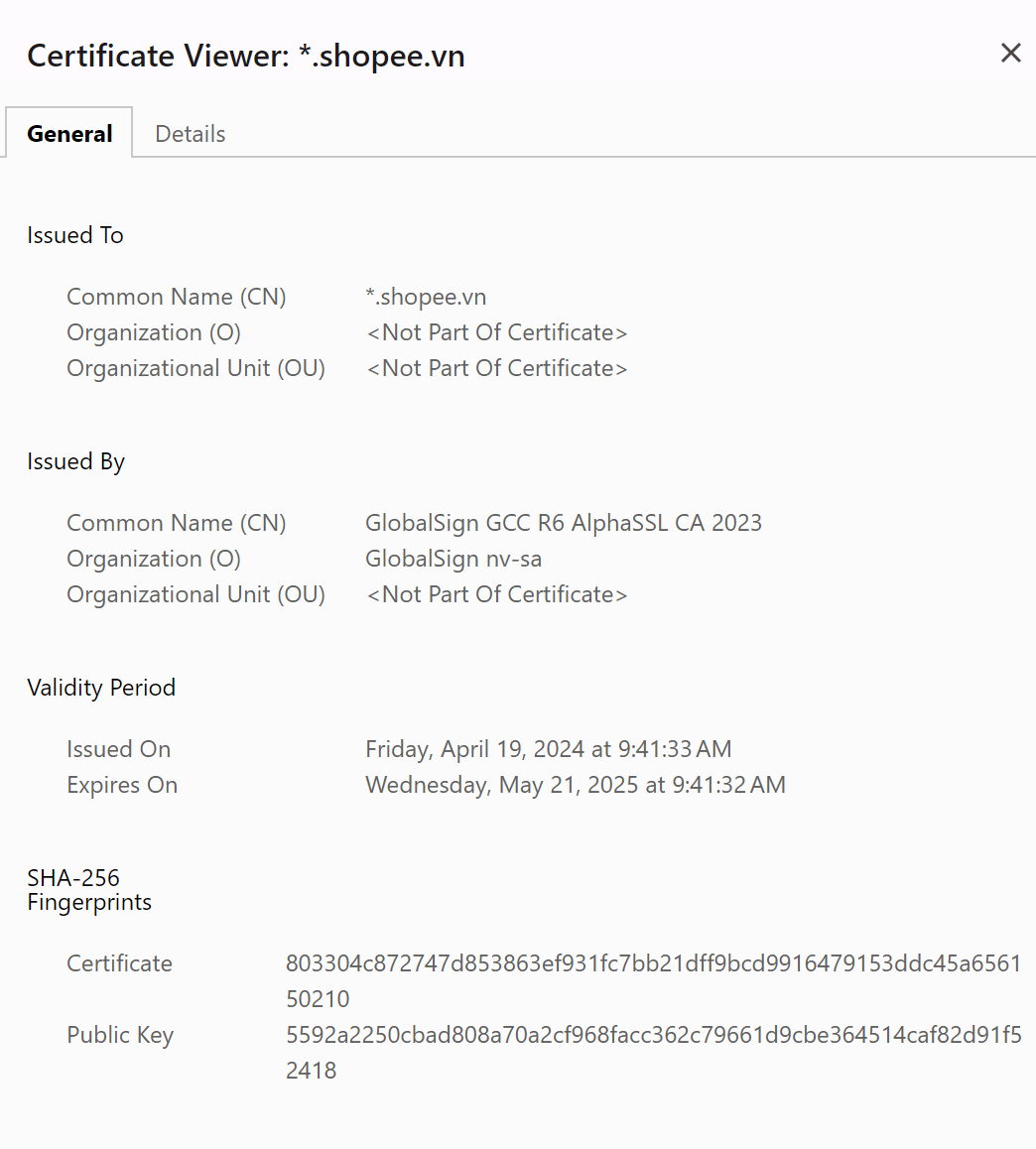
- Tên trang web: shoppe.vn

- Kích thước khóa: 2048 bit

- Nhà cung cấp chứng thực: GlobalSign nv-sa

- Một phần đầu của chuỗi khóa:

5592a2250cbad808a70a2cf968facc362c79661d9cbe364514caf82d91f52418



1. **Tìm 3 phần mềm được cung cấp trên Internet có kèm theo mã băm (tên trang web, tên phần mềm, dạng mã băm, mã băm). Download về 1 phần mềm và kiểm tra tính toàn vẹn của nó thông qua mã băm đính kèm.**

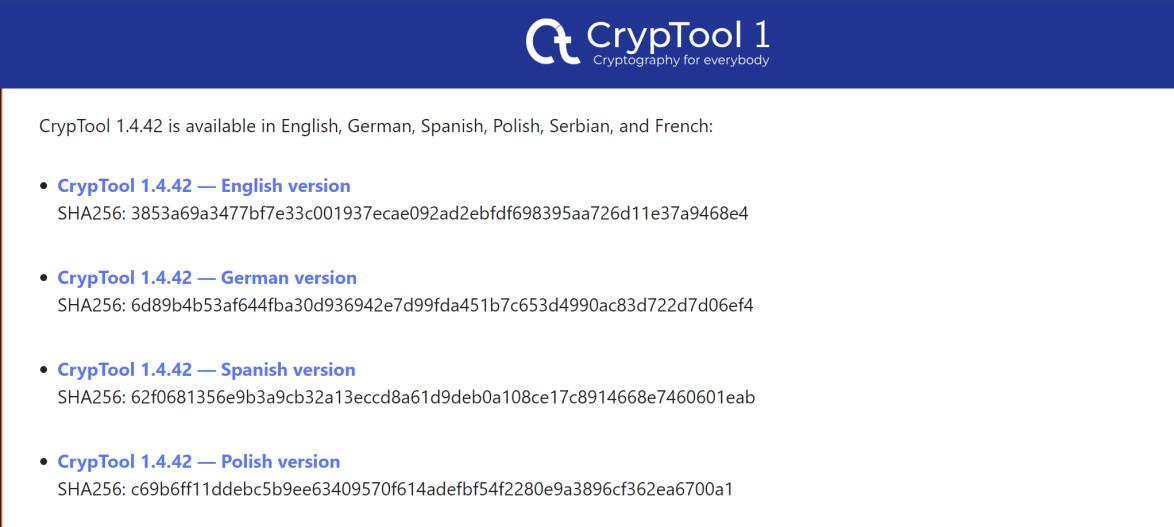
**Phần mềm 1:**

- Tên trang web: <https://www.cryptool.org/en/ct1/downloads/>

- Tên phần mềm: CrypTool

- Dạng mã băm: SHA256

- Mã băm: 3853a69a3477bf7e33c001937ecae092ad2ebfdf698395aa726d11e37a9468e4



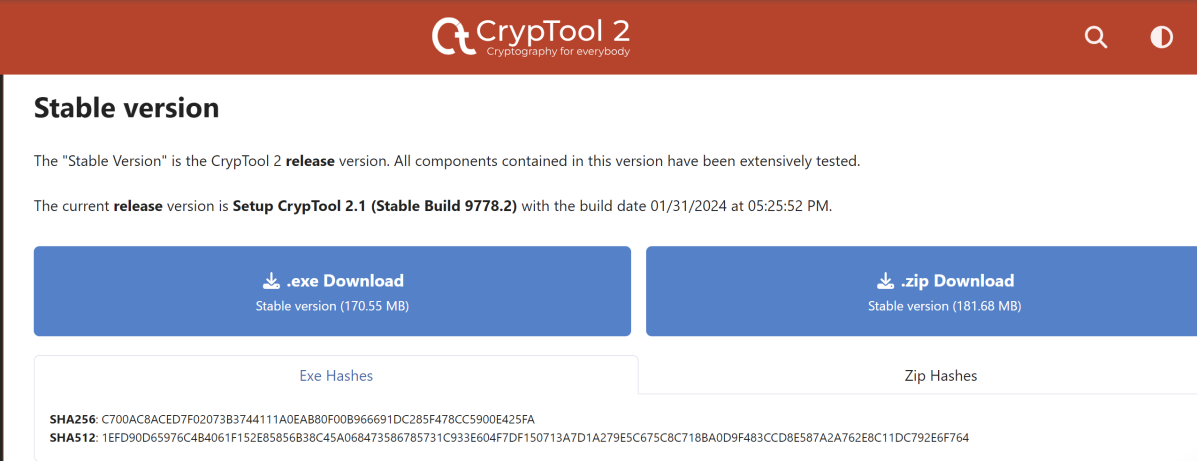
**Phần mềm 2:**

- Tên trang web: <https://www.cryptool.org/en/ct2/downloads/>

- Tên phần mềm: CrypTool2

- Dạng mã băm: SHA256, SHA512

- Mã băm: C700AC8ACED7F02073B3744111A0EAB80F00B966691DC285F478CC5900E425FA



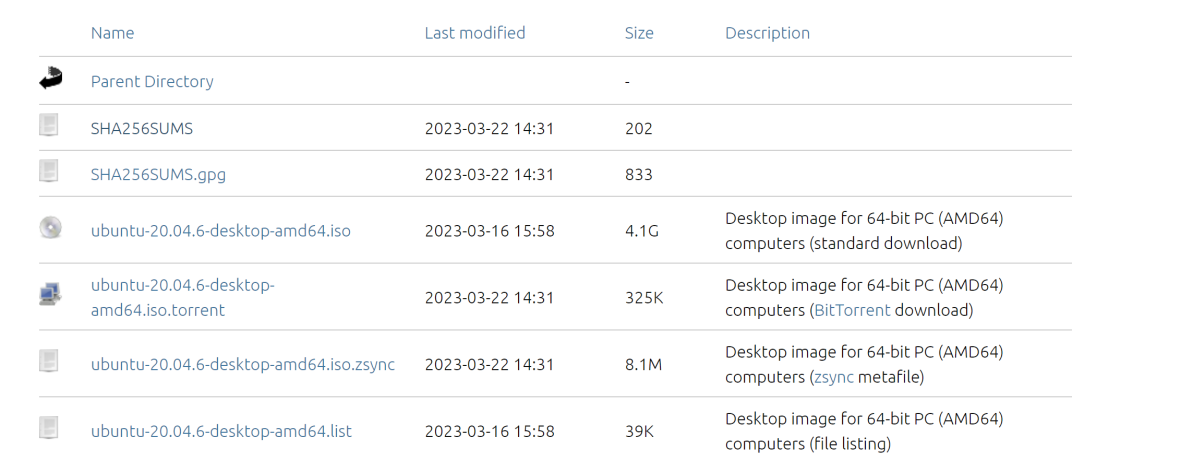
**Phần mềm 3:**

- Tên trang web: <https://releases.ubuntu.com/focal>

- Tên phần mềm: Ubuntu 20.04.6 LTS

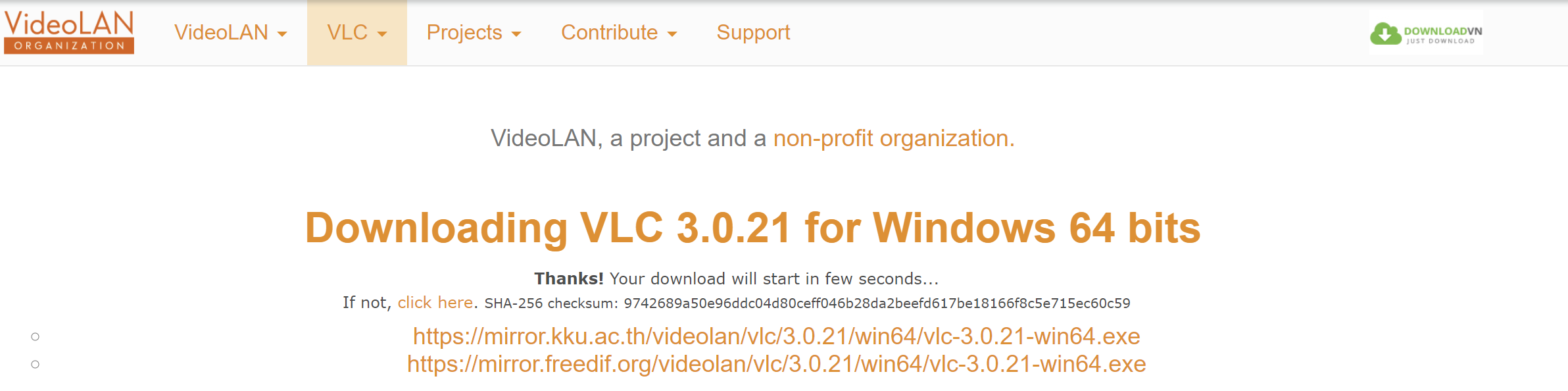
- Dạng mã băm: SHA256

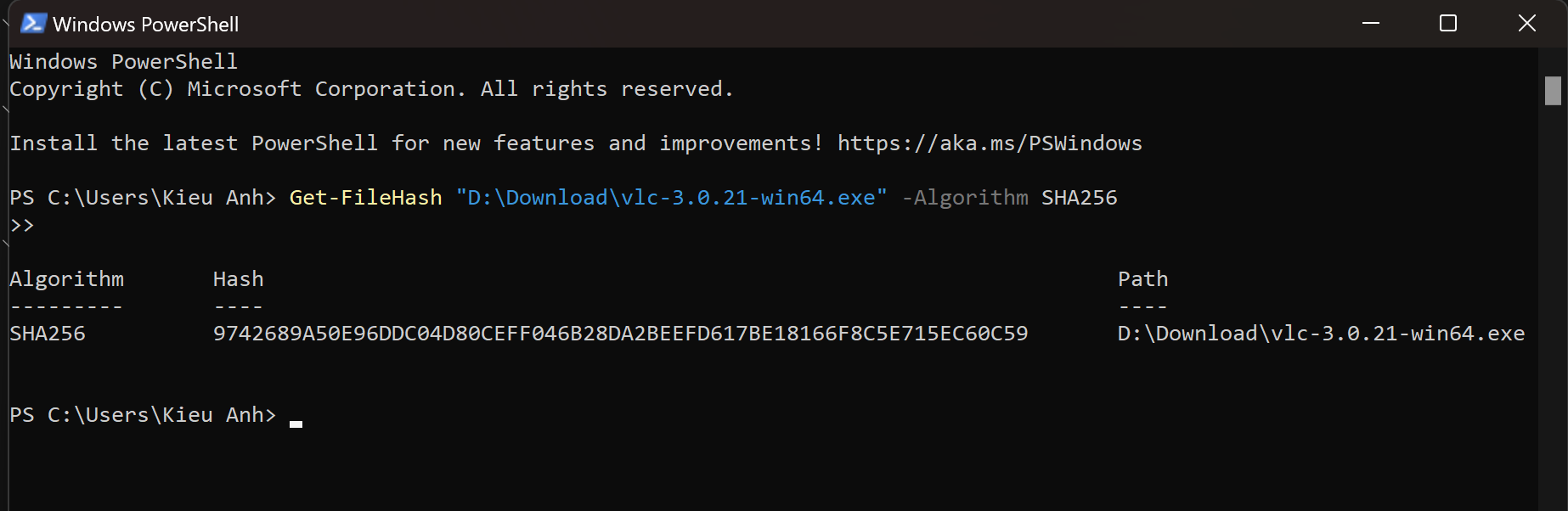
- Mã băm: e7f1517a7a1645e75679fa62d0b7ff2b8f9c133bc8adfb83bce34abed0d12fd0



Download 1 phần mềm và kiểm tra tính toàn vẹn:

Download phần mềm: VLC 3.0.21

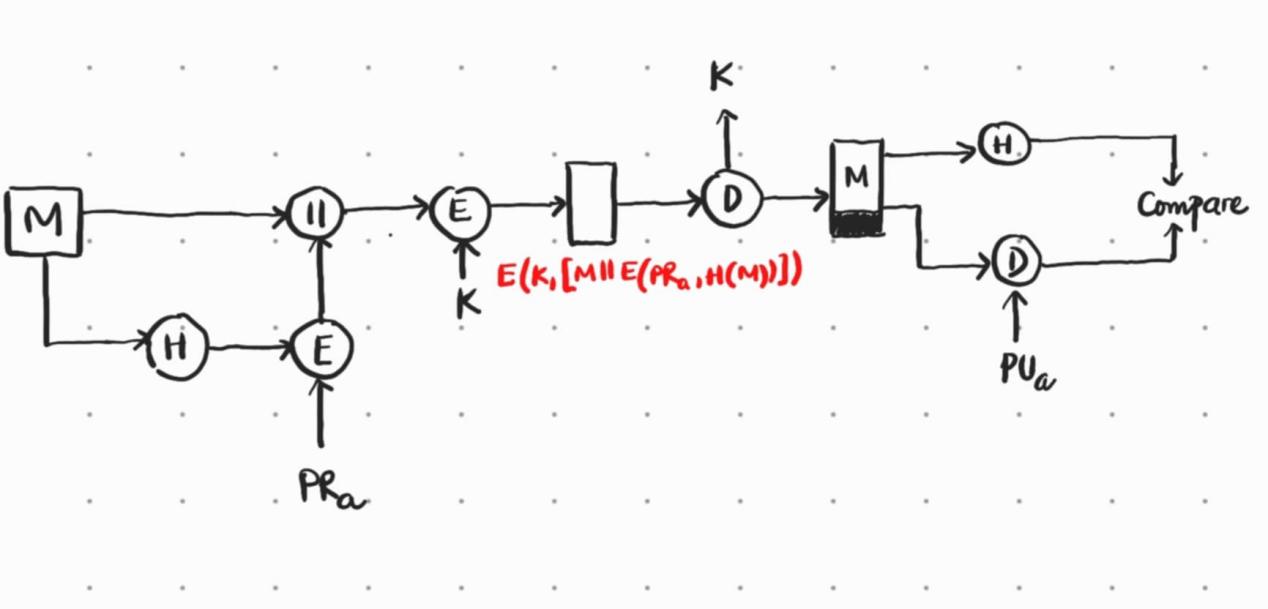




So sánh 2 mã băm thấy giống nhau

1. **Phác họa một hệ thống có đầy đủ các chức năng bảo mật, chứng thực, chữ ký số dựa trên các hình đã học. Phân tích hoạt động và ưu nhược điểm của hệ thống.**

Hệ thống có chức năng bảo mật, chứng thực, chữ kỹ số:

****

**\* Hoạt động:**

- Thông điệp **M** được đưa qua hàm băm **H** để tạo ra một chuỗi **H(M)**.

**- Chuỗi ngắn H(M)** sau đó được mã hóa bằng khóa riêng của người gửi **PRᴀ** (khóa riêng của A). Đây chính là **chữ ký số** của người gửi.

- Kết quả được kết hợp với thông điệp gốc **M** và mã hóa toàn bộ bằng khóa đối xứng **K.**

- Thông điệp đã được mã hóa và chữ ký số được gửi tới người nhận (dữ liệu được mã hóa bằng khóa đối xứng **K**).

- Người nhận giải mã thông điệp bằng khóa **K**, khôi phục lại thông điệp gốc và chữ ký số.

- Sau đó, người nhận lấy phần chữ ký số và tiến hành giải mã chữ ký bằng **khóa công khai của người gửi (PUᴀ)** để thu được chuỗi **H(M)**.

- Người nhận cũng chạy hàm băm **H** trên thông điệp nhận được để tạo ra một chuỗi H(M) mới

- Cuối cùng, so sánh hai chuỗi vừa tạo ra và chuỗi gốc đã được giải mã từ chữ ký số. Nếu chúng giống nhau, thông điệp được xác nhận là chính xác, không bị thay đổi trong quá trình truyền và đến từ người gửi hợp lệ.

**\* Ưu điểm:**

**- Tính bảo mật cao:** Dữ liệu được mã hóa và chỉ có thể giải mã bởi người nhận biết khóa, tránh bị rò rỉ hoặc truy cập trái phép.

**- Tính xác thực:** Nhờ chứng chỉ số, các bên tham gia có thể chứng thực danh tính của nhau, giảm thiểu nguy cơ bị giả mạo.

- **Tính toàn vẹn:** Chữ ký số đảm bảo rằng dữ liệu không bị thay đổi trong quá trình truyền tải.

**- Dễ dàng xác minh:** Khóa công khai được công khai, giúp người nhận dễ dàng xác minh tính hợp pháp của thông điệp.

**\* Nhược điểm:** **Chi phí duy trì v**iệc thiết lập và duy trì các chứng chỉ số từ CA có thể tốn kém, hệ thống cần phải được cấu hình cẩn thận và đúng cách để tránh lỗi bảo mật.