**Họ và tên: Tăng Dũng Cẩm**

**MSSV: 22520141**

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

- Trong trang web [vnpress.net](https://vnexpress.net/) ta tìm đc khoá công khai:

**Kích thước khoá**: 2048 bits

**Nhà cung cấp chứng thực cho trang**: GlobalSign nv-sa

**Chuỗi khoá**: b1e708dd3a24b74d13c4719278b2a7ae06884e92c58dac362aabcca4b2d7331a

A screenshot of a computer

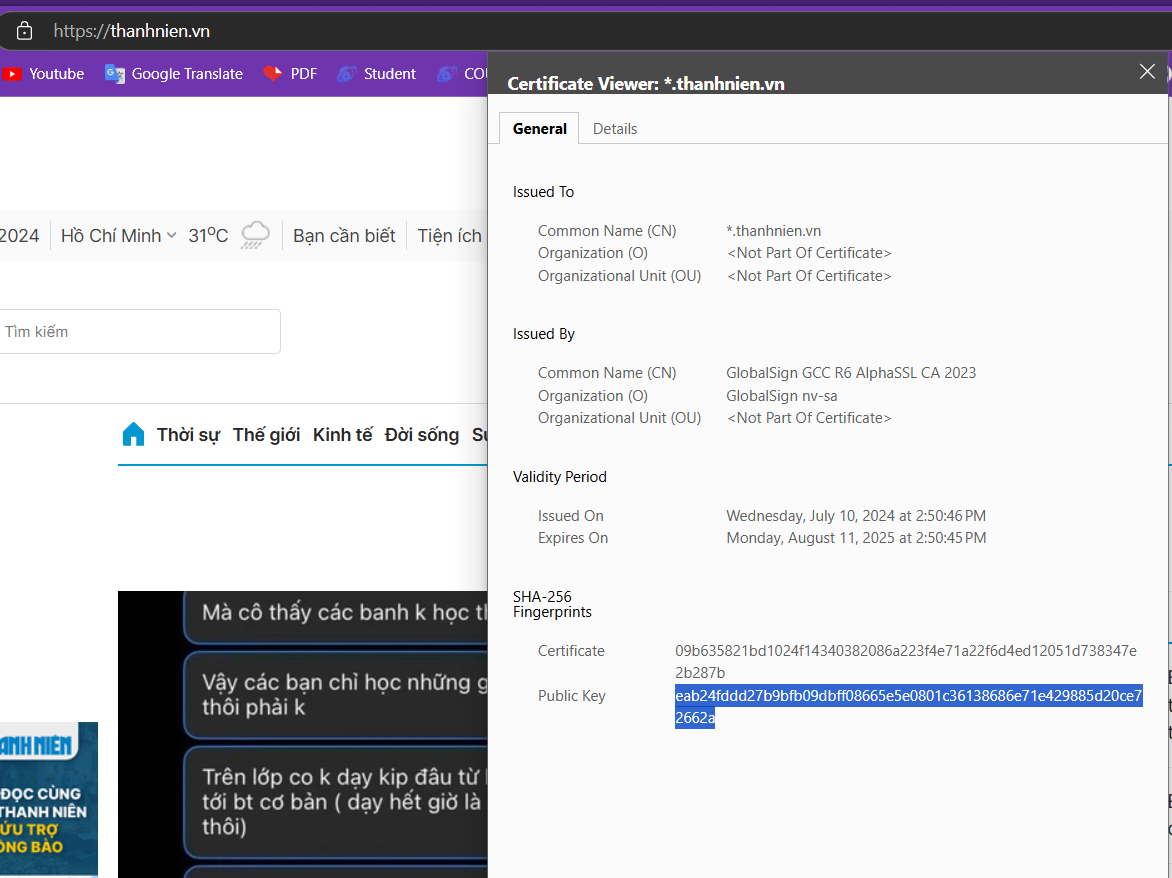
Description automatically generated

- Trong trang web [thanhnien.vn](https://thanhnien.vn/) ta tìm đc khoá công khai:

**Kích thước khoá**: 2048 bits

**Nhà cung cấp chứng thực cho trang**: GlobalSign nv-sa

**Chuỗi khoá**: eab24fddd27b9bfb09dbff08665e5e0801c36138686e71e429885d20ce72662a



- Trong trang web [baomoi.com](https://baomoi.com/) ta tìm đc khoá công khai:

**Kích thước khoá**: 2048 bits

**Nhà cung cấp chứng thực cho trang**: DigiCert Inc

**Chuỗi khoá**: 4a9ee3c47543514c7b3a1d910638bea587026f746210abc43bddaca88e91e18b

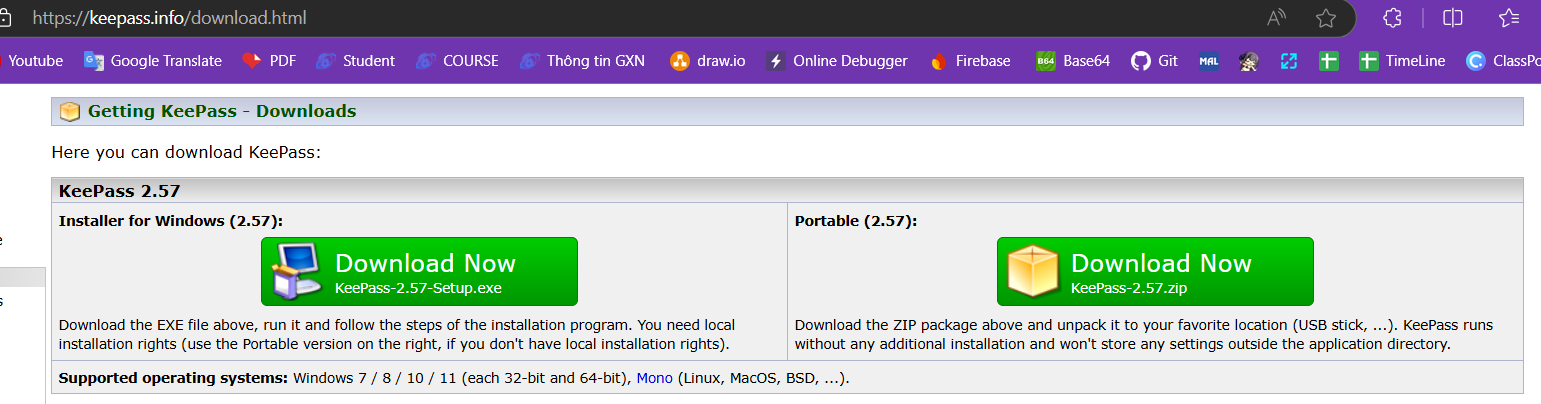
A screenshot of a computer

Description automatically generated

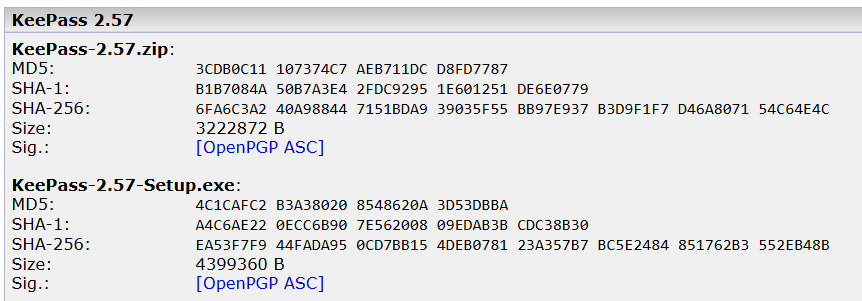
1. **Tìm 3 phần mềm được cung cấp trên Internet có kèm theo mã băm (tên trang web, tên phần mềm, dạng mã băm, mã băm). Download về 1 phần mềm và kiểm tra tính toàn vẹn của nó thông qua mã băm đính kèm.**

**Phần mềm KeePass**

* Trang: [keepass.info](https://keepass.info/integrity.html)

****

* Dạng mã băm và mã băm tương ứng:



**Hệ điều hành Windows**

* Trang: [Veracrypt.fr](https://www.veracrypt.fr/en/Downloads.html)
* Dạng mã băm: SHA256
* Mã băm tương ứng với các lựa chọn:

A screenshot of a computer

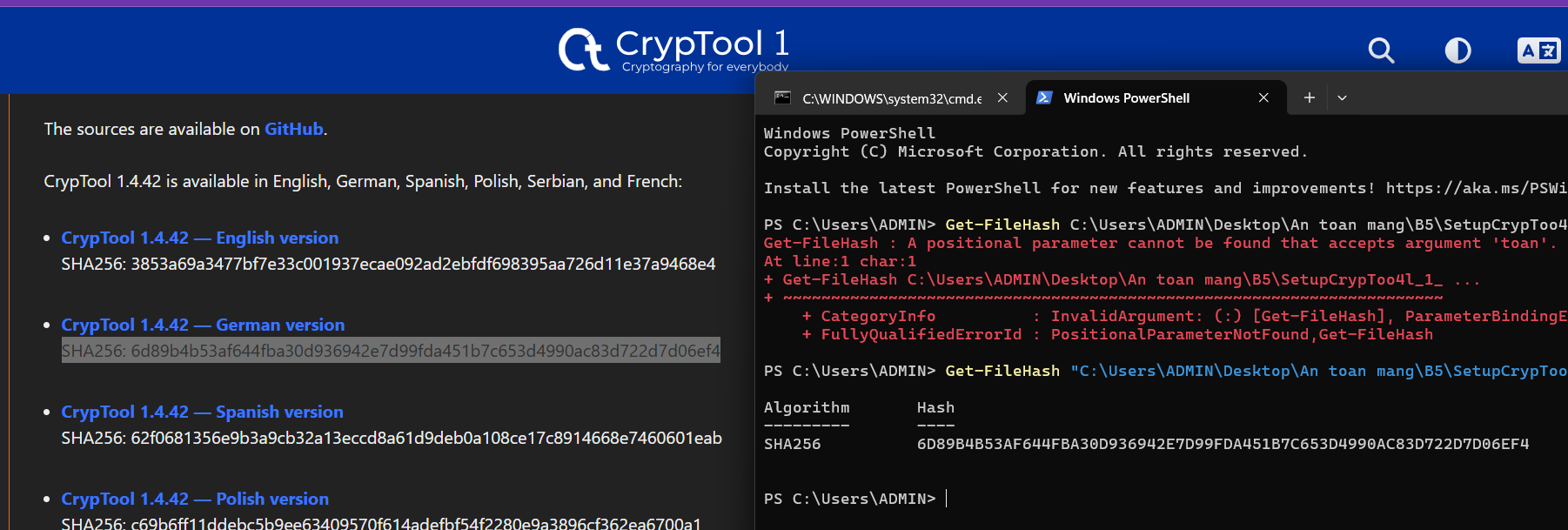
Description automatically generated

**CrypTool 1**

* Phần mềm được tải từ: [CT1 Downloads - CrypTool](https://www.cryptool.org/en/ct1/downloads/)
* Dạng mã băm là SHA256.
* Mã băm sau khi tải về:

6d89b4b53af644fba30d936942e7d99fda451b7c653d4990ac83d722d7d06ef4

* Dùng lệnh trong PowerShell để tìm mã băm trong file tải về.



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

**A diagram of a diagram

Description automatically generated**

Phân tích hoạt động của hệ thống:

* Khởi đầu với thông điệp M và chuỗi S:
  + Thông điệp M được đưa vào quá trình xử lý.
  + S có thể là một giá trị phụ hoặc chuỗi bí mật đi kèm với thông điệp để thêm tính bảo mật.
* Kết hợp thông điệp M và chuỗi S
* H (hàm băm hoặc hàm hash):
  + Sử dụng hàm băm (H) để tạo ra chuỗi băm, giúp xác thực tính toàn vẹn của thông tin trong các bước tiếp theo.
* E (mã hóa):
  + Mã hoá chuỗi băm với khoá bí mật của người gữi.
* Kết hợp thông điệp M và kết quả của việc mã hoá sau đó tiếp tục mã hoá với khoá K được dùng chung giữa người gữi và người nhận.
* Truyền qua kênh truyền một dữ liệu được mã hoá có thể biểu diễn theo biểu thức

E (K, (M | | E (PRa, H ( M | | S ) ) ) )

* D (giải mã):
  + Tại đầu nhận, thực hiện quá trình giải mã bằng cách sử dụng khóa K đã được trao đổi để tìm ra thông tin đã mã hóa trước đó.
  + Thông tin này bao gồm thông điệp M và phần thông tin được biểu diễn theo biểu thức sau:

E ( PRa , H ( M | | S ) )

* Thông điệp M sẽ lại được ghép với một chuỗi S được quy ước dùng chung giữa người gữi và nhận. Sau đó sẽ được đưa vào hàm băm để ra một chuỗi băm
* Phần thông tin E ( PRa , H ( M | | S ) ) sẽ được giãi mã với mã công khai của a để ra được chuỗi băm H ( M | | S )
* So sánh và xác thực:
  + So sánh 2 chuỗi băm để kiểm tra tính toàn vẹn của thông điệp M.

Ưu điểm:

* Bảo mật cao: Hệ thống này sử dụng cả hàm băm và mã hóa, giúp bảo vệ dữ liệu khỏi việc bị giả mạo hay thay đổi trong quá trình truyền tải.
* Khả năng xác thực: Có thành phần kiểm tra tính toàn vẹn của thông điệp (Compare), đảm bảo rằng dữ liệu đã được nhận đúng như dữ liệu ban đầu.
* Phức hợp nhiều cơ chế bảo mật: Việc sử dụng đồng thời nhiều thành phần (hàm băm, mã hóa, chữ kí số, xác thực) giúp tăng cường độ bảo mật.

Nhược điểm:

* Chi phí tính toán cao: Do hệ thống sử dụng nhiều bước mã hóa, giải mã và tính toán hàm băm, có thể đòi hỏi tài nguyên tính toán lớn.
* Độ phức tạp: Quá trình thực thi phức tạp, đòi hỏi sự phối hợp tốt giữa các thành phần, có thể dẫn đến lỗi nếu không được triển khai cẩn thận.