BÀI THỰC HÀNH SỐ 6

Môn: MẬT MÃ VÀ AN NINH MẠNG

-o0o-

Họ và tên: Nguyễn Hữu Bảo

MSSV: 1811523

* + 1. **MỤC TIÊU**

Mục tiêu của bài thực hành này cung cấp kỹ năng an ninh hệ thống E-mail cá nhân, an ninh hệ thống Web.

Các nội dung chính trong bài thực hành gồm 2 phần:

* An ninh hệ thống E-mail cá nhân với Thunderbird và OpenPGP.
* An ninh hệ thống Web với Apache Web Server và SSL.
  + 1. **TÀI LIỆU THAM KHẢO**

# [1]. <https://wiki.mozilla.org/Thunderbird:OpenPGP:2020>

# [2]. <https://httpd.apache.org/>

# [3]. <https://windowsreport.com/create-self-signed-certificate/>

[4]. <https://www.sslshopper.com/article-how-to-create-and-install-an-apache-self-signed-certificate.html>

* + 1. **CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH**

Các trang thiết bị và phiên bản phần mềm sử dụng trong bài thực hành:

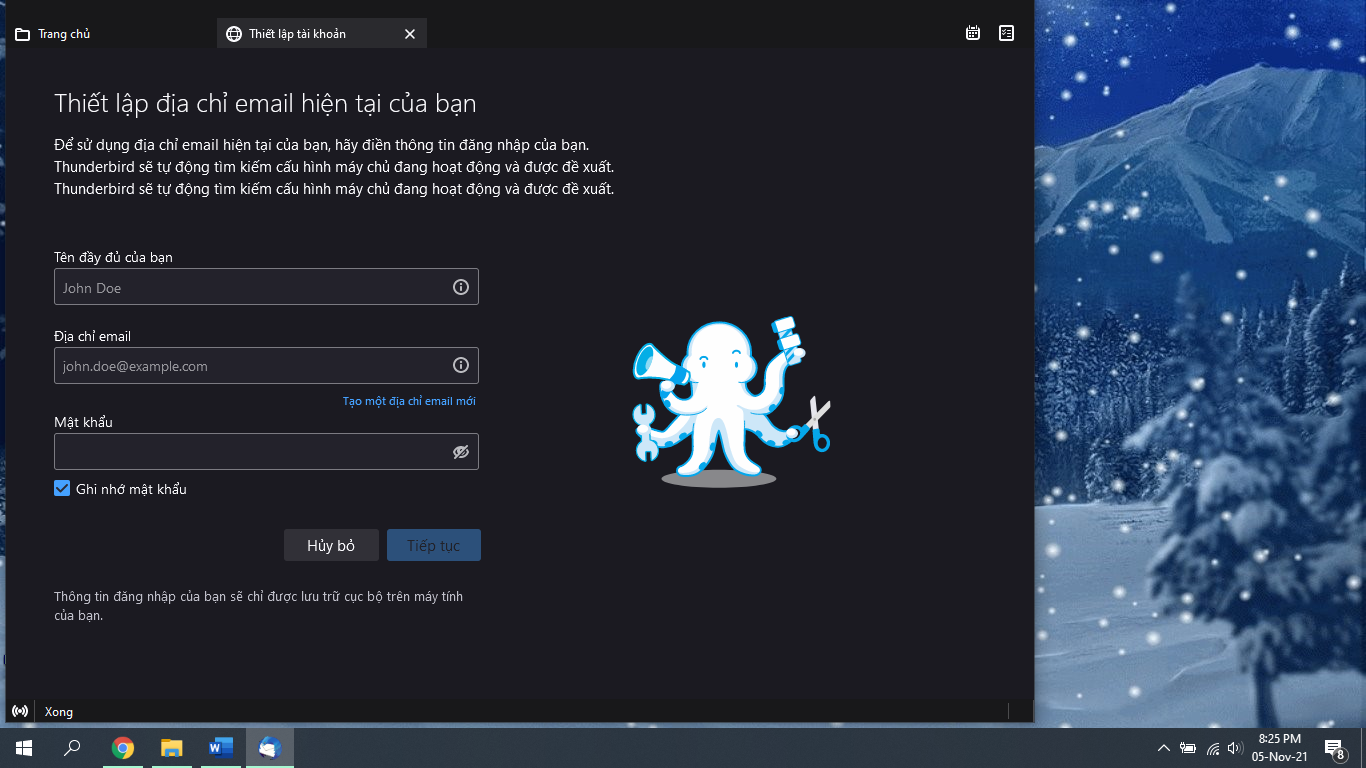
* 01 máy tính truy cập đến Internet.
* Trình gởi và nhận thư: Mozilla Thunderbird phiên bản 78.10.0.
* Apache Web Server và OpenSSL.
  + 1. **CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI**
* Sinh viên cần trả lời thông tin(văn bản, hình ảnh) vào các phần yêu cầu trong bài thực hành vào lưu lại thành tập tin lab6.doc
* Thời gian làm bài là 14 ngày.
  + 1. **NỘI DUNG THỰC HIỆN**
       - 1. **An ninh hệ thống E-mail cá nhân**

1. *Cài đặt Mozillla Thunderbird*

**Mozilla Thunderbird** là chương trình miễn phí, nguồn mở hoạt động trên mọi nền tảng hệ điều hành giúp quản lý việc nhận, gửi và lưu trữ thư điện tử. Một phần mềm quản lý thư điện tử phía người dùng là một chương trình giúp bạn tải về và quản lý thư điện tử mà không cần sử dụng trình duyệt Internet. Bạn có thể quản lý nhiều tài khoản thư điện tử khác nhau sử dụng chương trình này. Tài khoản của bạn phải được tạo ra trước khi dùng với **Thunderbird**.

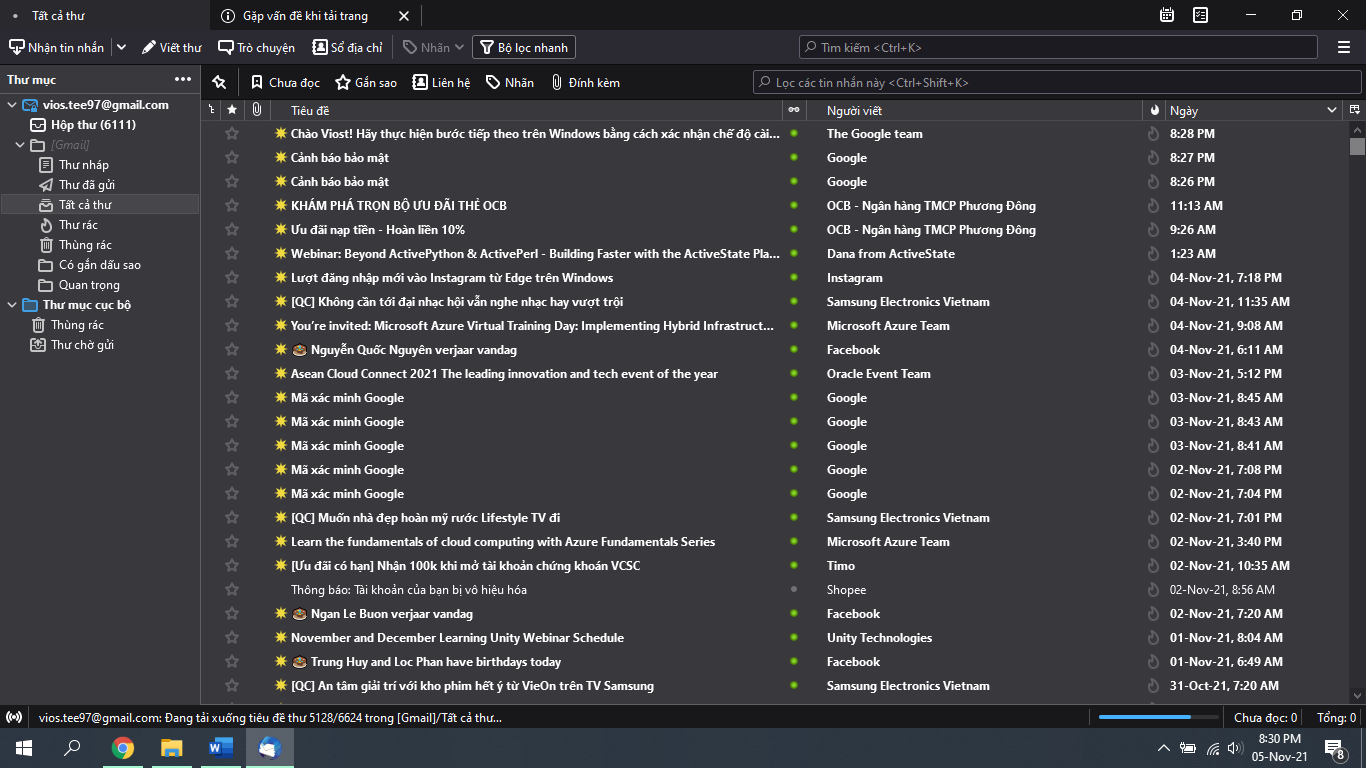
**Download Thunderbird từ** <http://www.mozilla.org/en-US/thunderbird/>

Các bước ngắn gọn để cài đặt Thunderbird**:**



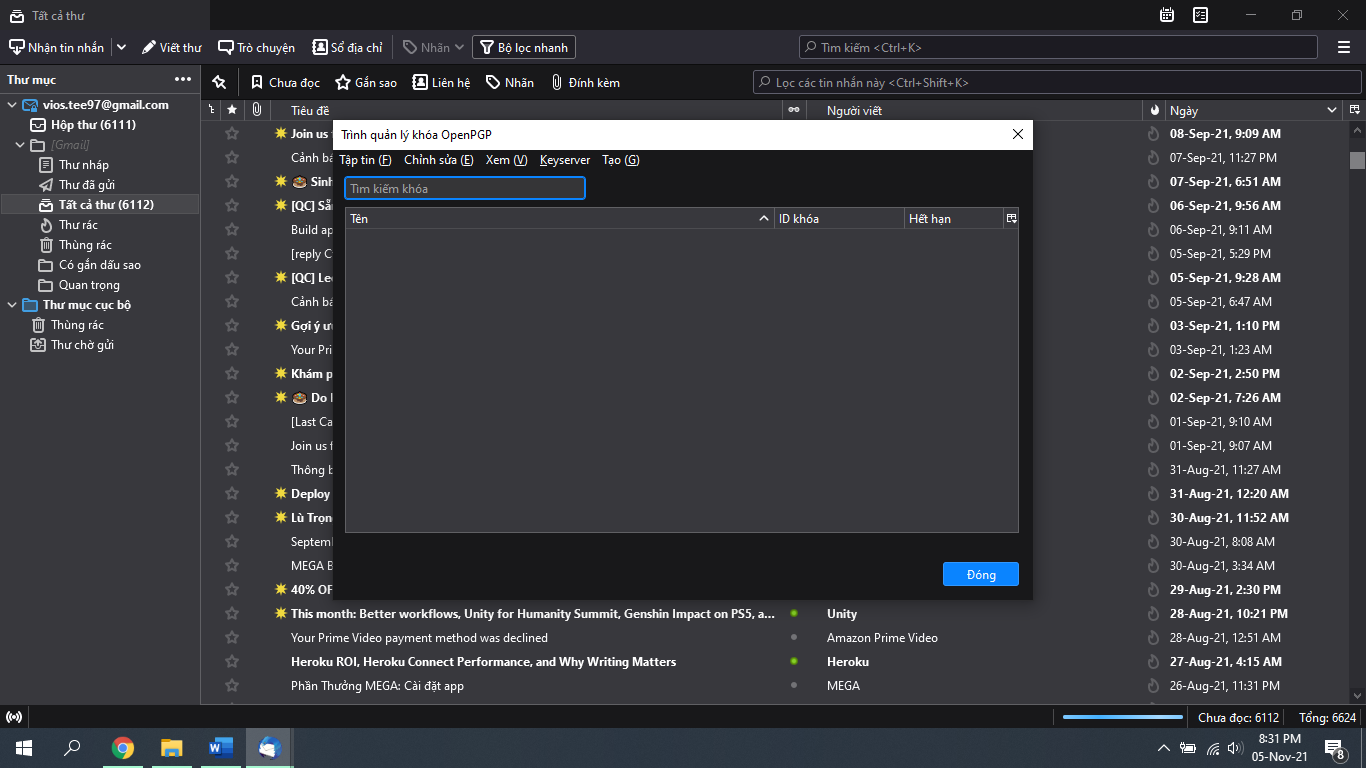
1. *Đăng ký một tài khoản thư điện tử vào Thunderbird*

Các bước ngắn gọn để đăng ký một tài khoản thư điện tử của bạn vào thunderbird:

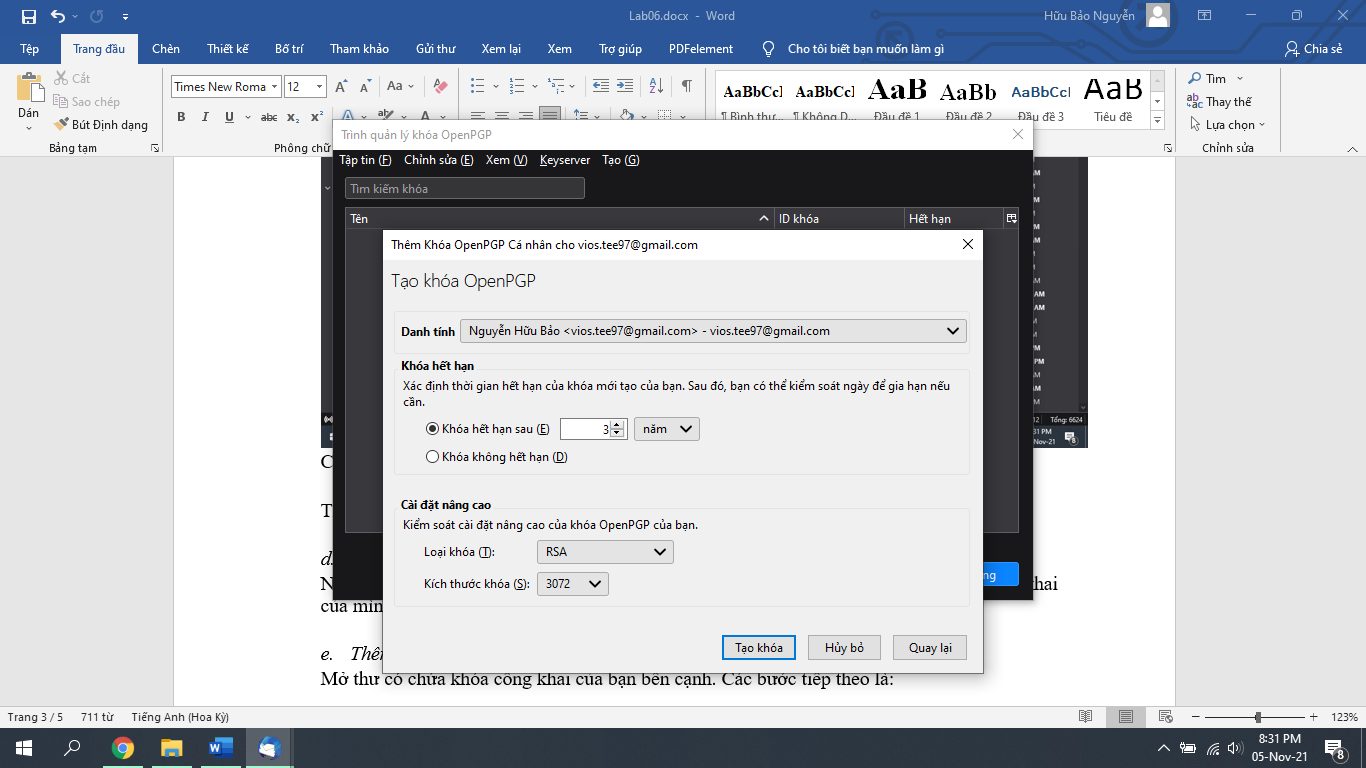


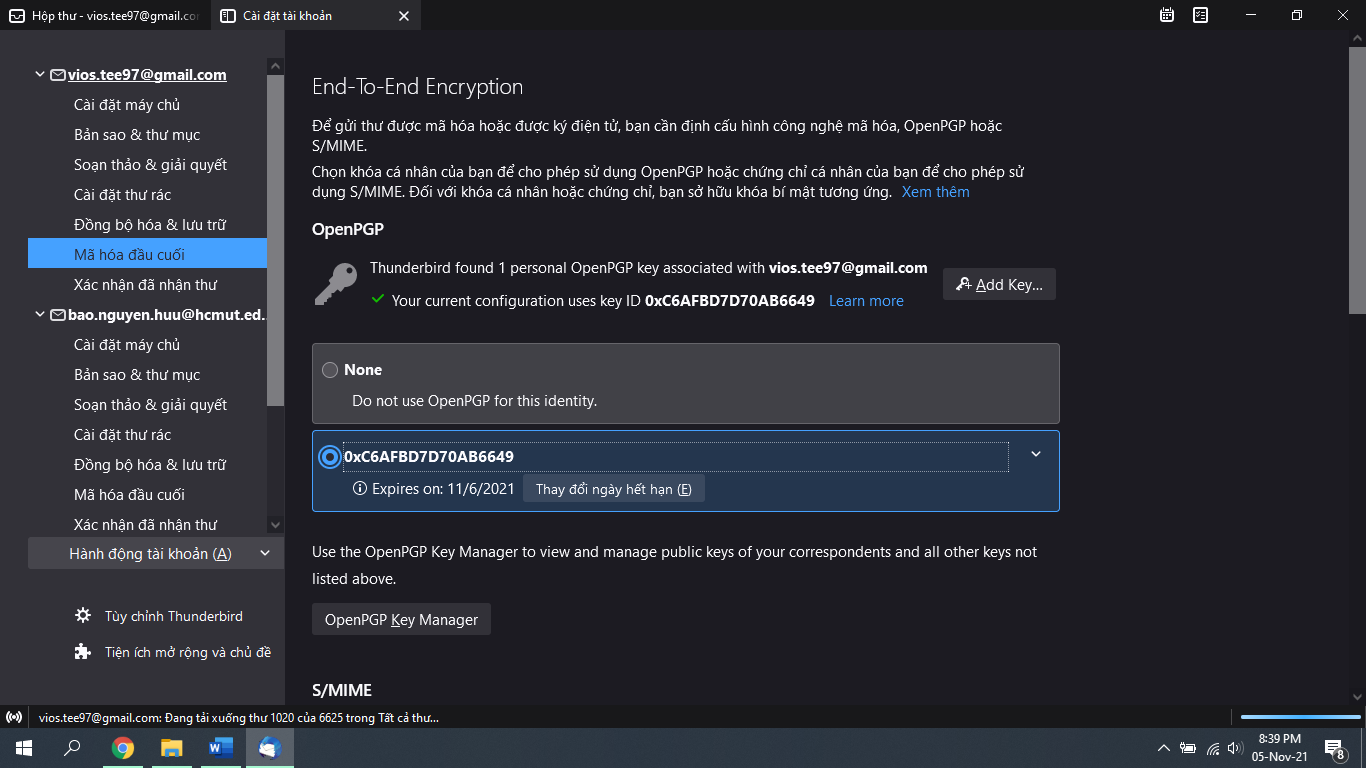
1. *Tạo cặp khóa từ OpenPGP Key Manager*

Từ **Tools-> OpenPGP Key Manager**, cửa sổ hiện ra là:



**Chọn Generate -> New Key Pair, cửa sổ hiện ra là:**

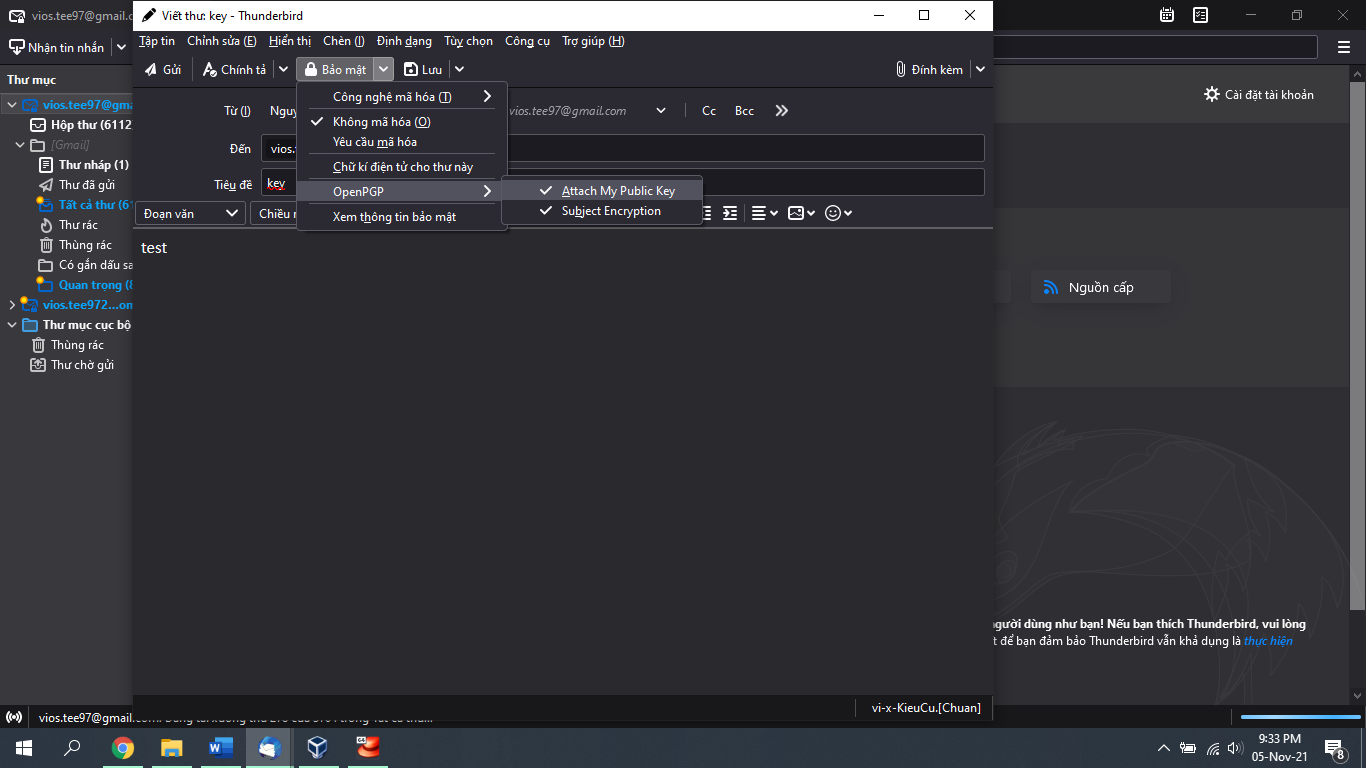




Thực hiện các bước tiếp theo để tạo cho tài khoản của mình một cặp khóa.

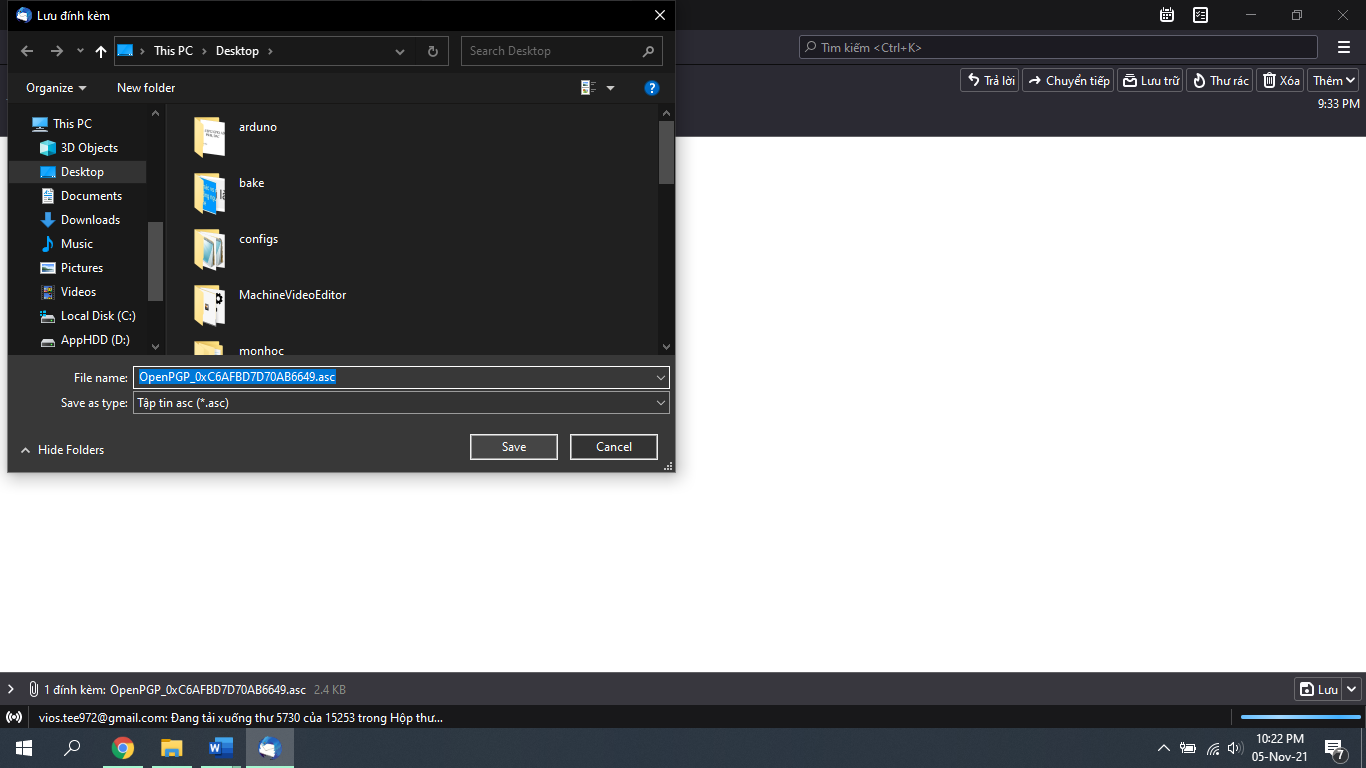
1. *Tạo thư và gởi đính kèm khóa công khai*

Nhấp vào “Write” để tạo một bức thư.gửi đến cho người bên cạnh có đính kèm khóa công khai của mình (chọn **Security** -> **Attach My Public Key).**



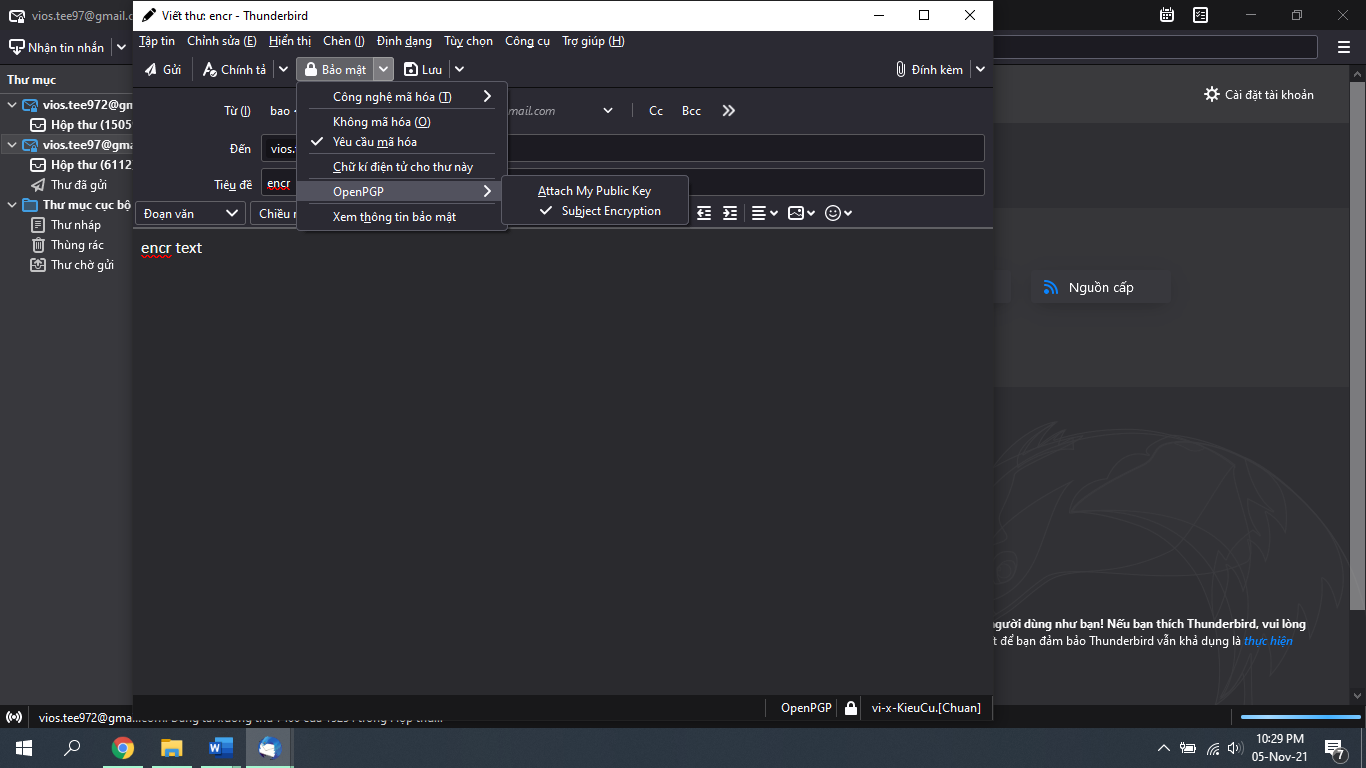
1. *Thêm khóa công khai của các người dùng khác*

Mở thư có chứa khóa công khai của bạn bên cạnh. Các bước tiếp theo là:



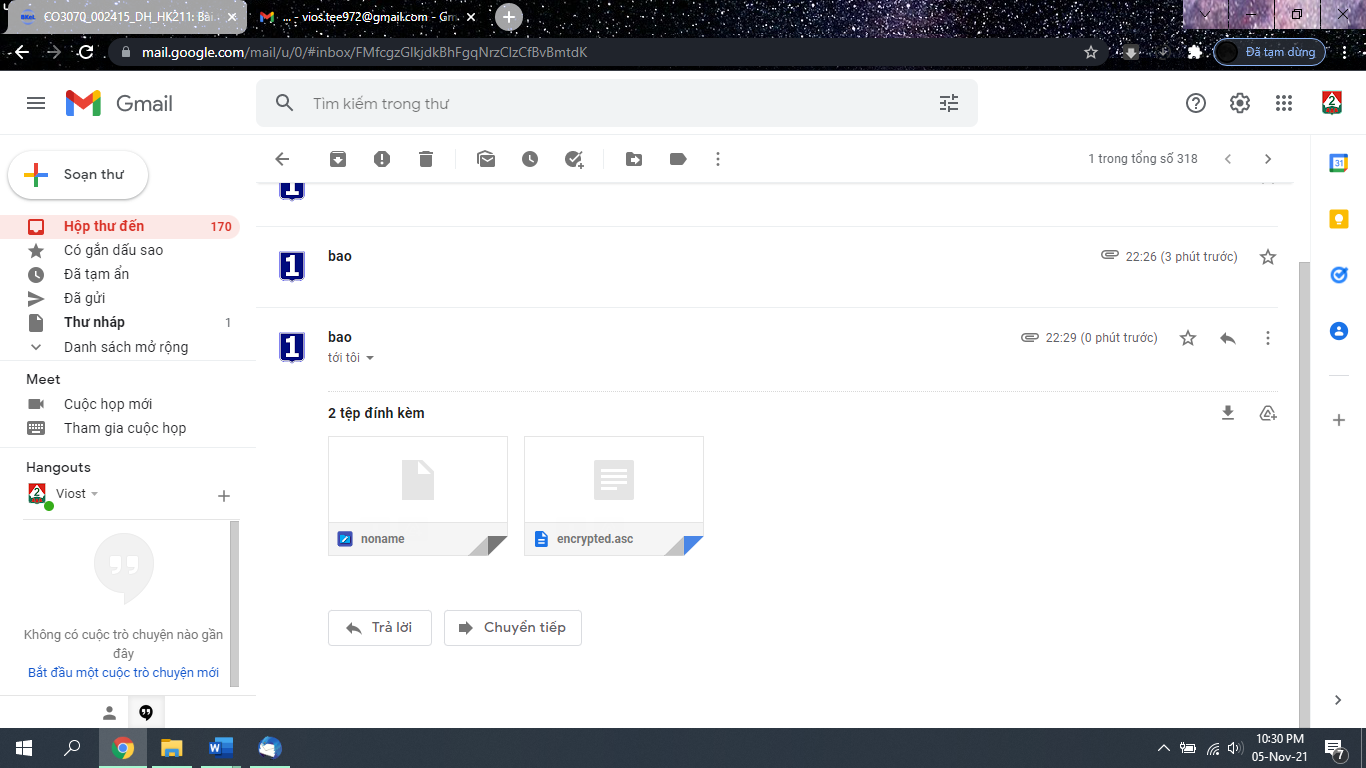
1. *Tạo thư, mã hóa và gửi đi*

Các bước thực hiện là:

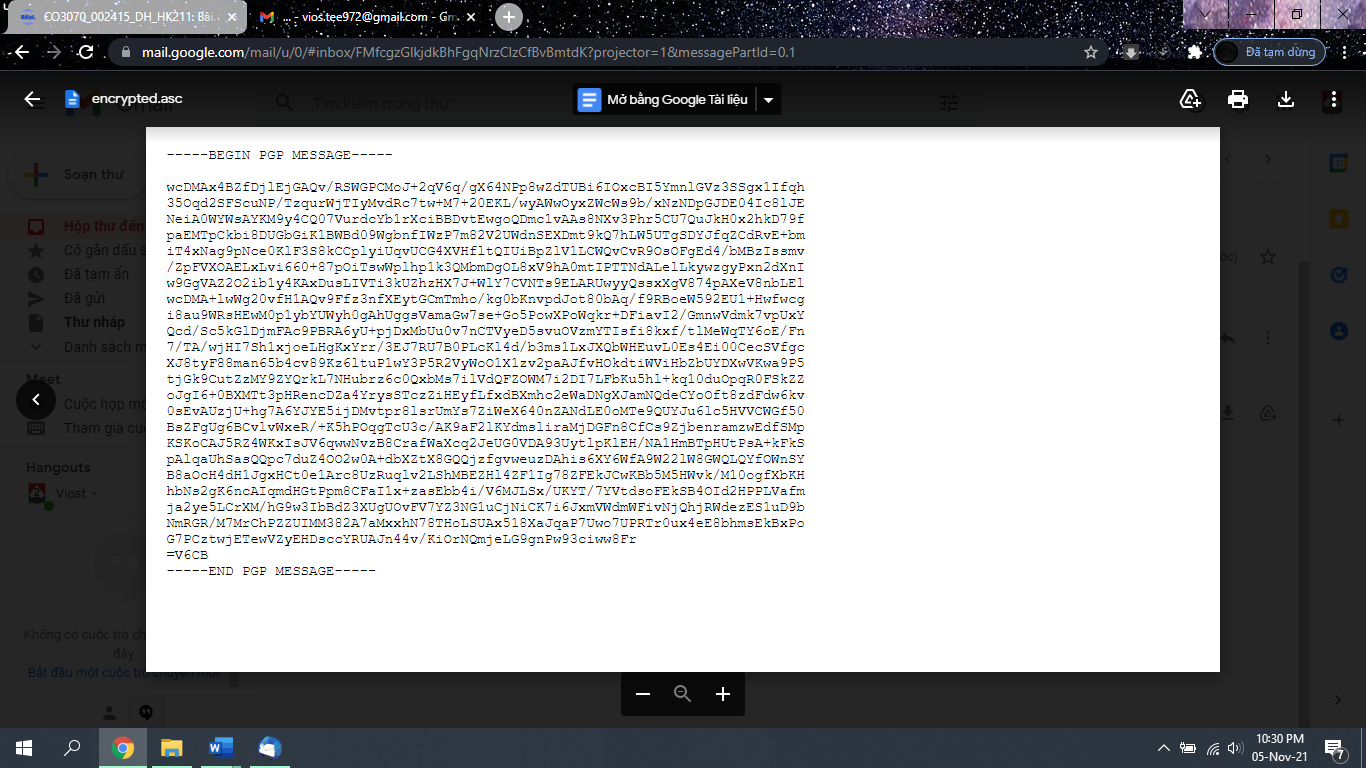


1. *Nhận thư. giải mã, đọc thư*

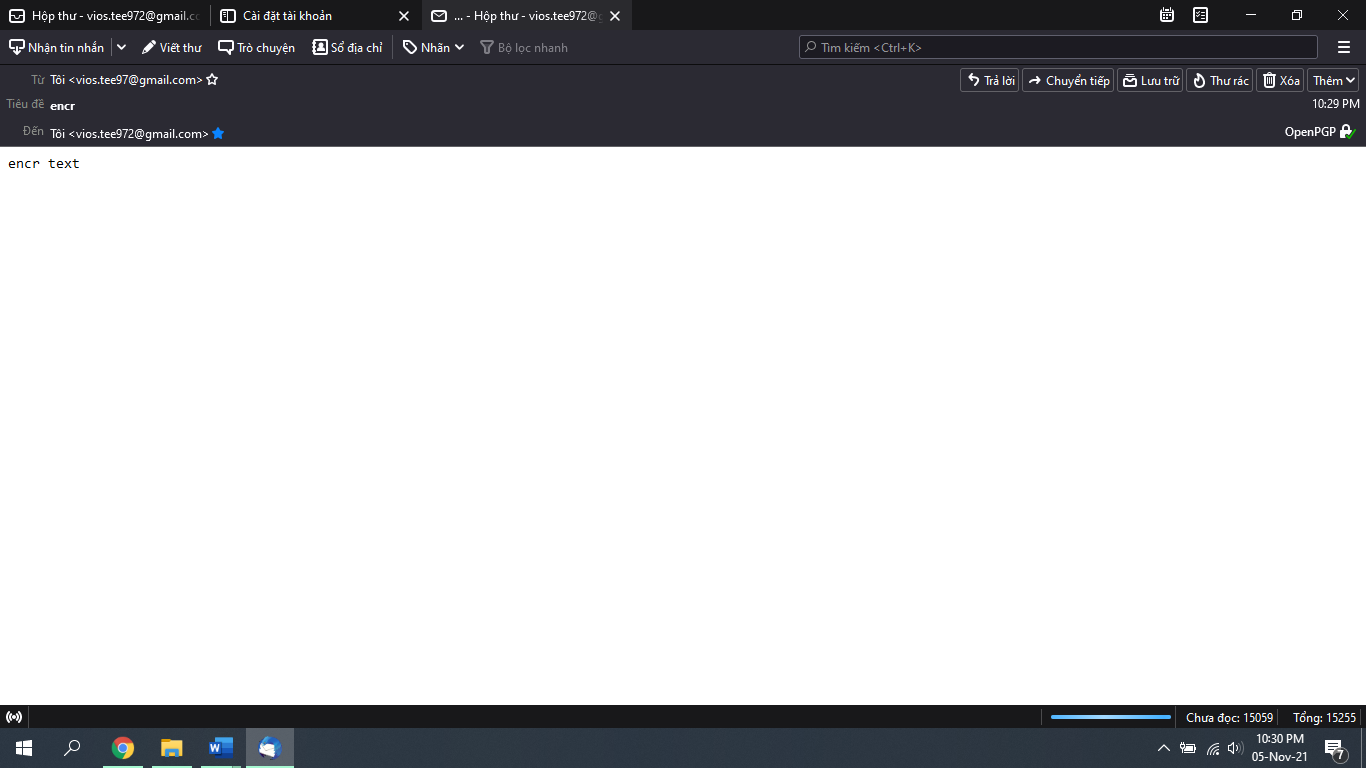
Các bước thực hiện là:



**Mở trình duyệt và đọc thư nói trên, cho biết nội dung thể hiện:**

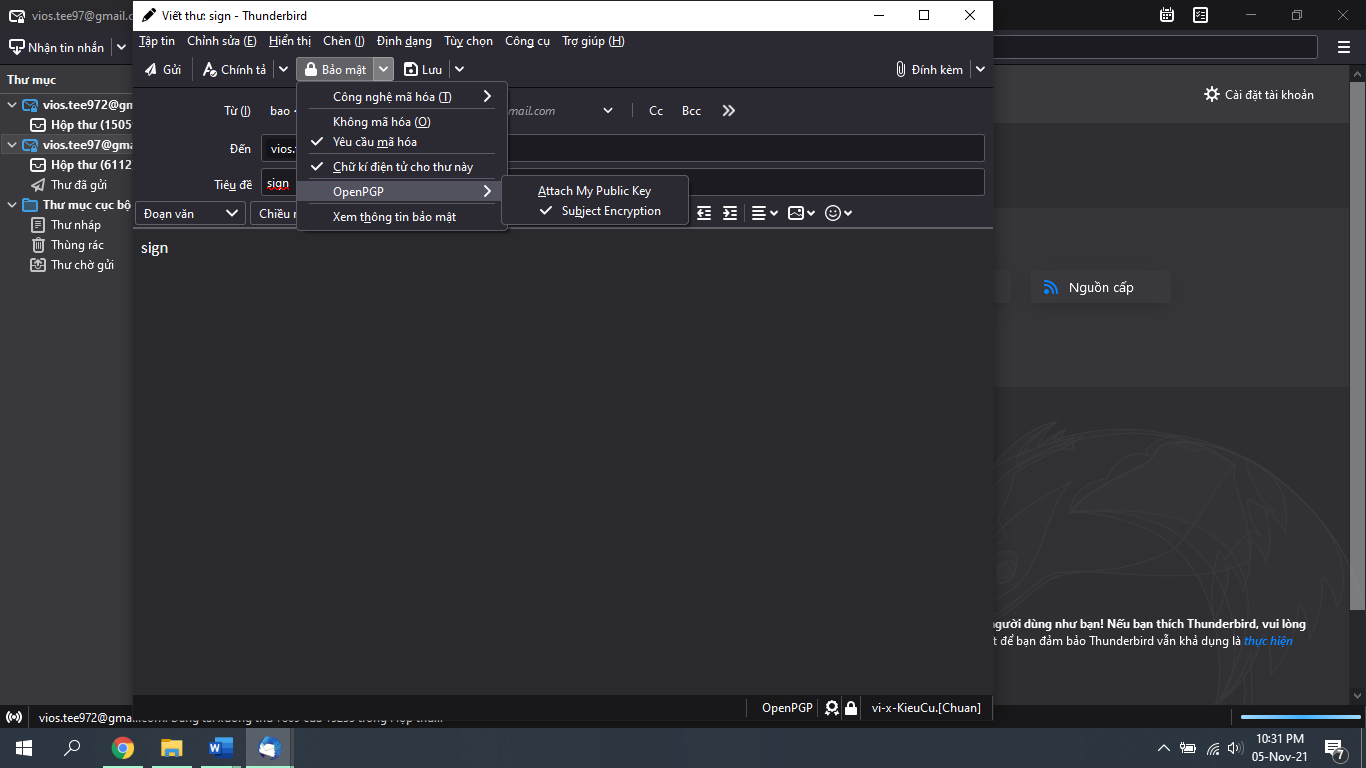


**Nếu mở bằng app thunderbird:**



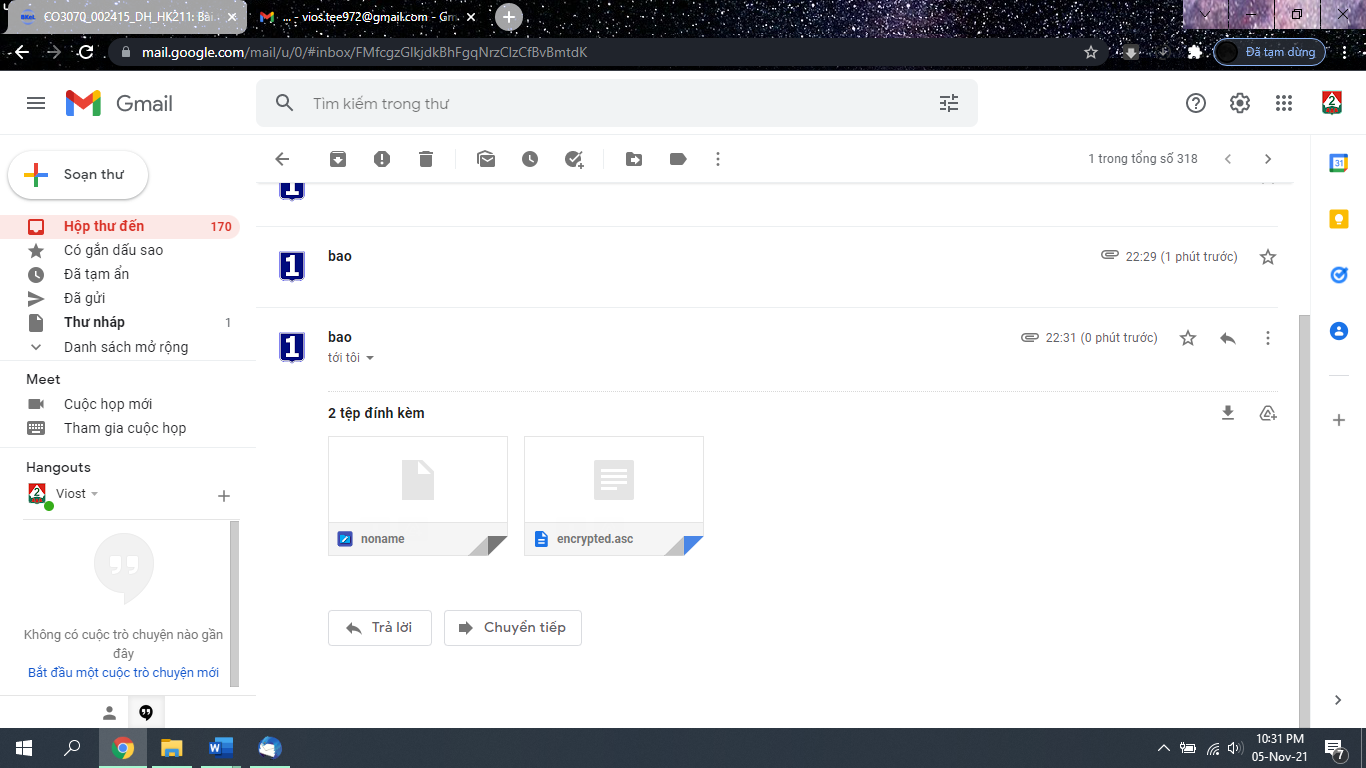
1. *Tạo thư, tạo chữ ký số, mã hóa và gửi đi*

Các bước thực hiện là:

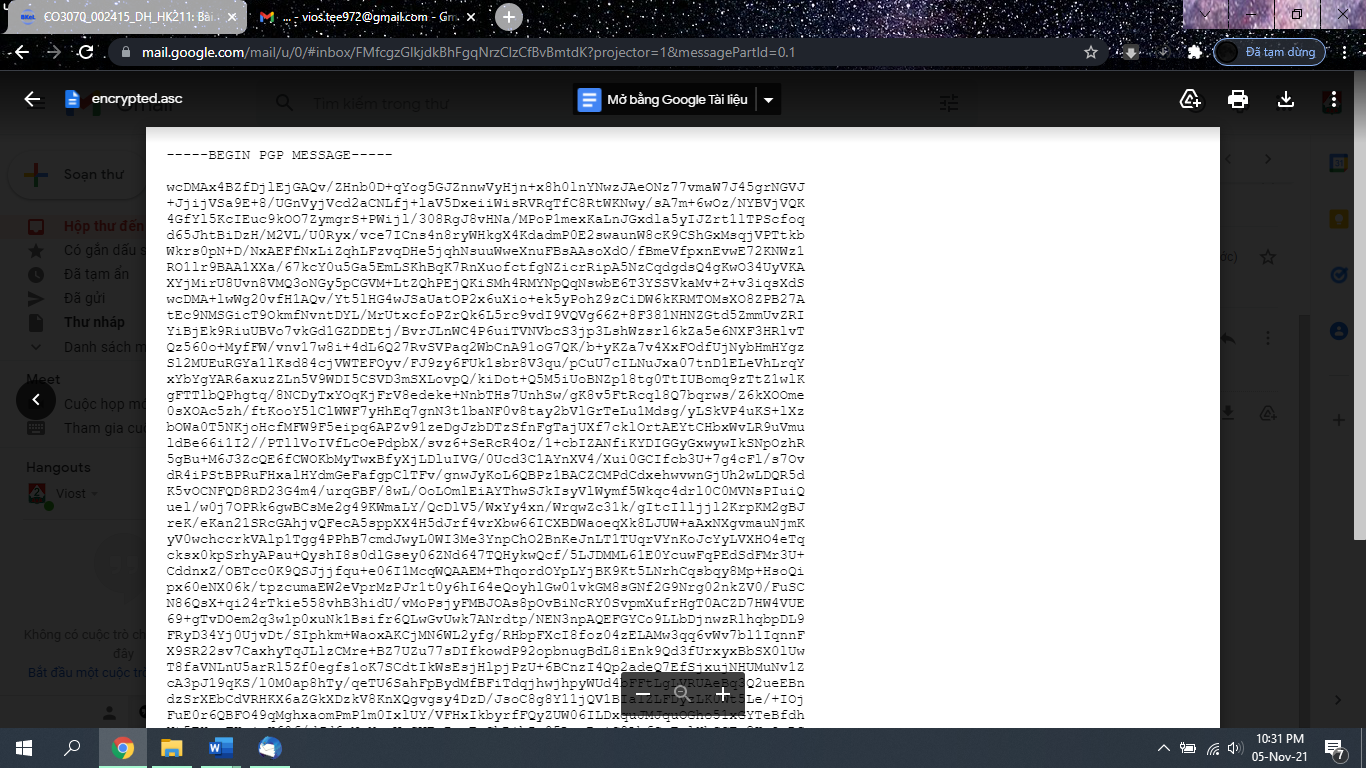


1. *Nhận thư. giải mã, xác minh chữ ký số, đọc thư*

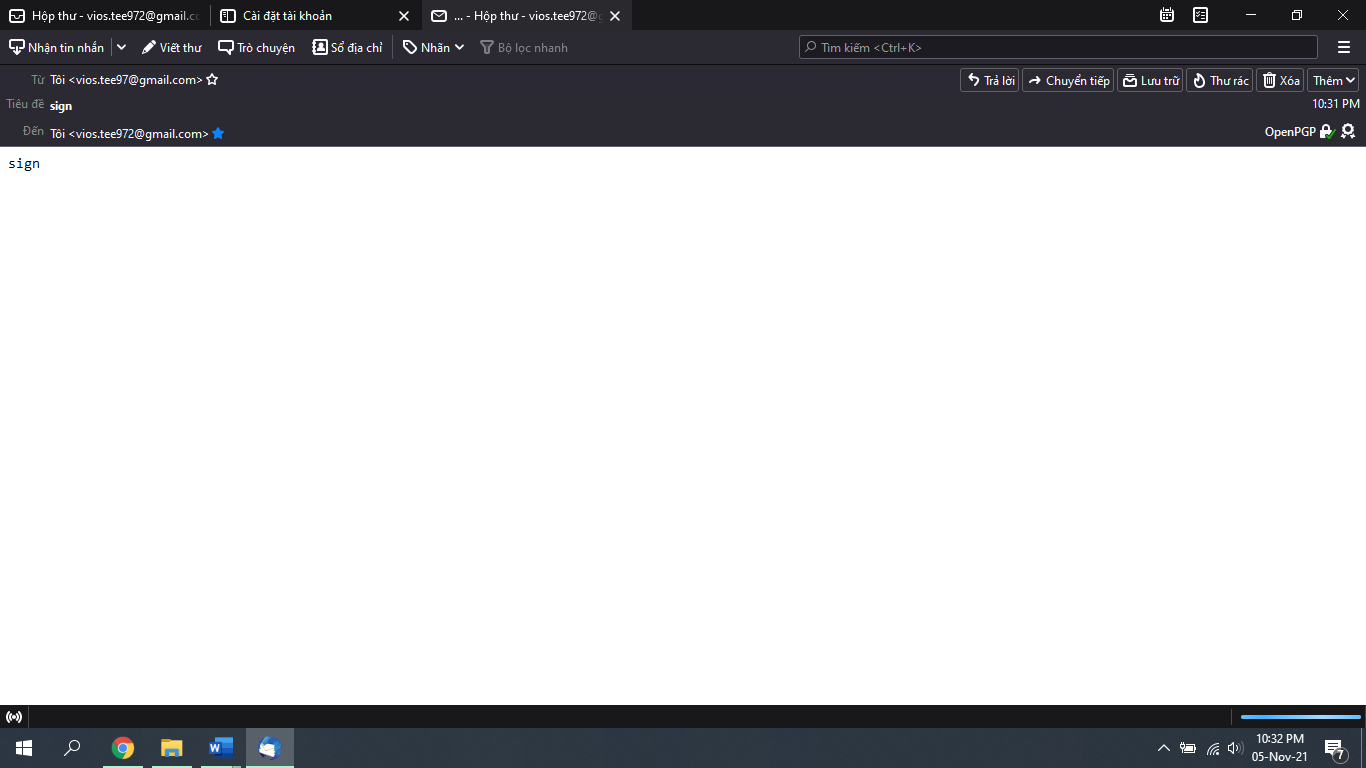
Các bước thực hiện là:



**Mở trình duyệt và đọc thư nói trên, cho biết nội dung thể hiện:**



**Nếu mở bằng app thunderbird:**



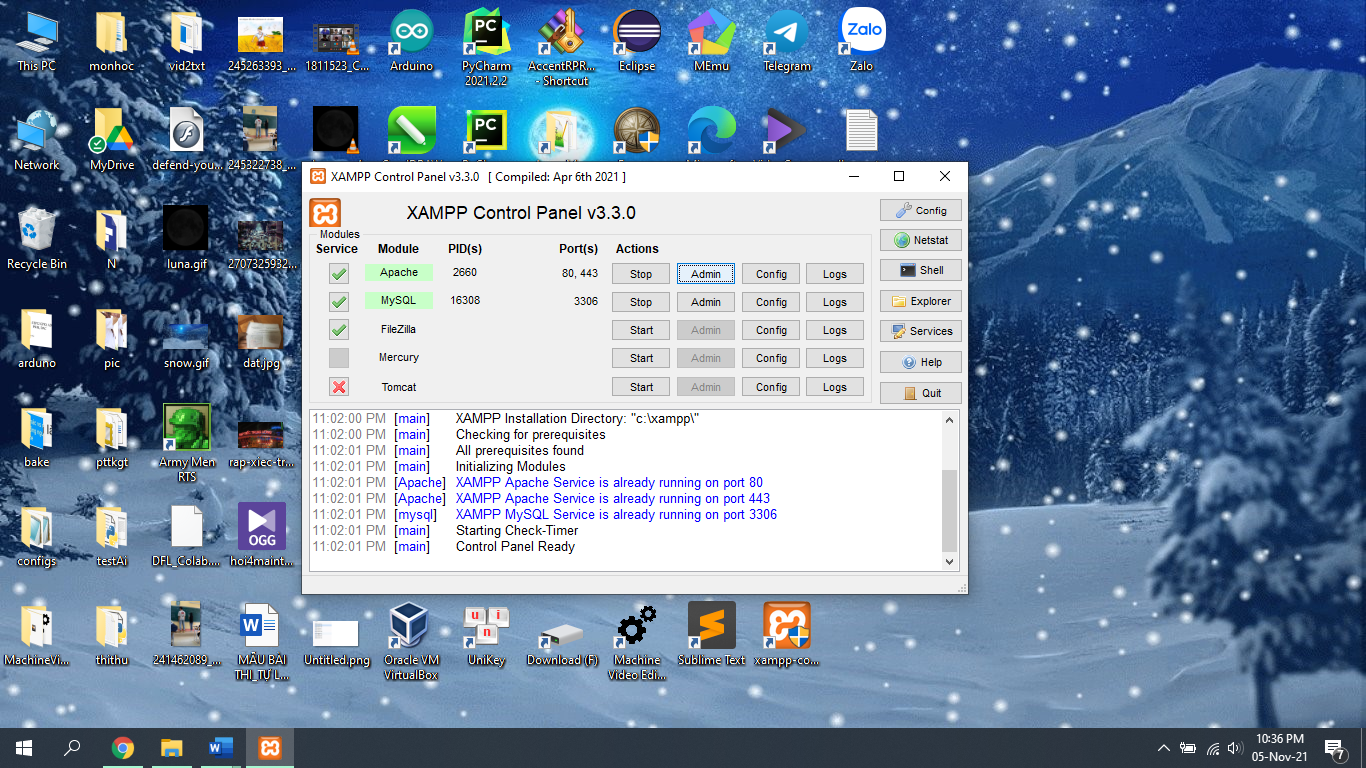
* + - * 1. **An ninh hệ thống Web**

1. *Cài đặt và cấu hình Apache Web Server*

**Apache** là phần mềm web server miễn phí mã nguồn mở. Tên chính thức của Apache là Apache HTTP Server được điều hành và phát triển bởi Apache Software Foundation.

Download Apache Web Server từ <https://httpd.apache.org/download.cgi>

Các bước ngắn gọn để cài đặt và cấu hình Apache Web Server**:**



**Lưu ý:**  [Cần disable IIS đối với các hệ điều hành MS Windows](https://windowsjet.com/disabling-iis-internet-information-services-in-windows-10-879/).

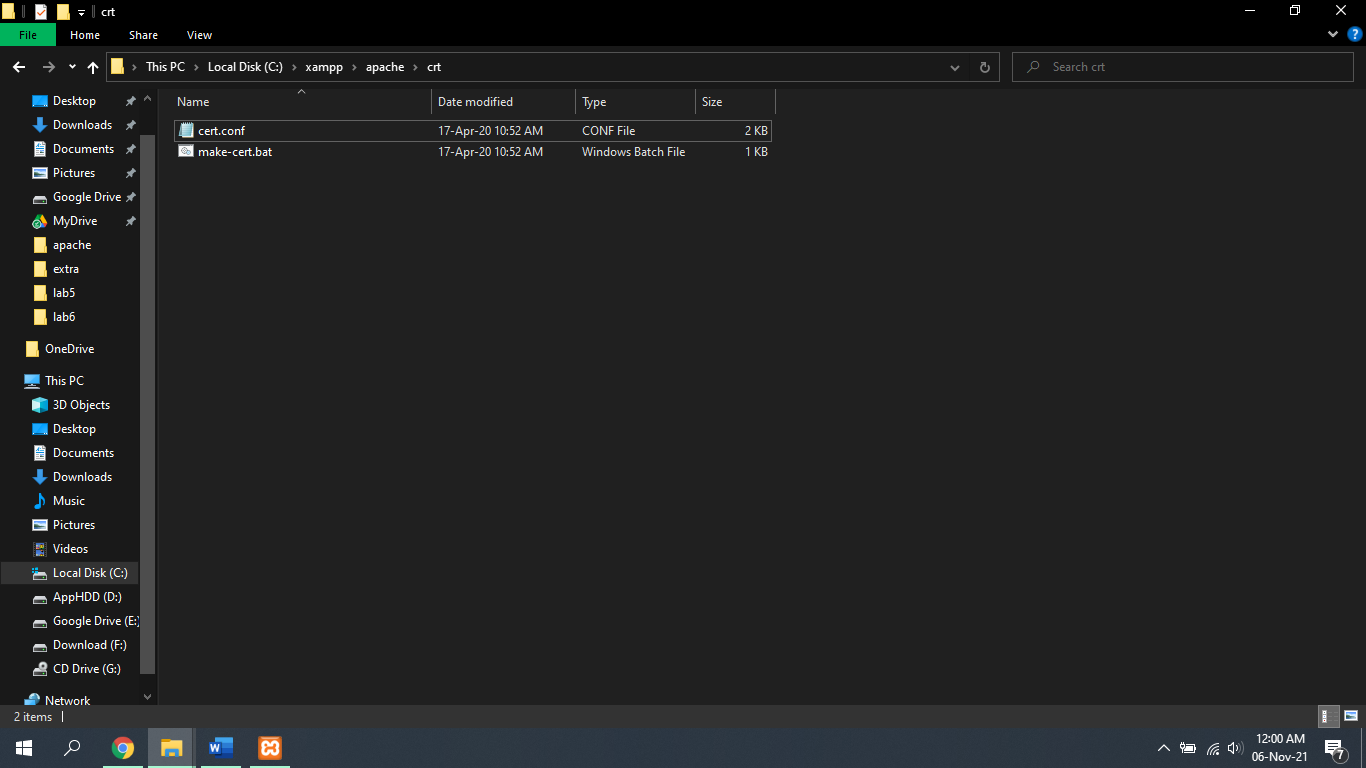
1. *Tạo chứng chỉ SSL tự ký bằng OpenSSL*

Các bước thực hiện là:

Tạo thư mục crt trong đường dẫn C:\xampp\apache



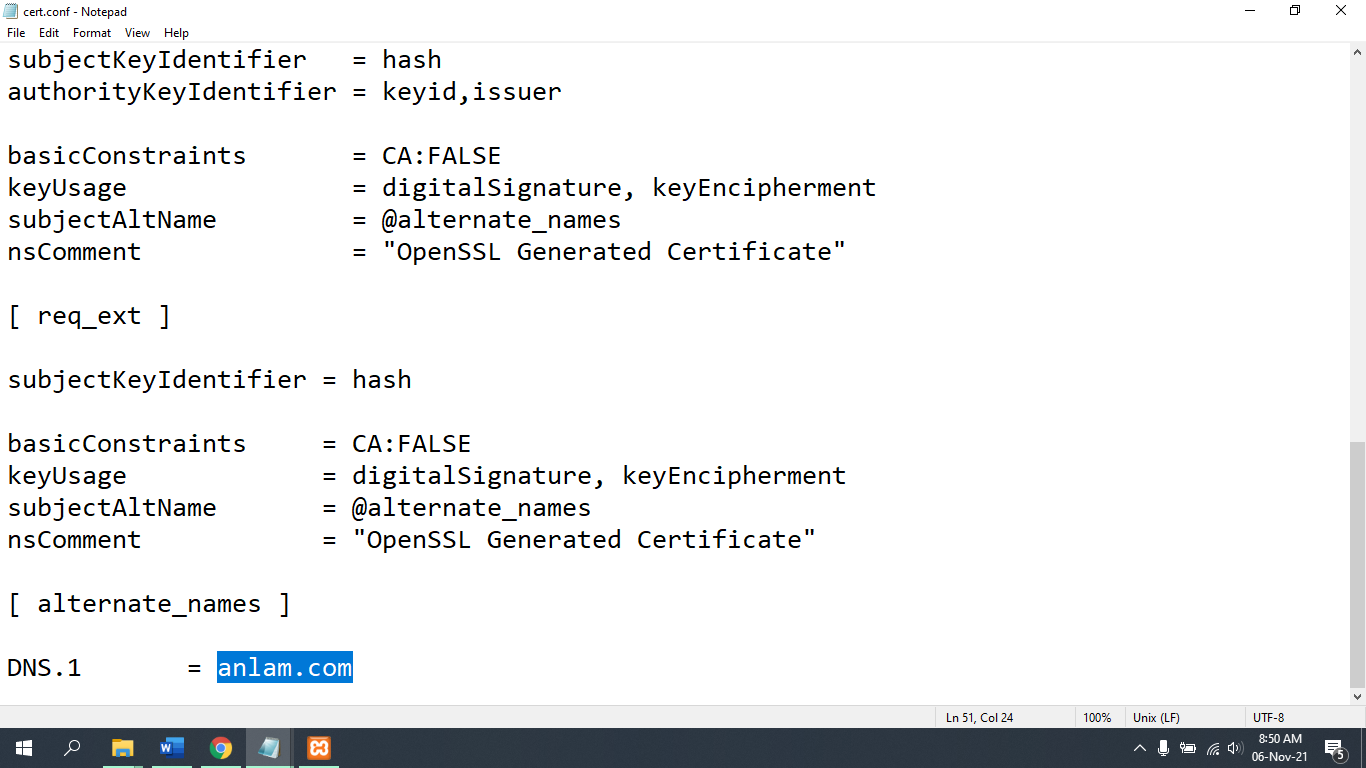
**Vào https://github.com/ngoisaoso/Enabling-SSL-with-XAMPP tải 2 tập tin cert.conf make-cert.bat về. 2 tập tin này sẽ dùng để tạo chứng chỉ SSL cho tên miền tùy thích.**



**Mở file cert.conf và thay đổi commonName mặc định thành tên tuỳ ý, ví dụ anlam.com**

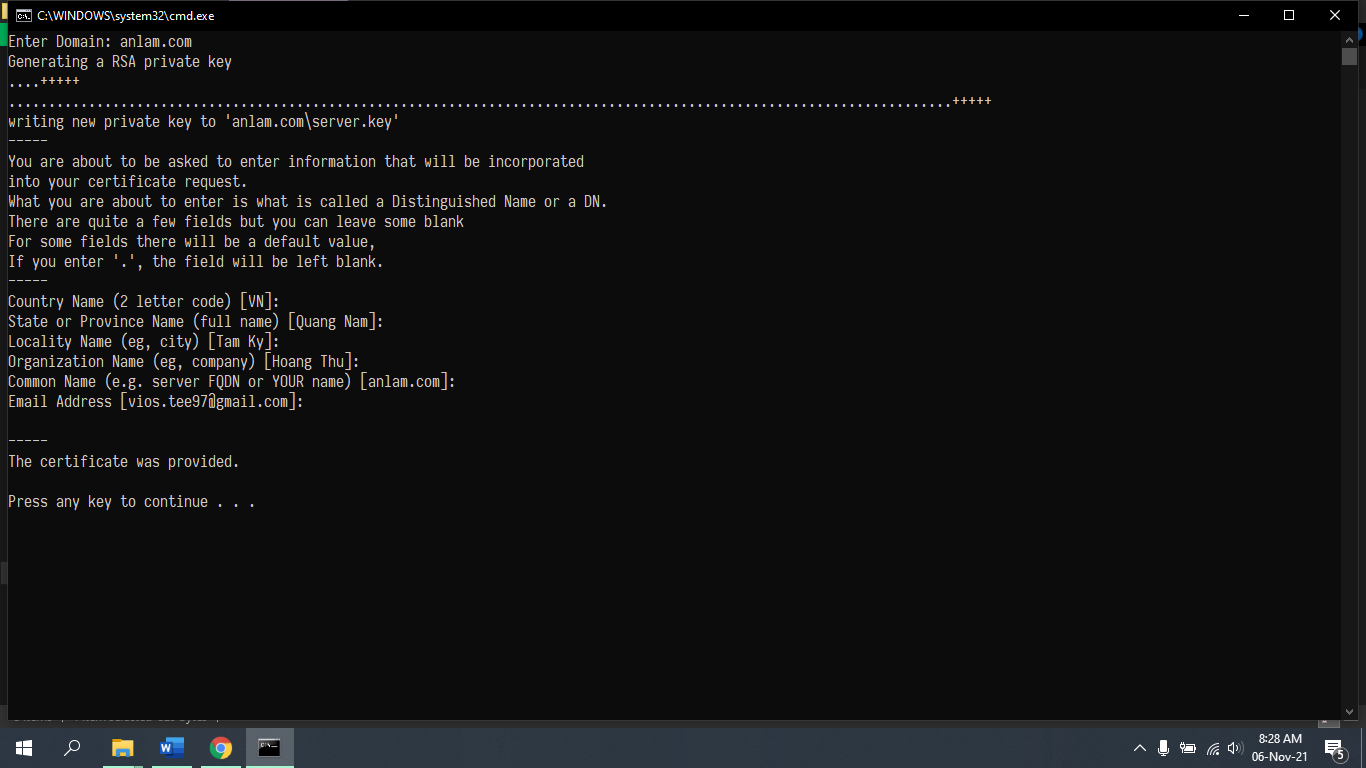


**Đổi DNS.1 thành anlam.com**

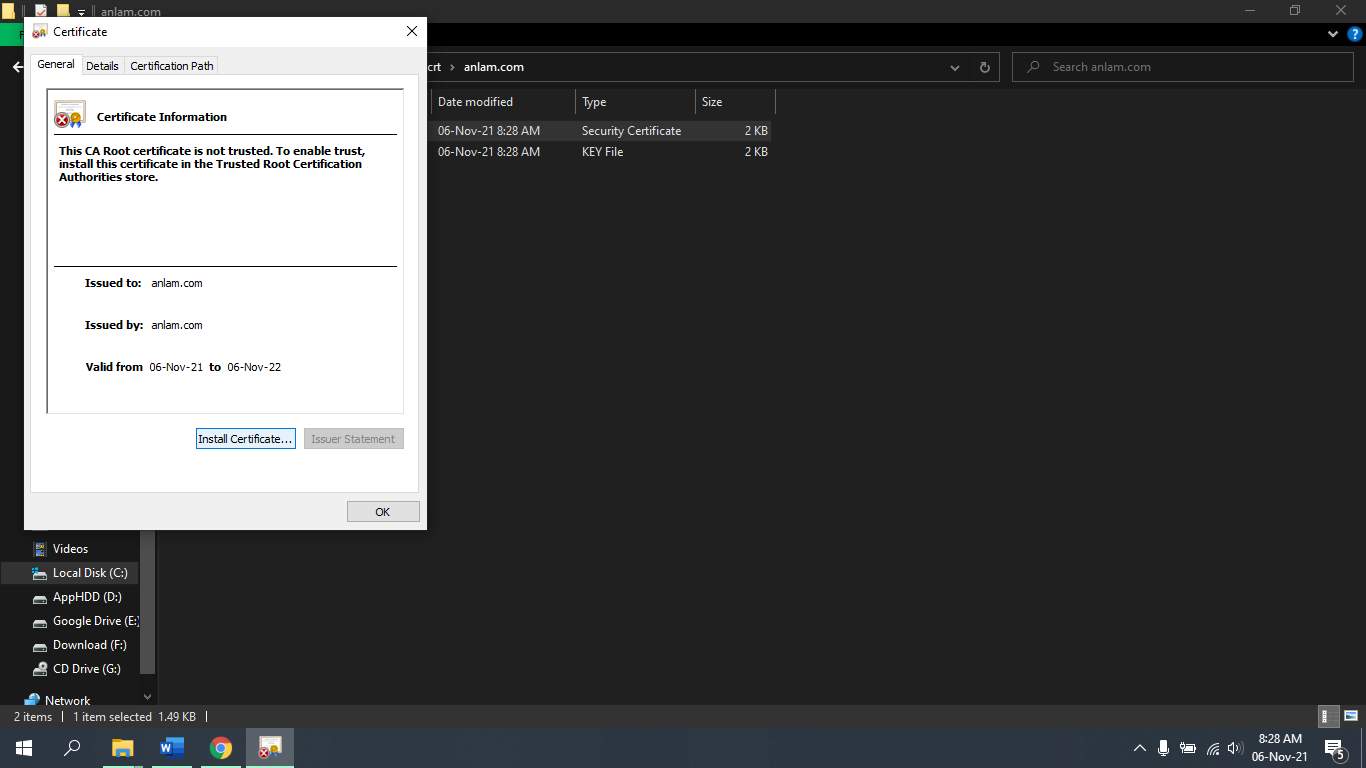


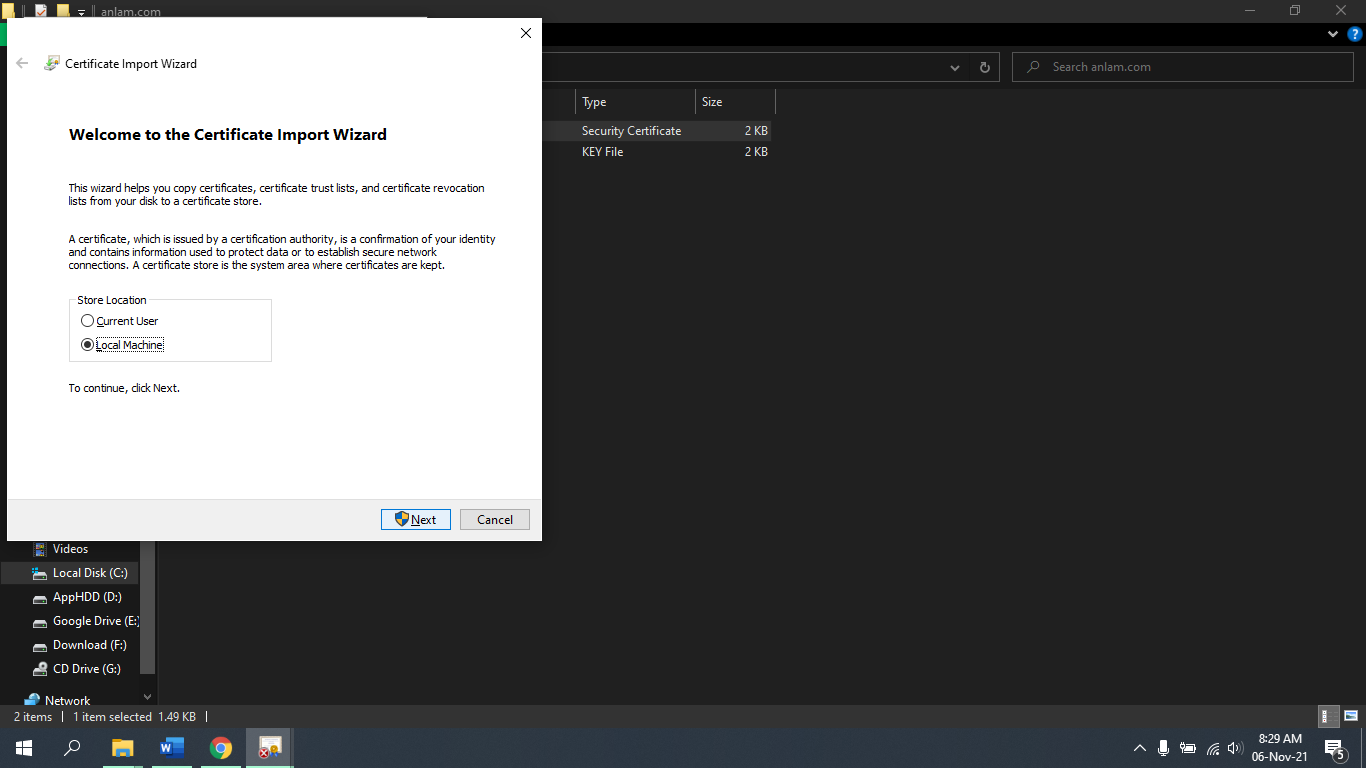
**Chạy make-cert.bat và nhập các thông tin cần thiết**

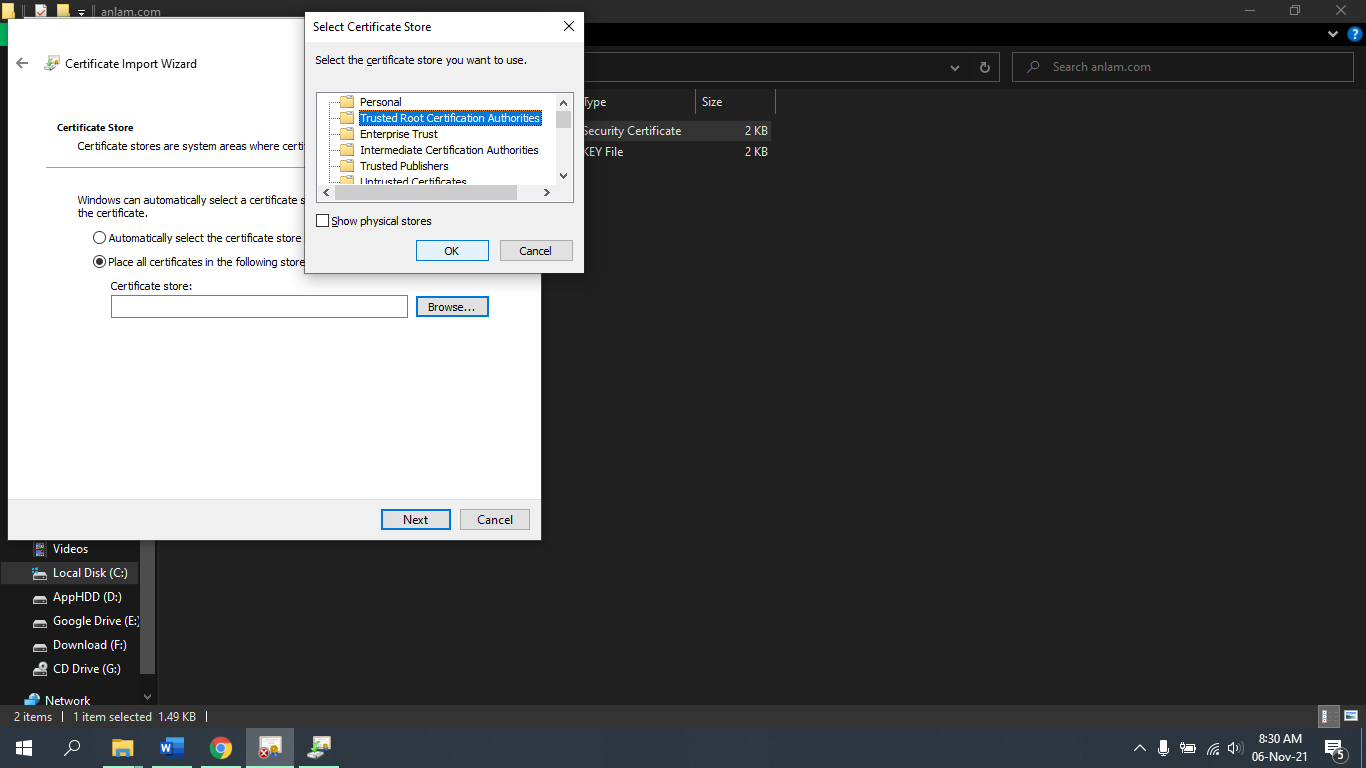
**Sau đó, bạn sẽ thấy thư mục cùng tên với tên commonName được tạo. Trong thư mục đó ta sẽ có server.crt and server.key. Đây là chứng chỉ SSL certificate.**

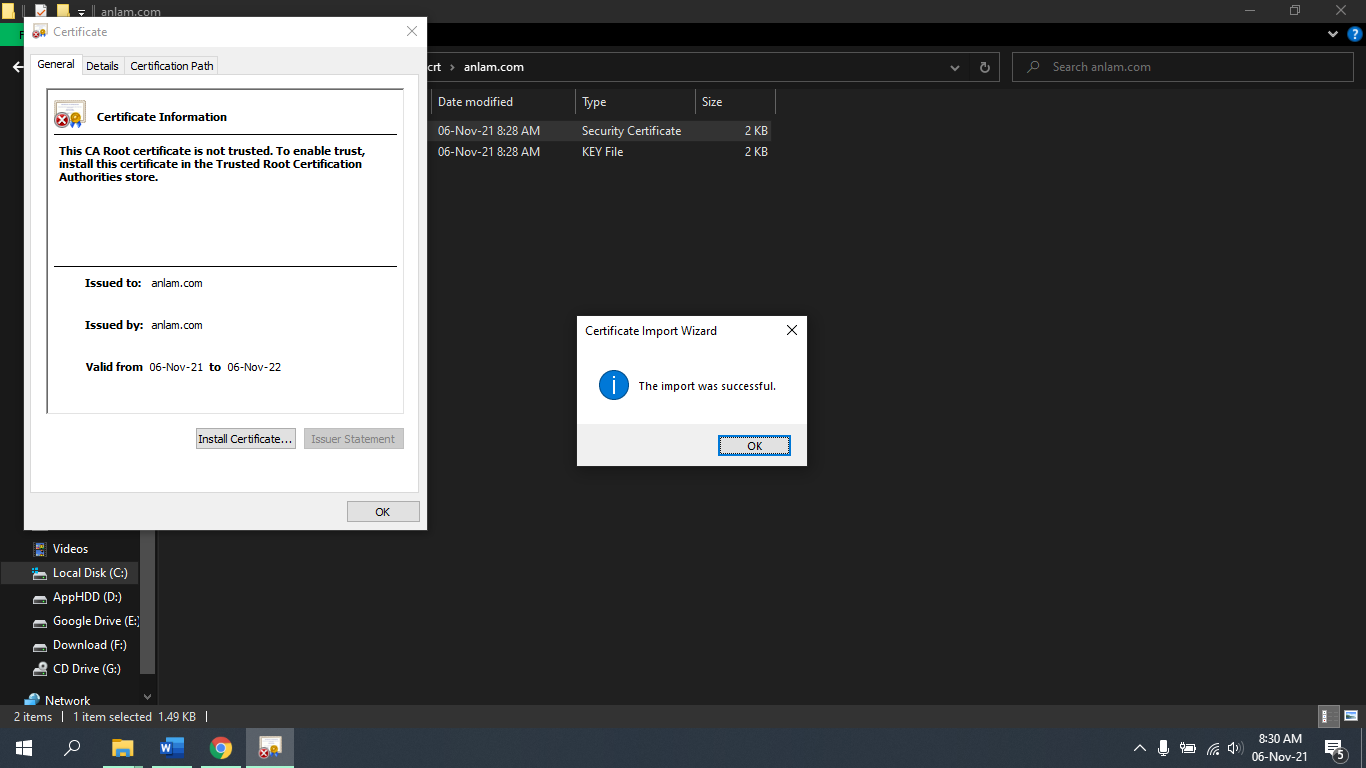


**Nhấp đúp chuột vào server.crt để cài đặt nó trên Windows**







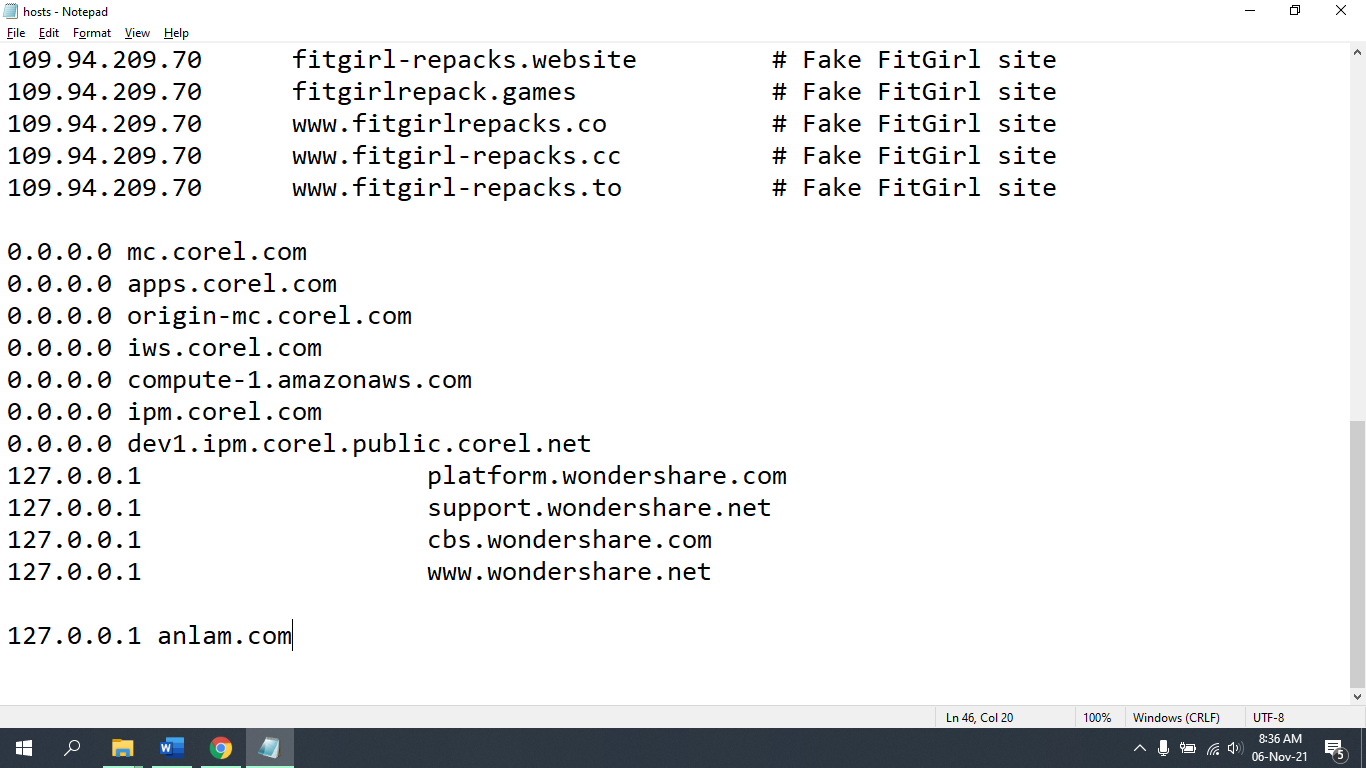


1. **Cài đặt Apache Web Server với chứng chỉ SSL đã tạo**

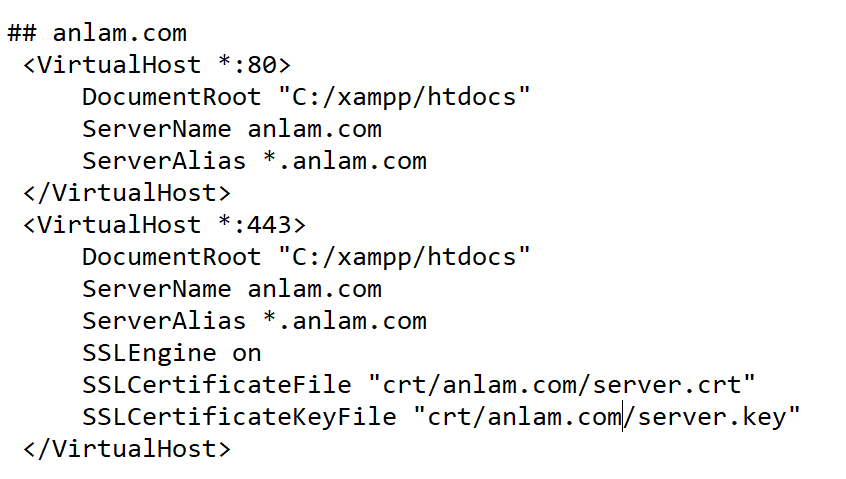
**Mở tệp C:\Windows\System32\drivers\etc\hosts và thêm dòng**

**127.0.0.1 anlam.com**

**Điều này sẽ giúp XAMPP khi truy cập http://anlam.com sẽ trỏ tên miền này về IP localhost**



**Mở tệp C:\xampp\apache\conf\extra\httpd-xampp.conf và thêm dòng mới này dưới cùng:**

****

**Khởi động lại apache, vào anlam.com**



1. **Tìm hiểu và cho biết khác biệt các loại chứng chỉ SSL (DV, OV, EV)**

**Xác thực miền (DV) là mức xác thực thấp nhất và xác minh rằng bất kỳ ai yêu cầu chứng chỉ sẽ kiểm soát miền mà nó bảo vệ.**

**Xác thực tổ chức (OV) xác minh danh tính của tổ chức (ví dụ: doanh nghiệp, tổ chức phi lợi nhuận hoặc tổ chức chính phủ) của người đăng ký chứng chỉ.**

**Xác thực mở rộng (EV), giống như OV, xác minh danh tính của một tổ chức. Tuy nhiên, EV thể hiện tiêu chuẩn tin cậy cao hơn OV và yêu cầu kiểm tra xác thực nghiêm ngặt hơn để đáp ứng tiêu chuẩn của Phần mở rộng của Diễn đàn trình duyệt / CA.**

**Khác biệt:**

**Chứng chỉ DV đã được xác thực miền là loại chứng chỉ SSL / TLS phổ biến nhất. Chúng chỉ được xác minh bằng cách sử dụng tên miền. Thông thường, CA trao đổi email xác nhận với một địa chỉ được liệt kê trong bản ghi WHOIS của miền. Ngoài ra, CA cung cấp tệp xác minh mà chủ sở hữu đặt trên trang web để được bảo vệ hoặc người nộp đơn tạo bản ghi DNS xác minh quyền kiểm soát của CA. Bất kỳ phương pháp nào trong số này đều xác nhận rằng miền được kiểm soát bởi bên yêu cầu chứng chỉ. Vui lòng xem yêu cầu Xác thực tên miền của SSL.com để biết thông tin về các phương pháp DV mà chúng tôi hỗ trợ.**

**Chứng chỉ OV thường được sử dụng bởi các tập đoàn, chính phủ và các tổ chức khác muốn cung cấp thêm một lớp niềm tin cho khách truy cập của họ. Ngoài chứng chỉ SSL / TLS, OV và IV cũng thường được sử dụng để ký mã, ký tài liệu, xác thực ứng dụng khách và chứng chỉ email S / MIME. Để biết thêm thông tin, vui lòng tham khảo các yêu cầu OV và IV của SSL.com.**

**Chứng chỉ EV cung cấp mức độ tin cậy tối đa cho khách truy cập và cũng yêu cầu CA nỗ lực nhiều nhất để xác thực. Theo nguyên tắc do CA / Diễn đàn trình duyệt đặt ra, tài liệu bổ sung phải được cung cấp để cấp chứng chỉ EV (như được mô tả trong các yêu cầu EV của SSL.com). Như với OV, EV liệt kê tên công ty trong chính chứng chỉ. Chứng chỉ EV chỉ có thể được cấp cho các doanh nghiệp và các tổ chức đã đăng ký khác, không được cấp cho cá nhân.**

1. **Cho biết cách tạo và duy trì chứng chỉ SSL miễn phí từ Let’s Encrypt**

**Vào Control Panel của tài khoản hosting, chọn Truy cập SSH.**

-HẾT-