BÀI THỰC HÀNH SỐ 6

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lê Bảo Khánh**

**MSSV: 1911363**

**Nhóm: L01**

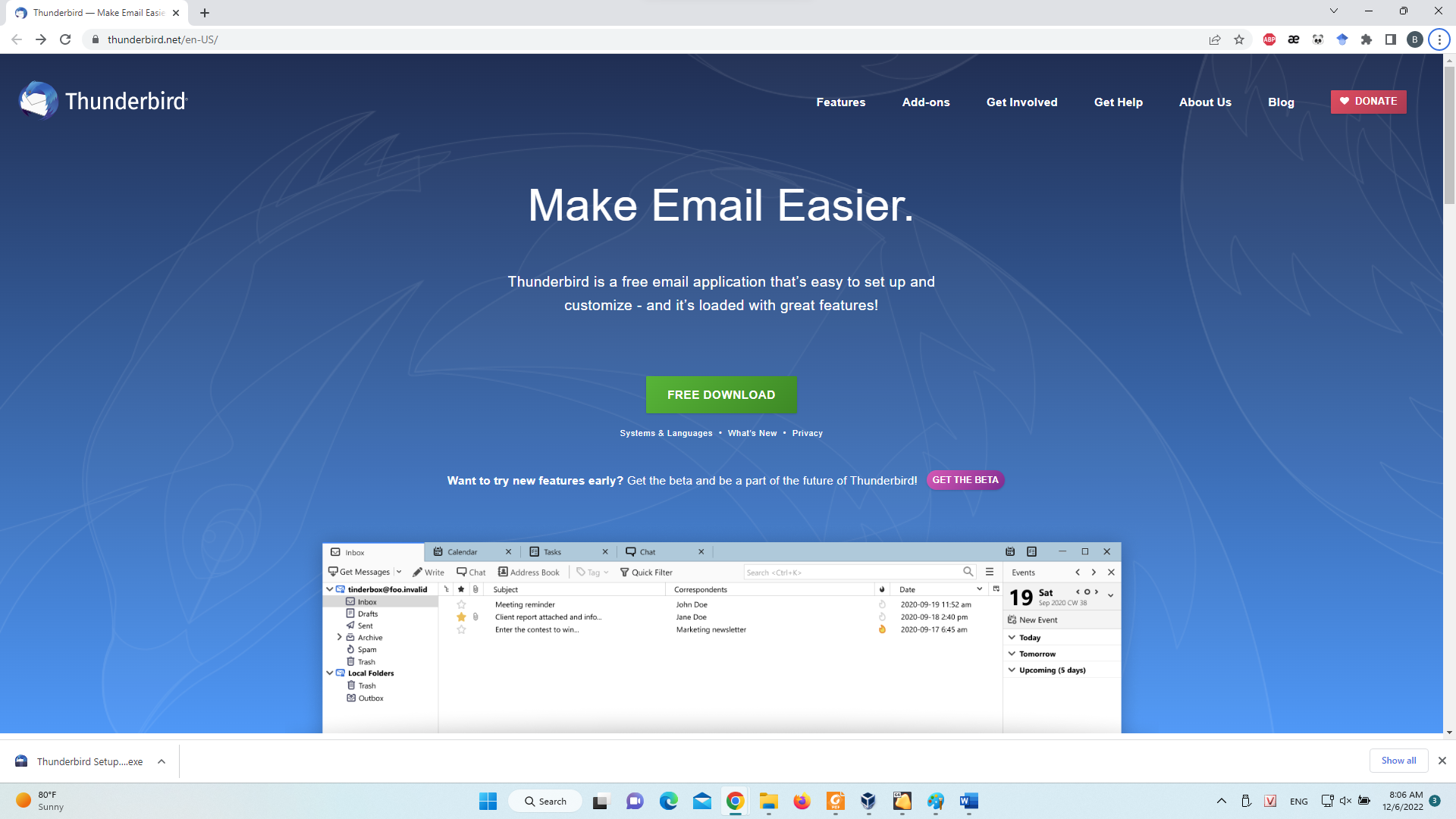
* + - * 1. **An ninh hệ thống E-mail cá nhân**

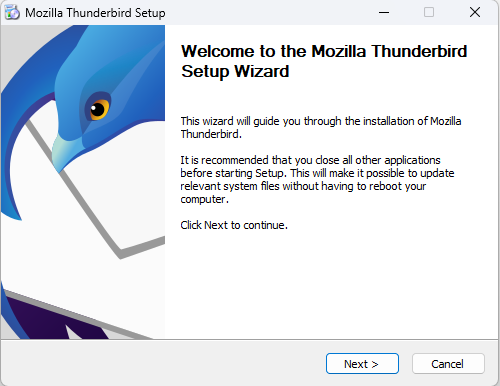
1. *Cài đặt Mozillla Thunderbird*

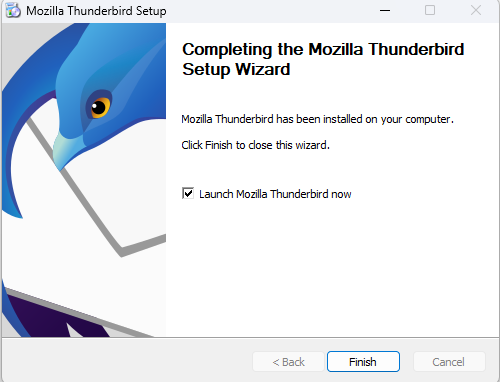
**Mozilla Thunderbird** là chương trình miễn phí, nguồn mở hoạt động trên mọi nền tảng hệ điều hành giúp quản lý việc nhận, gửi và lưu trữ thư điện tử. Một phần mềm quản lý thư điện tử phía người dùng là một chương trình giúp bạn tải về và quản lý thư điện tử mà không cần sử dụng trình duyệt Internet. 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**:**

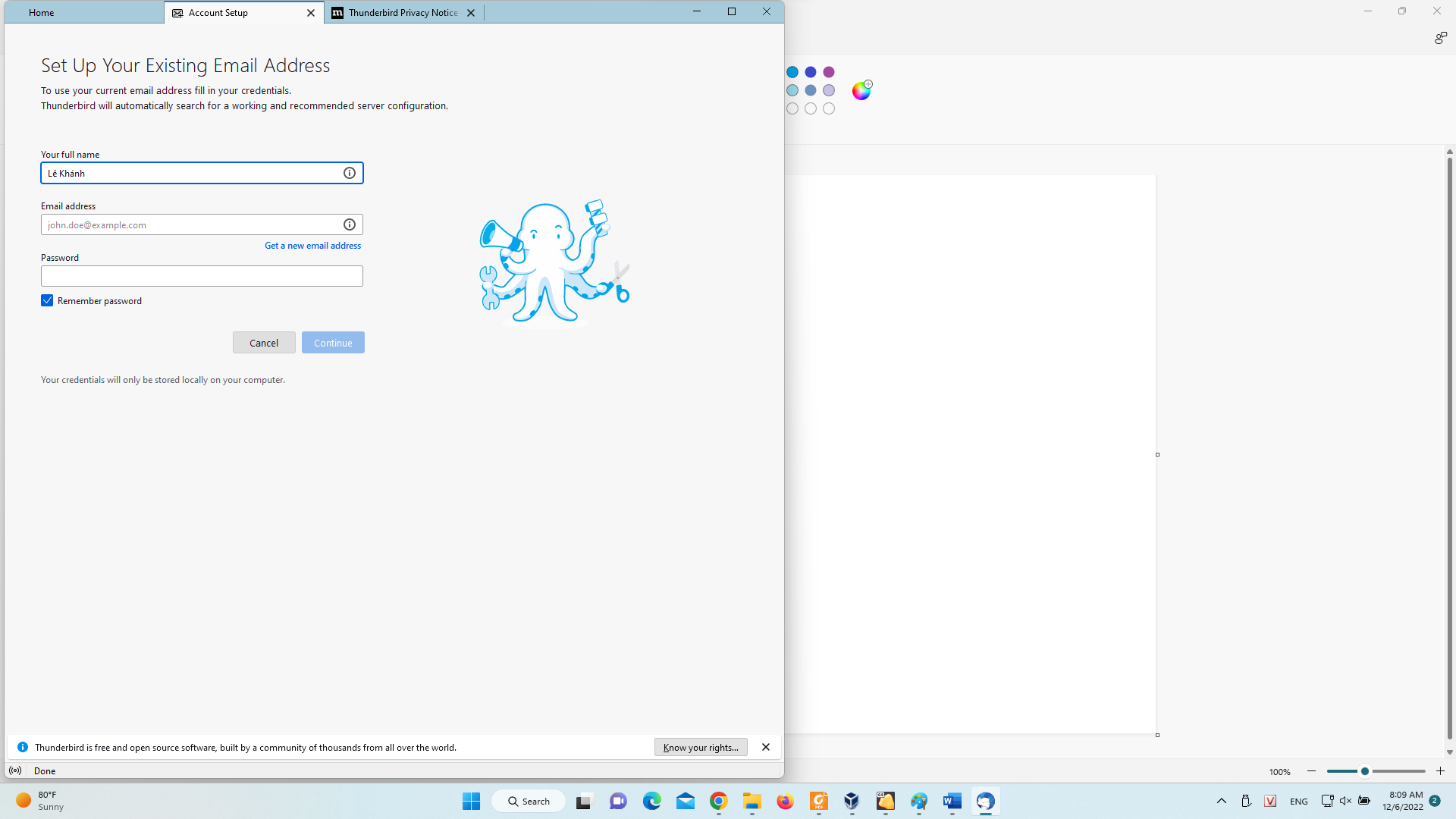
****

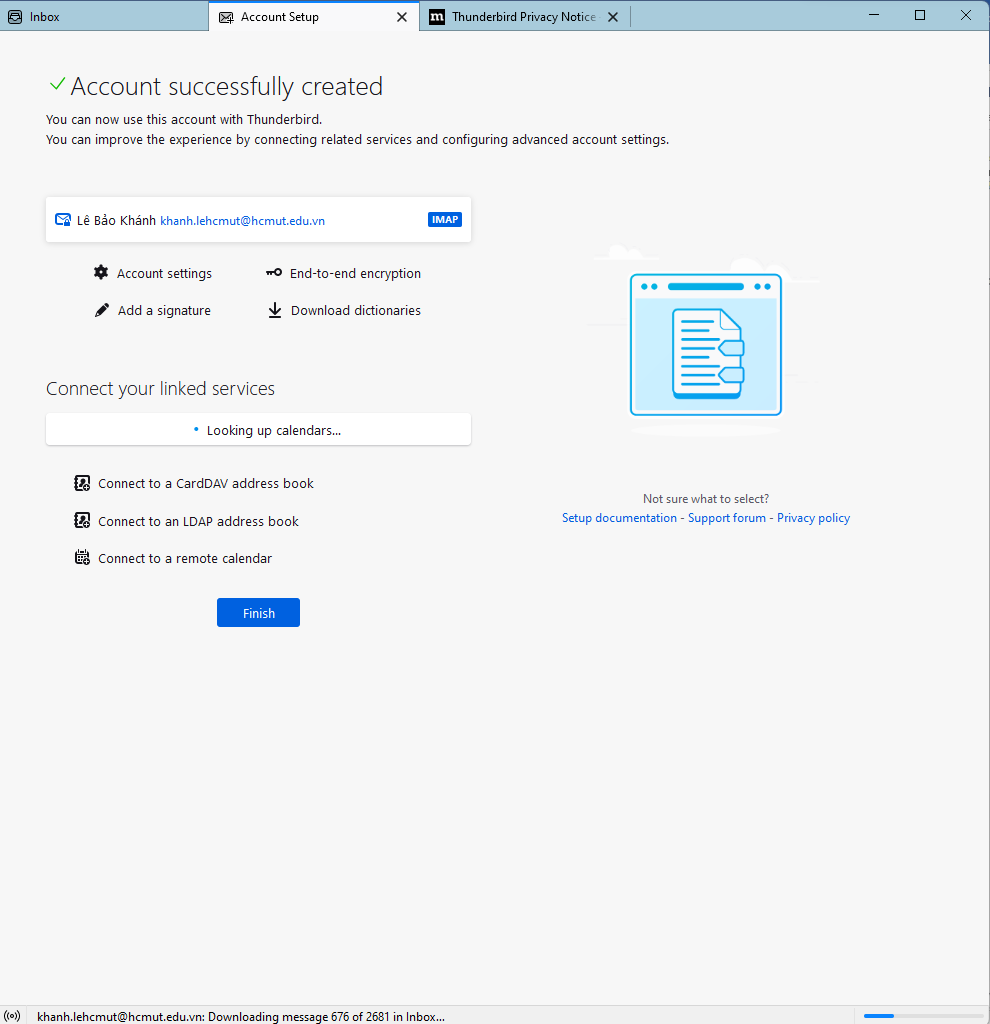
****

****

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:

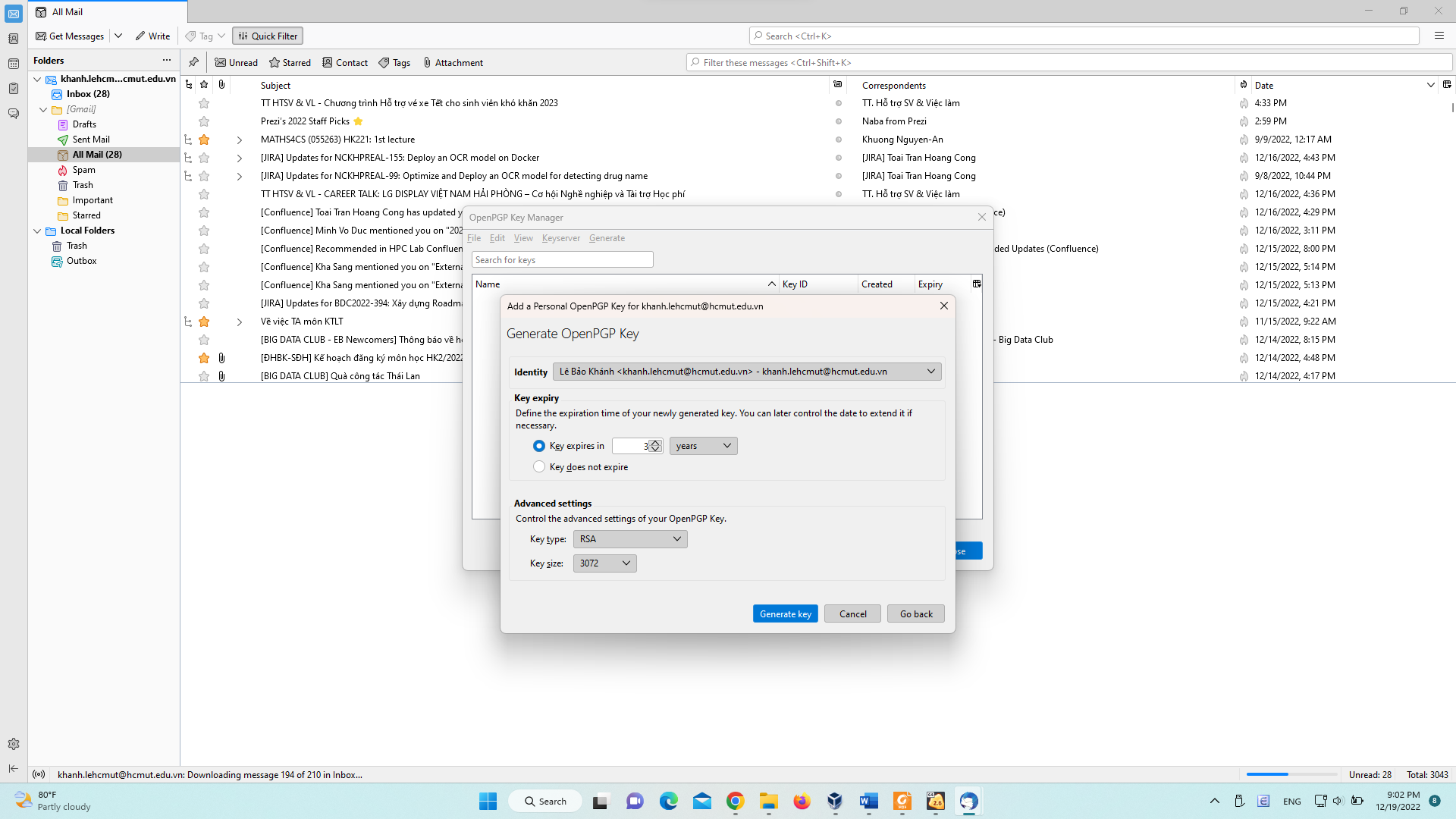
****

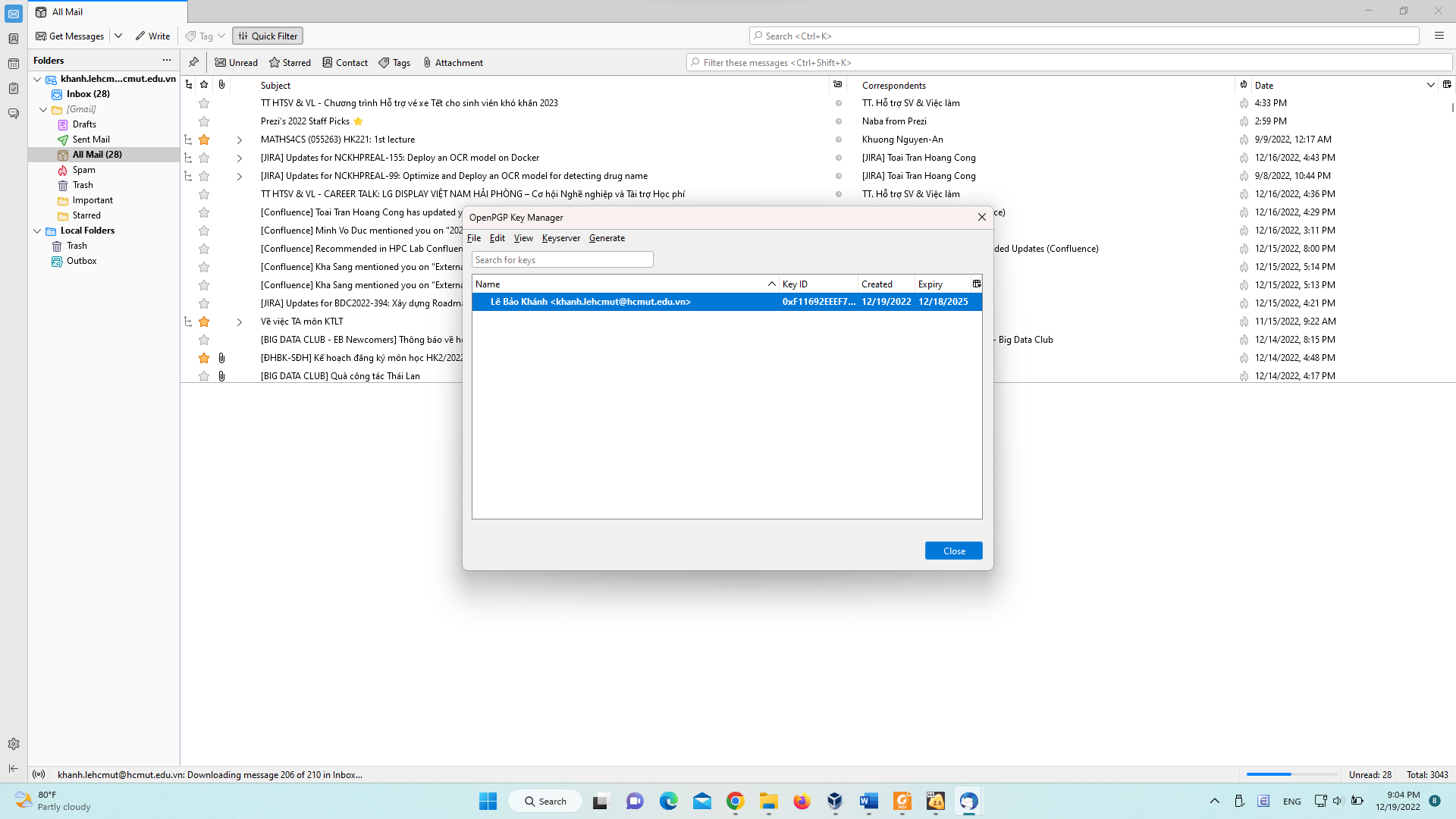
****

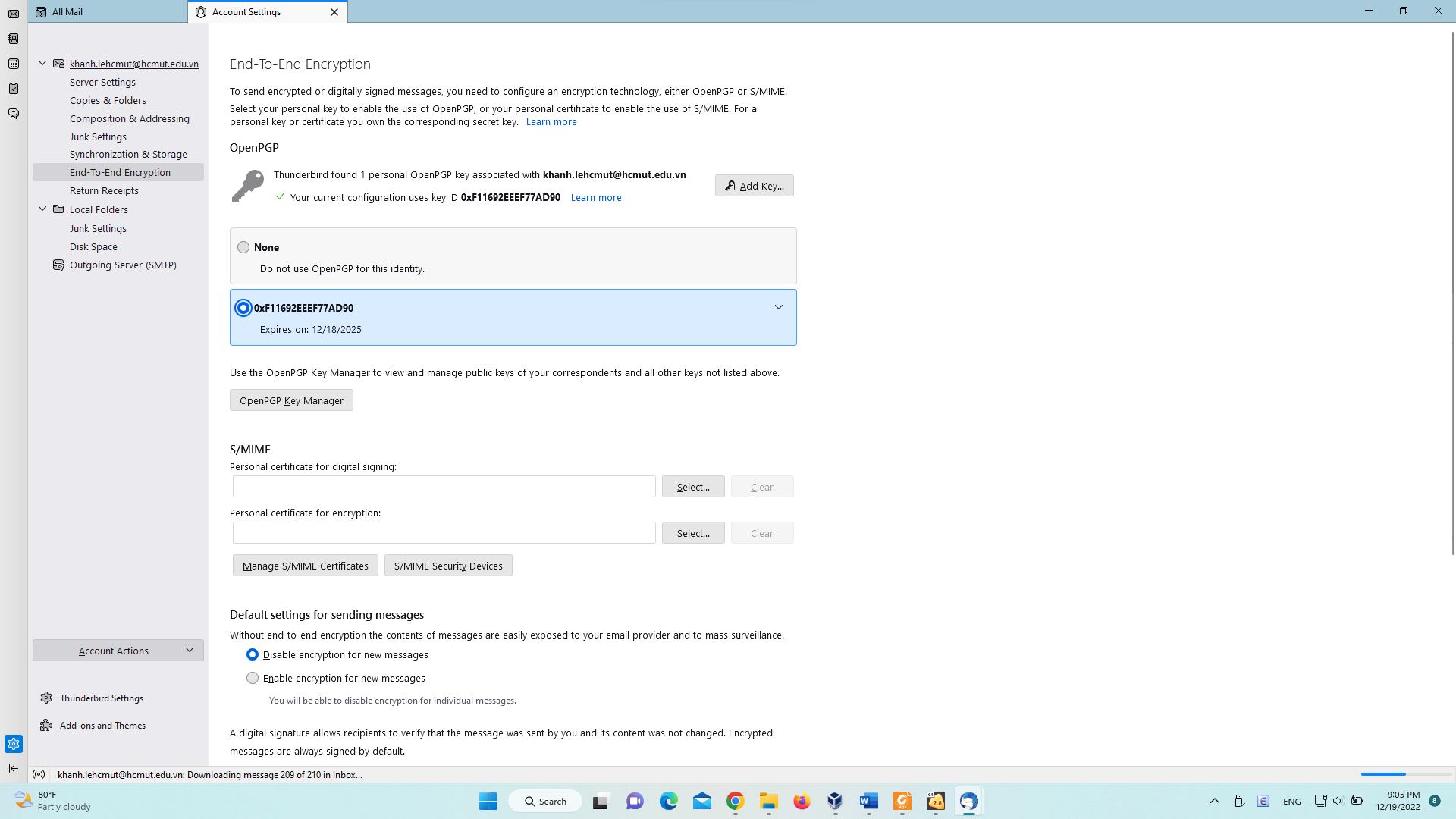
1. *Tạo cặp khóa từ OpenPGP Key Manager*

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

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

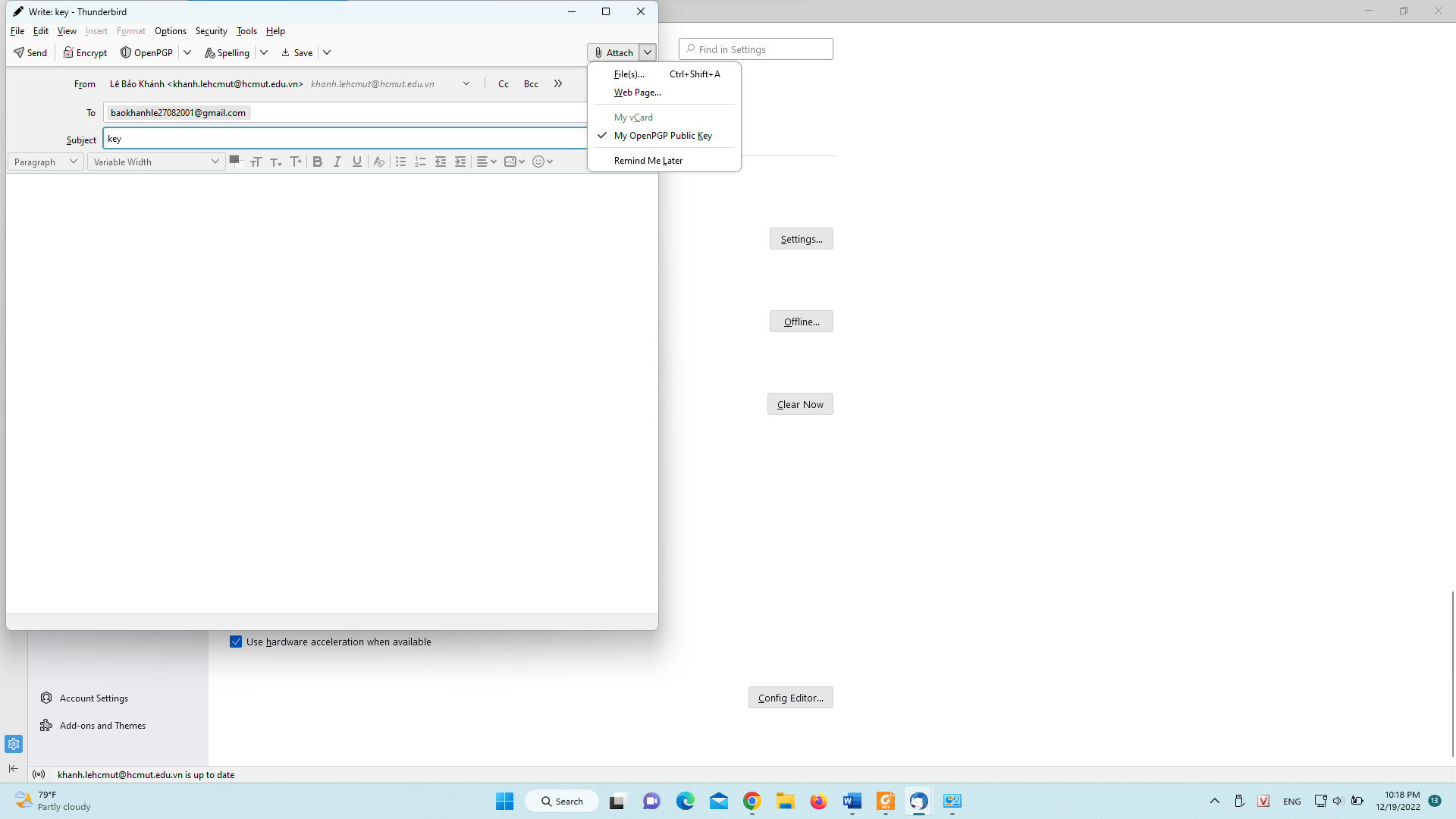
**** Thực hiện các bước tiếp theo để tạo cho tài khoản của mình một cặp khóa.





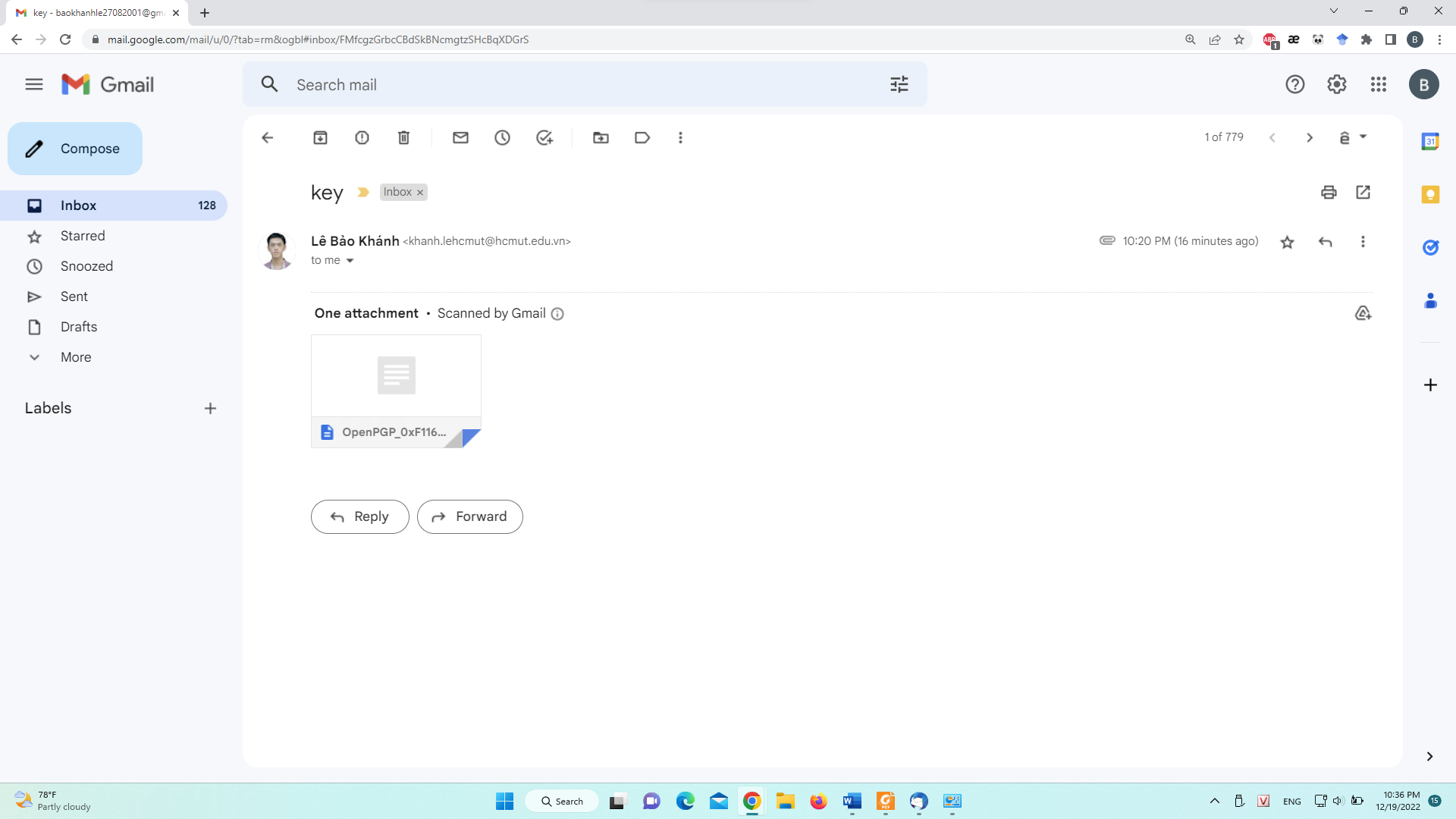
1. *Tạo thư và gởi đính kèm khóa công khai*

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

****

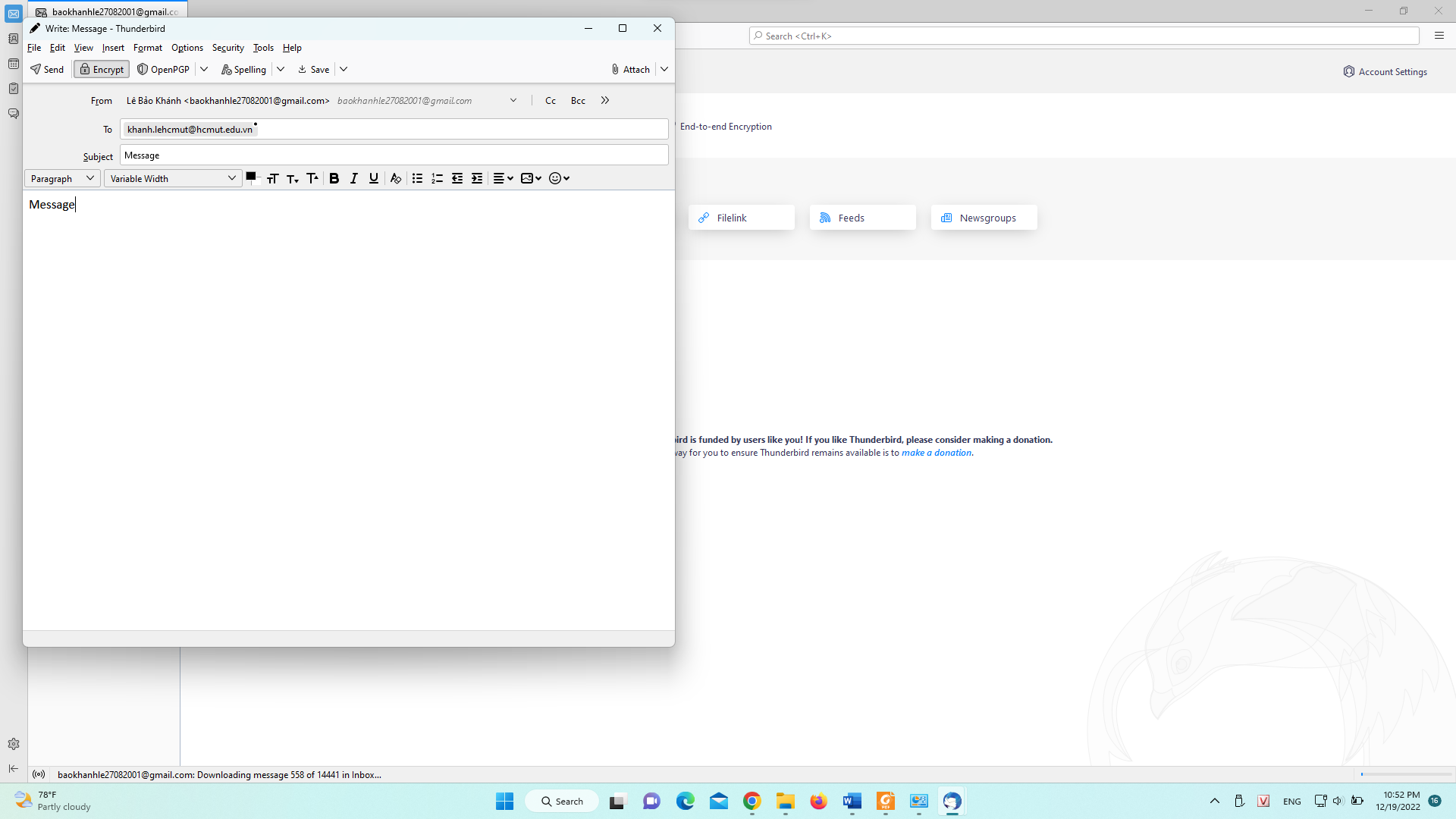
1. *Thêm khóa công khai của các người dùng khác*

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

****

1. *Tạo thư, mã hóa và gửi đi*

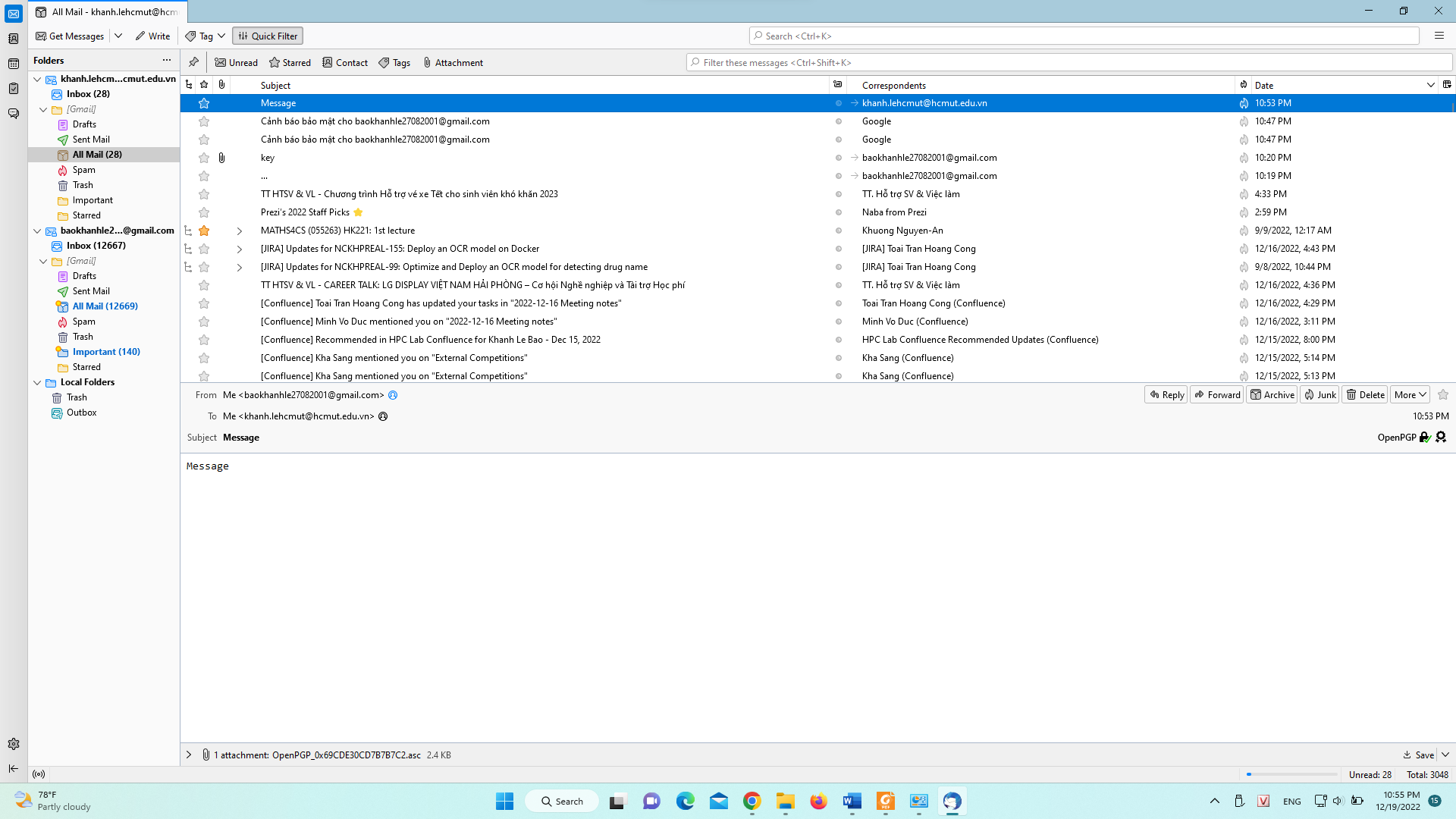
Các bước thực hiện là:



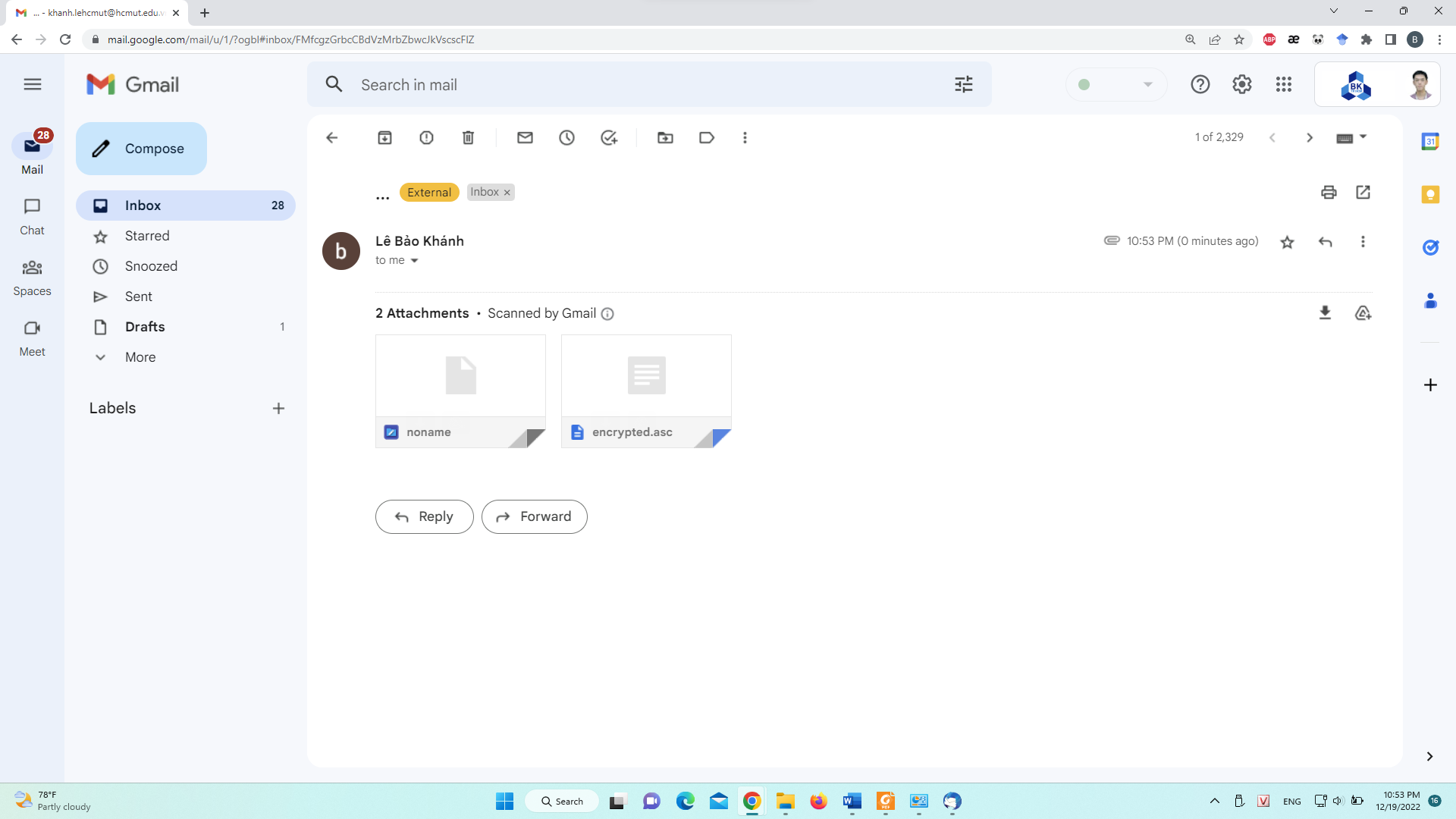
1. *Nhận thư. giải mã, đọc thư*

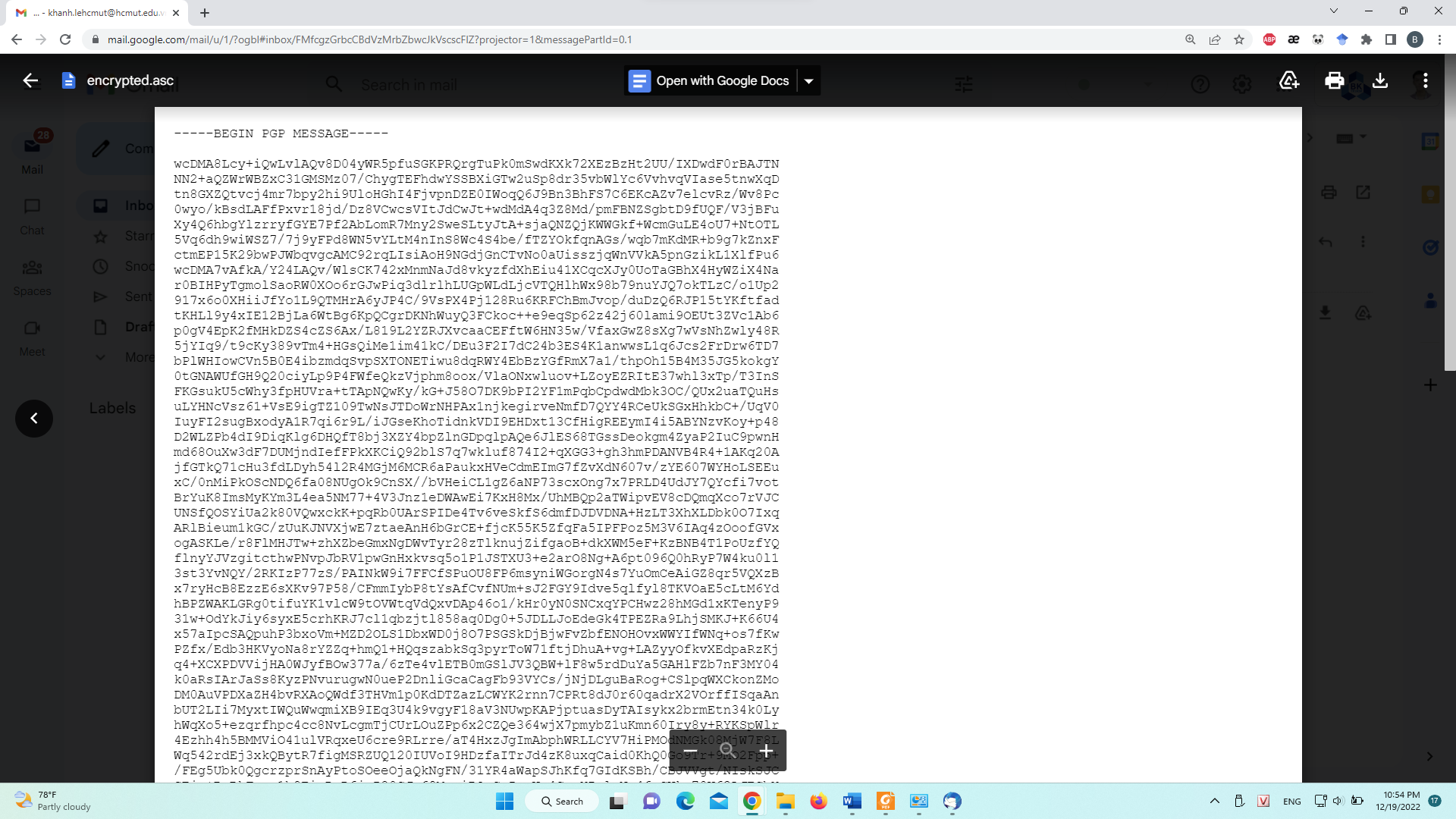
Các bước thực hiện là:

Mở bằng app Thunderbird

****

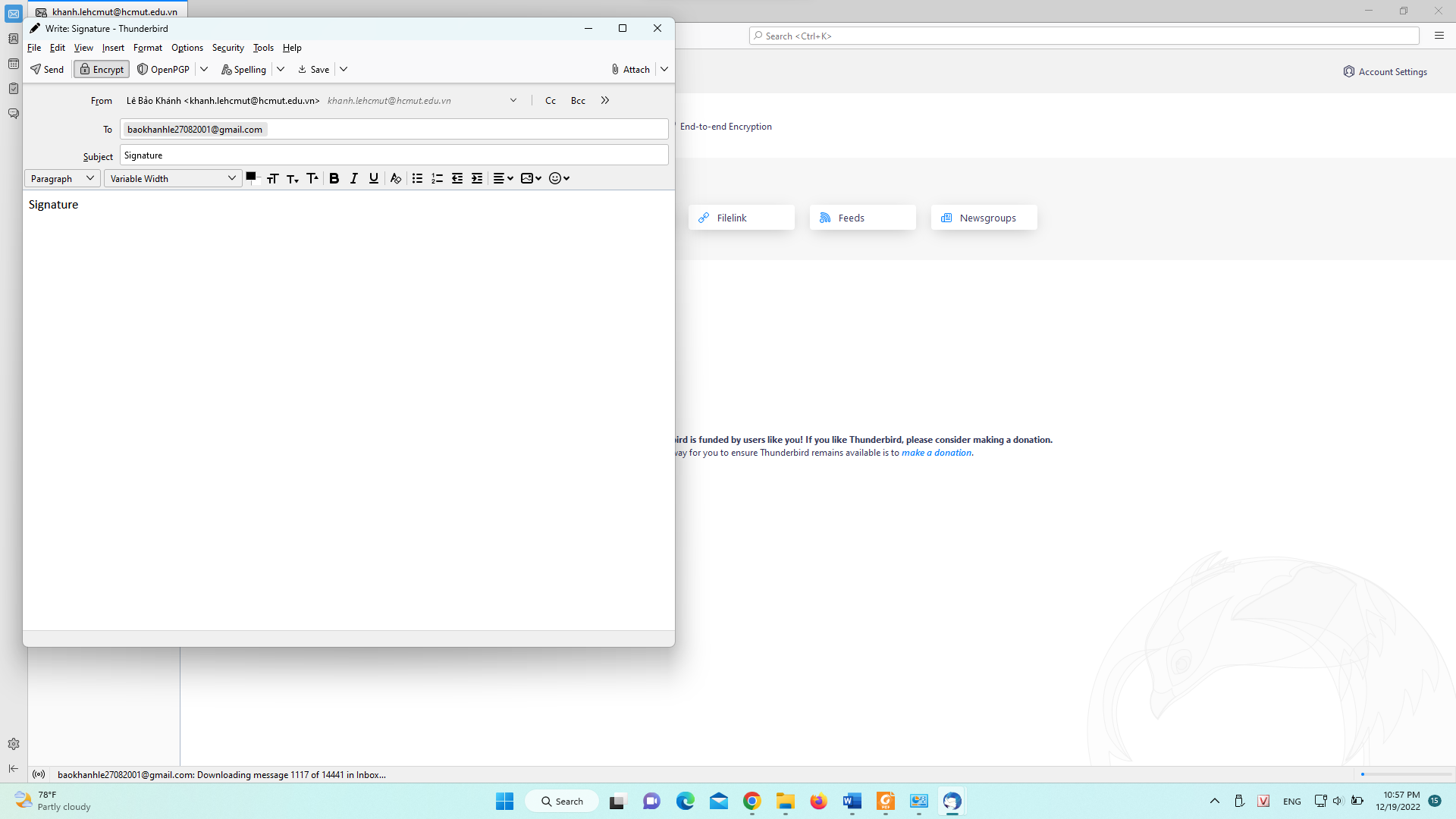
**Mở trình duyệt và đọc thư nói trên, cho biết nội dung thể hiện:**

****

****

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

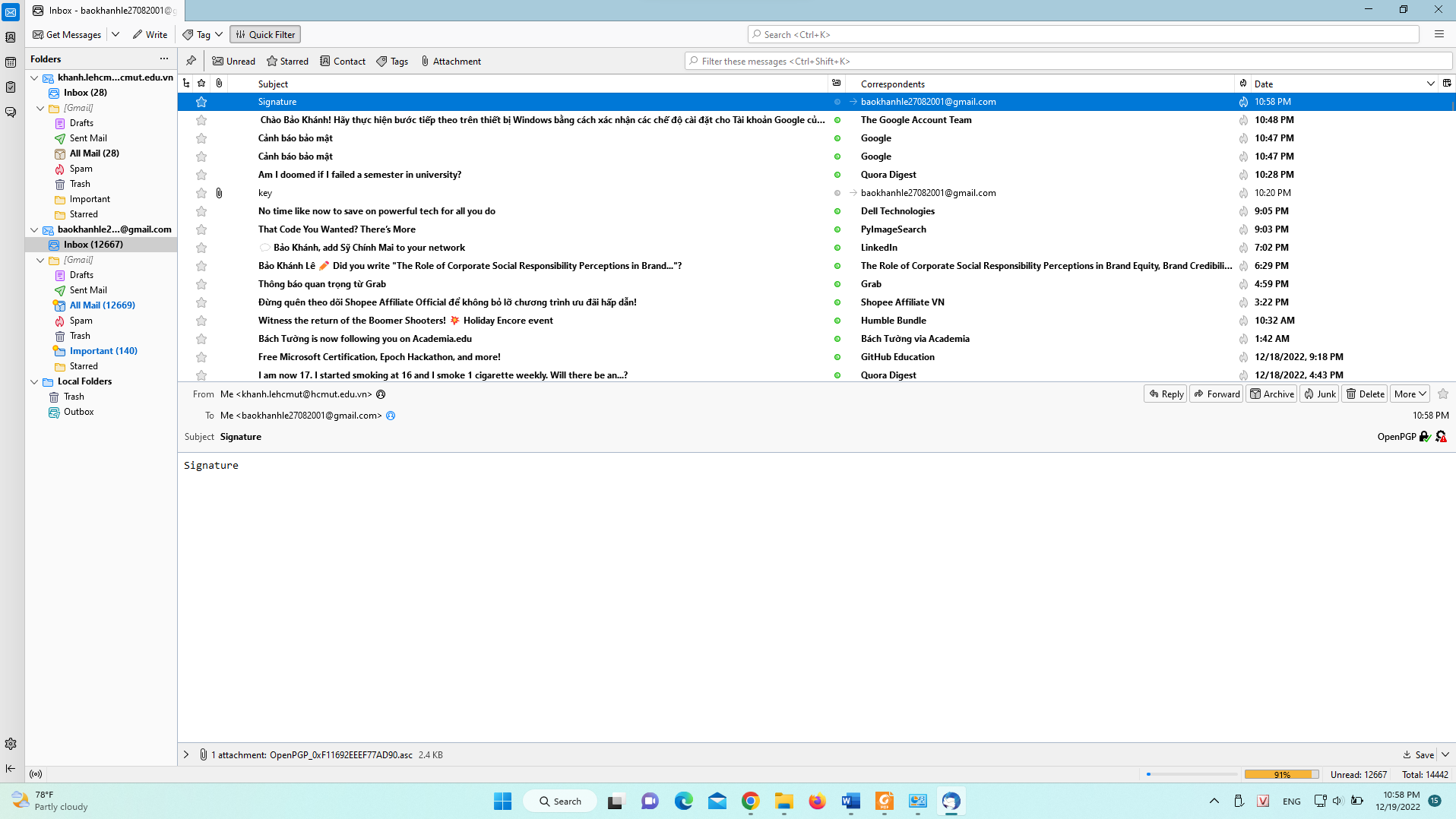
Các bước thực hiện là:

******

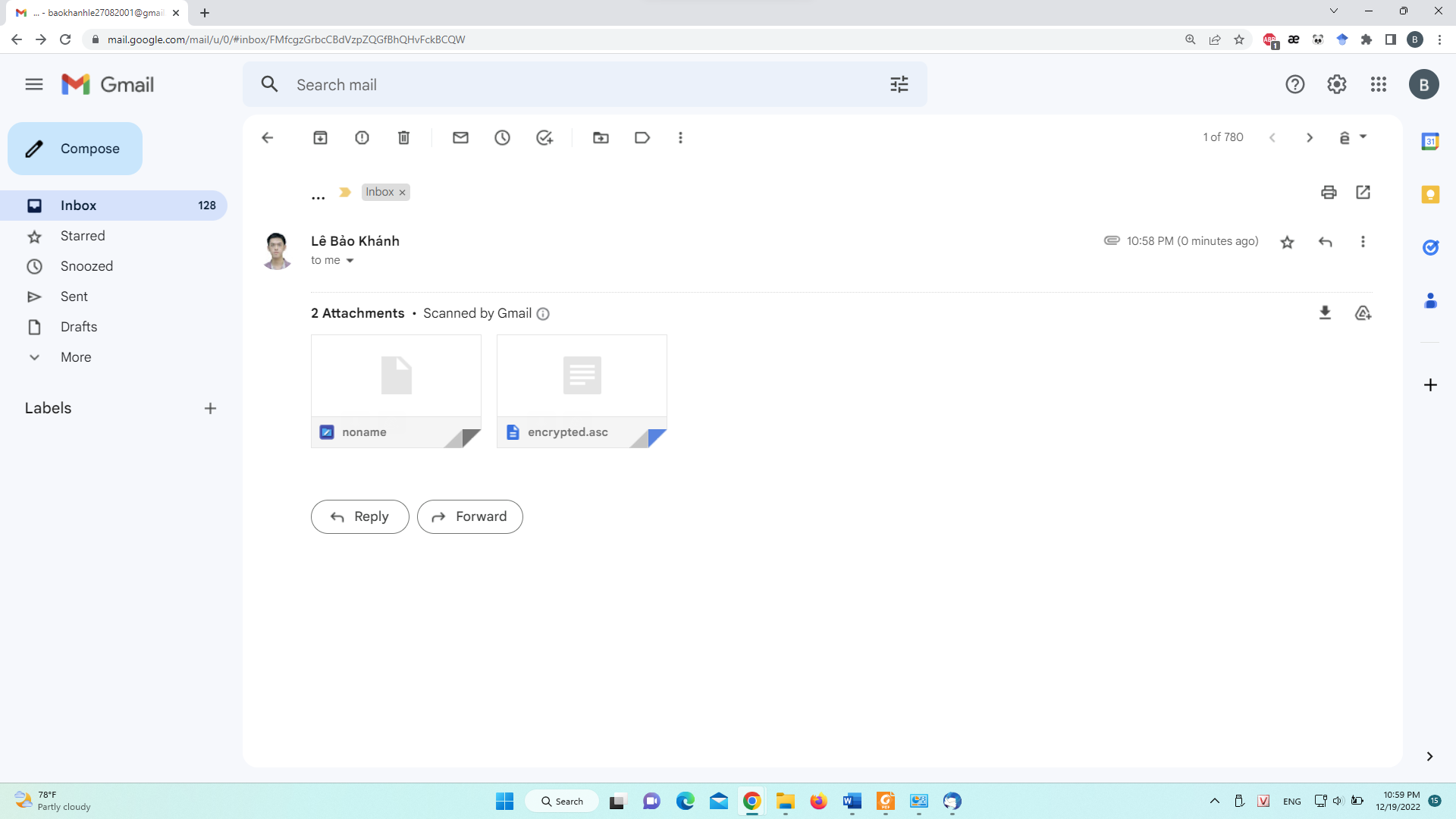
1. *Nhận thư. giải mã, xác minh chữ ký số, đọc thư*

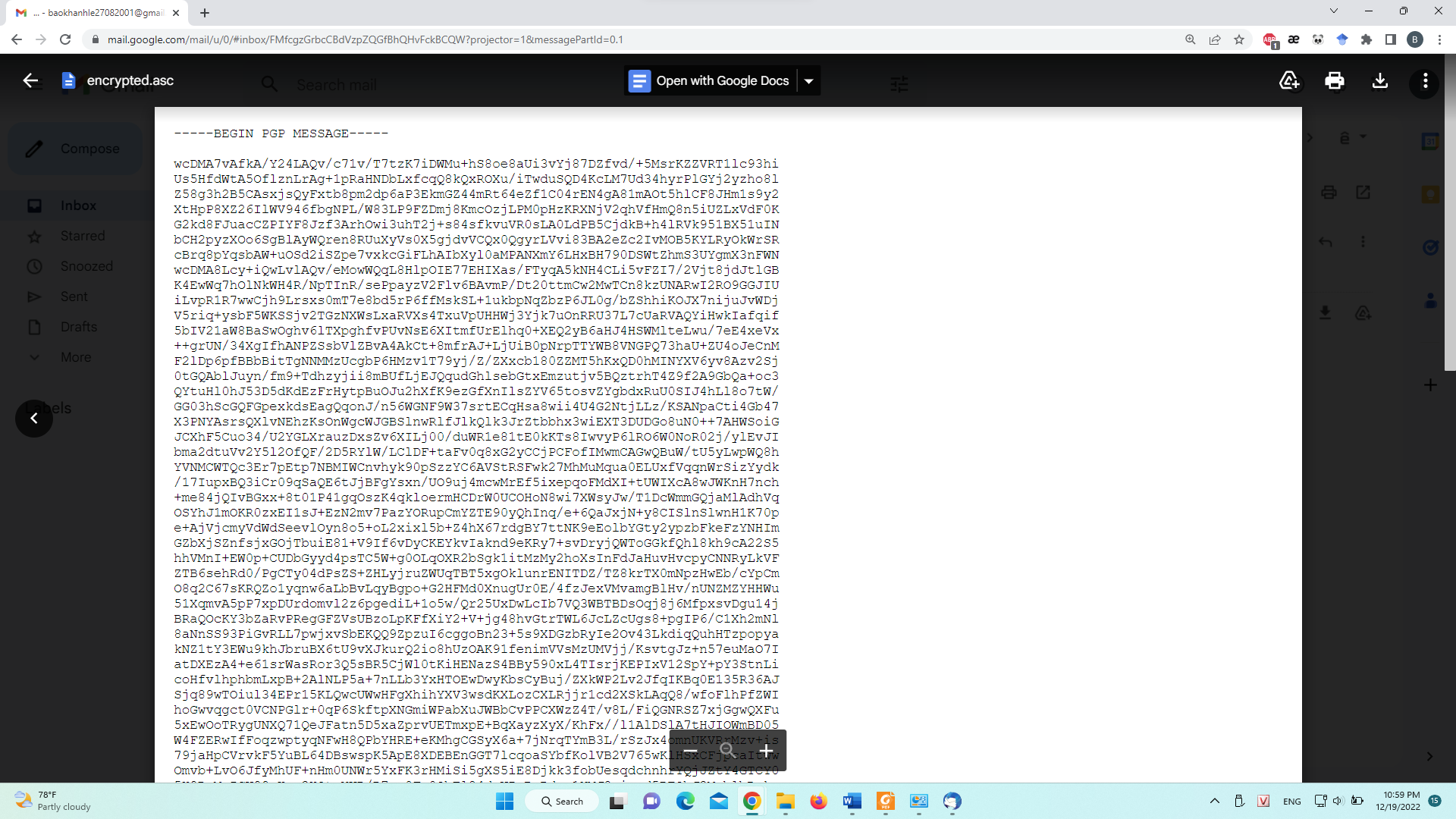
Các bước thực hiện là:

**Mở bằng app Thunderbird:**

****

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

****

****

* + - * 1. **An ninh hệ thống Web**

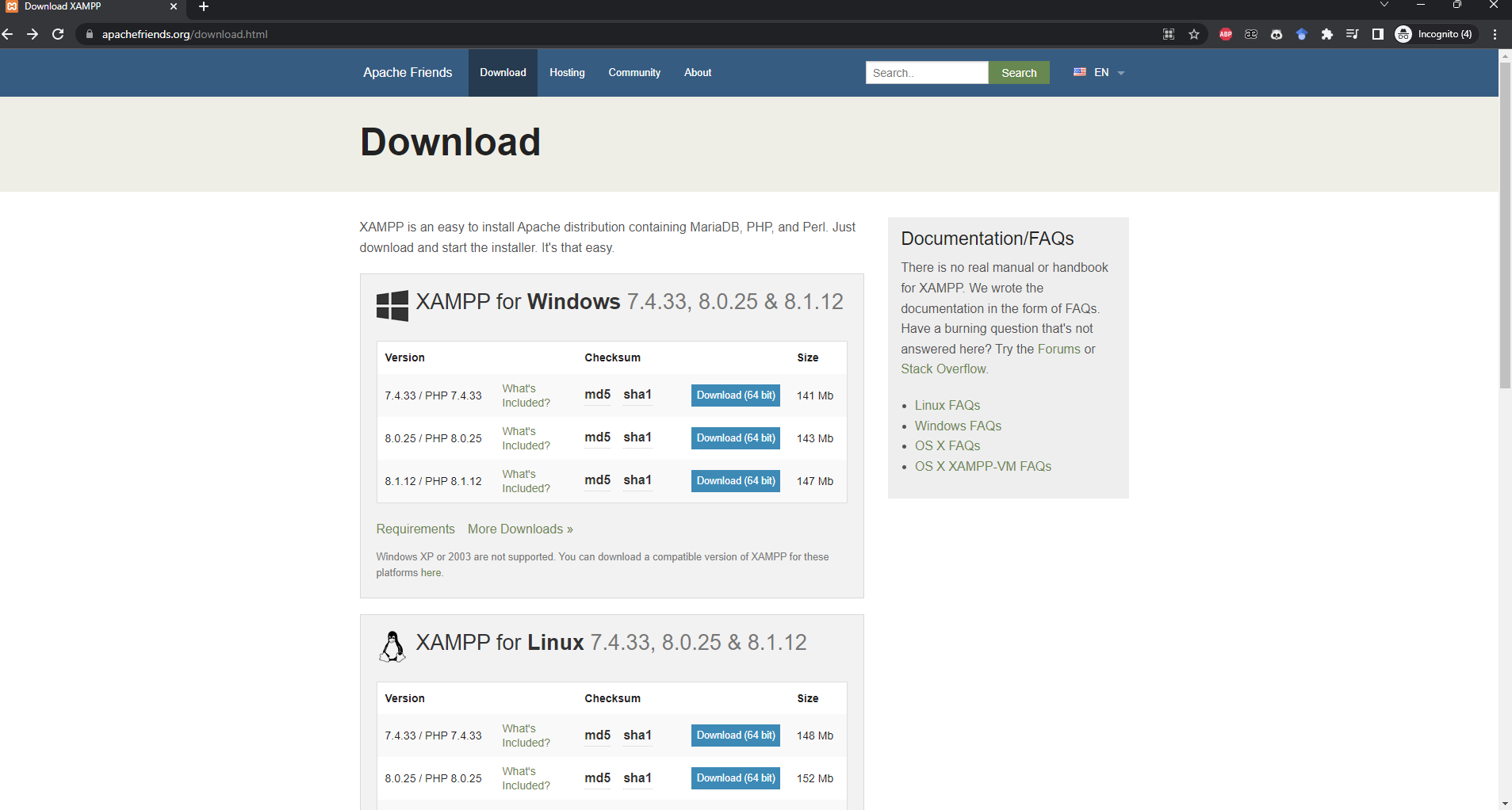
1. *Cài đặt và cấu hình Apache Web Server*

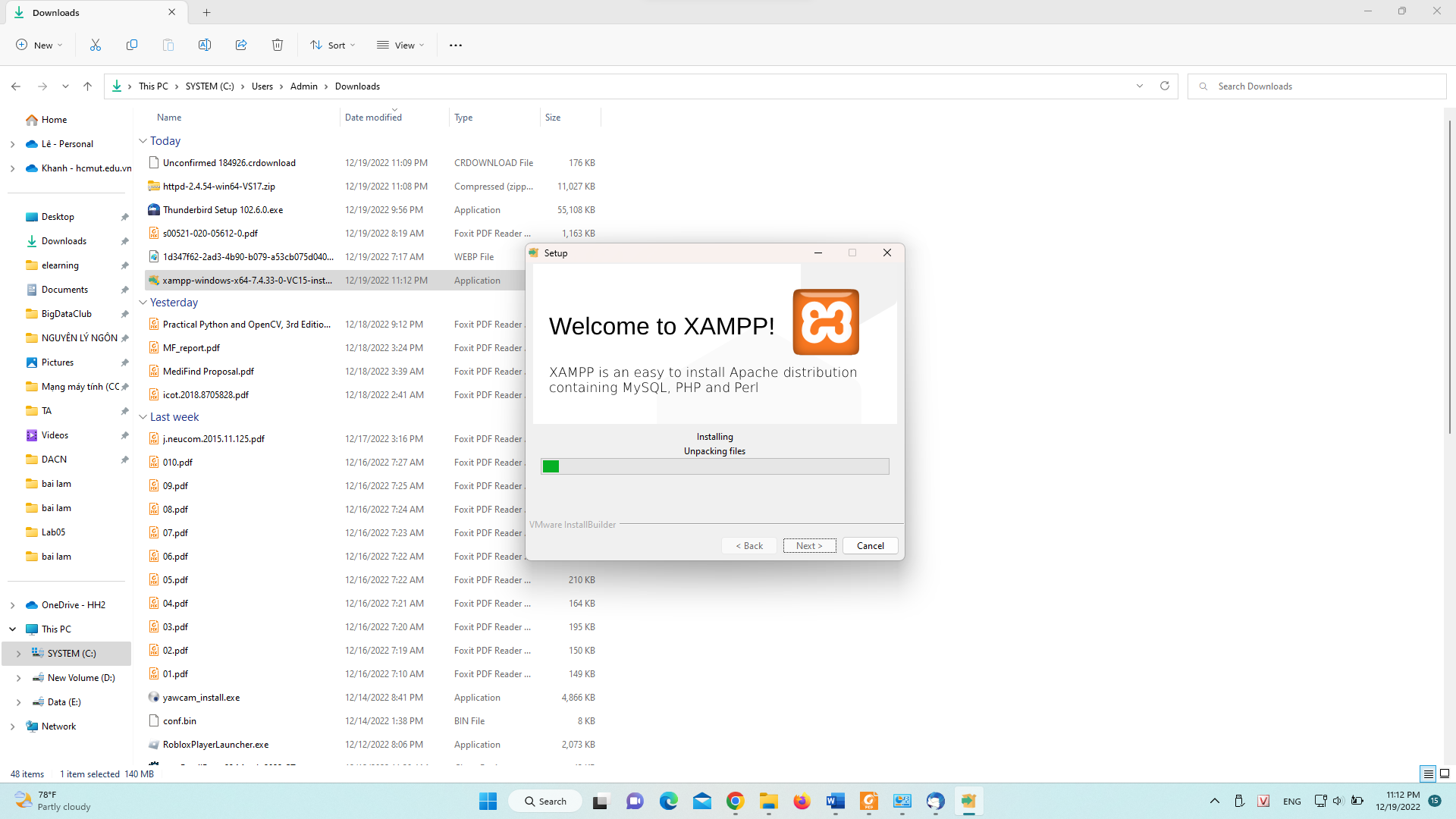
**Apache** là phần mềm web server miễn phí mã nguồn mở. Tên chính thức của Apache là Apache HTTP Server được điều hành và phát triển bởi Apache Software Foundation.

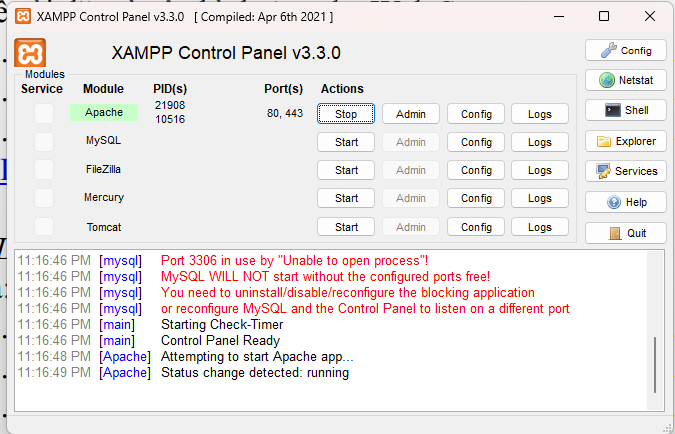
Download Apache Web Server từ <https://httpd.apache.org/download.cgi>

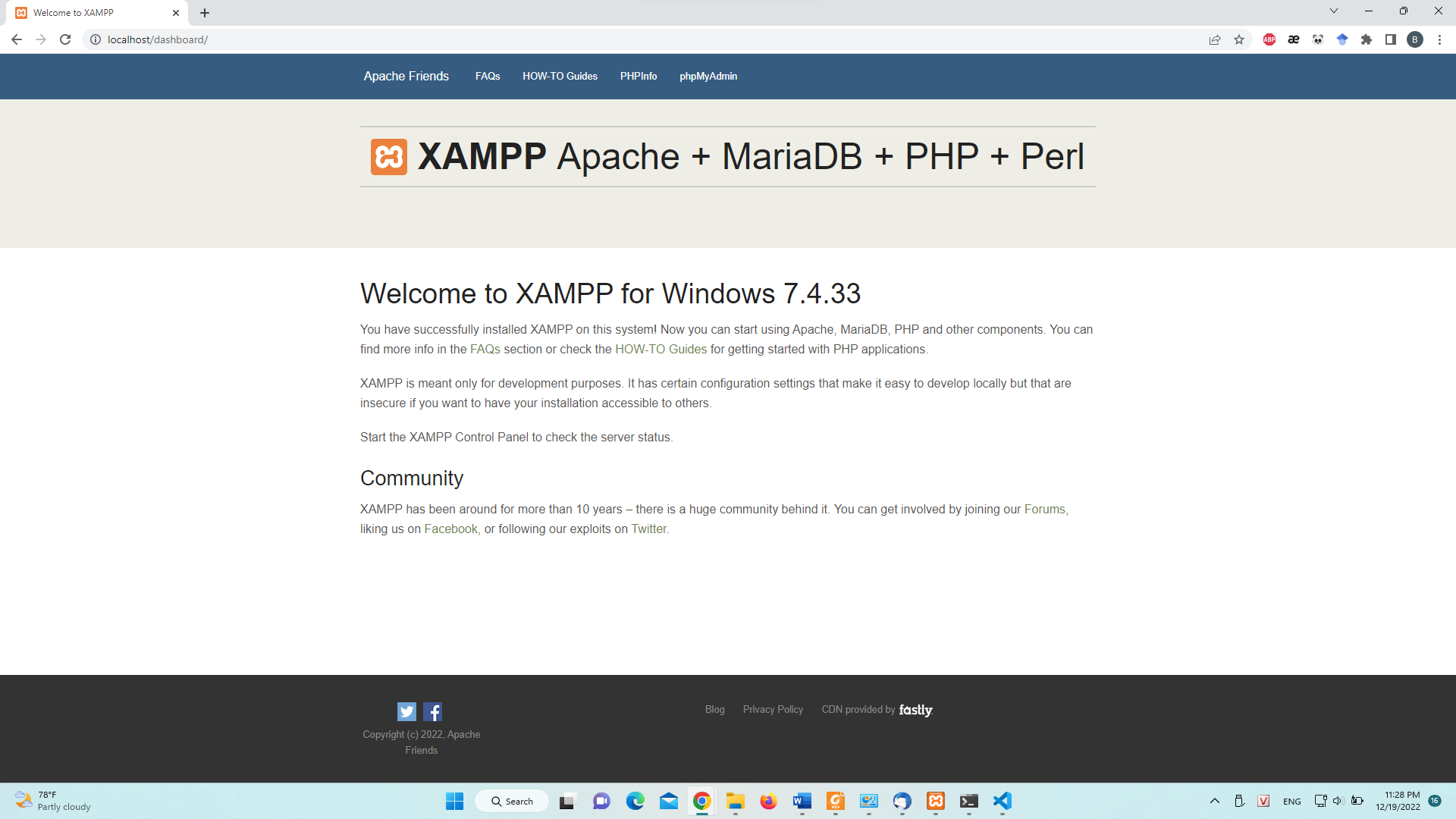
Các bước ngắn gọn để cài đặt và cấu hình Apache Web Server**:**

Download Xampp (tích hợp Apache Web Server):







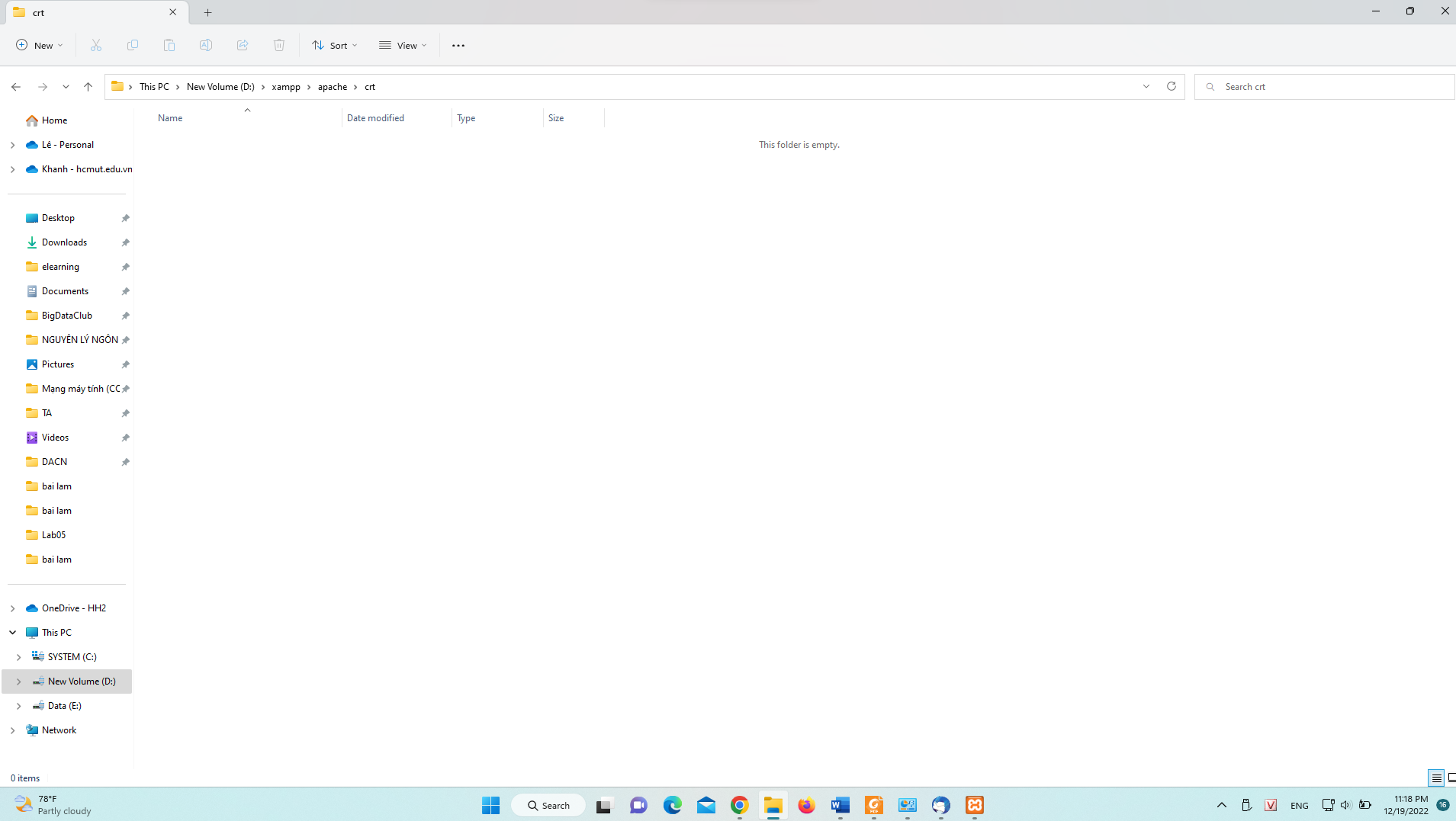


**Lưu ý:**  [Cần disable IIS đối với các hệ điều hành MS Windows](https://windowsjet.com/disabling-iis-internet-information-services-in-windows-10-879/).

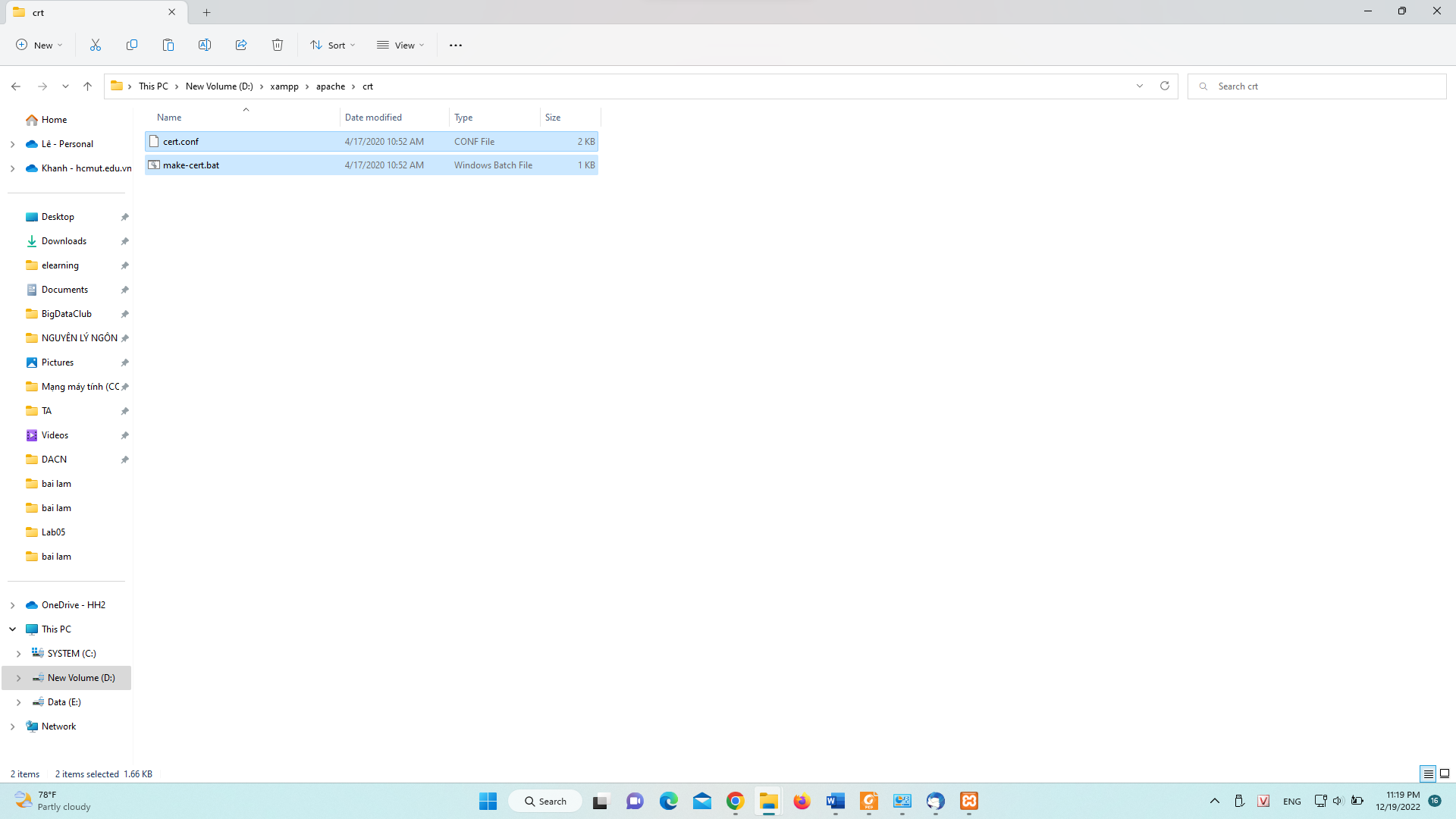
1. *Tạo chứng chỉ SSL tự ký bằng OpenSSL*

Các bước thực hiện là:

**+** Tạo thư mục crt trong đường dẫn D:\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.**

****

**+ Config lại file cert.conf**

[ req ]

default\_bits        = 2048

default\_keyfile     = server-key.pem

distinguished\_name  = subject

req\_extensions      = req\_ext

x509\_extensions     = x509\_ext

string\_mask         = utf8only

[ subject ]

countryName                 = Country Name (2 letter code)

countryName\_default         = VN

stateOrProvinceName         = State or Province Name (full name)

stateOrProvinceName\_default = Ho Chi Minh

localityName                = Locality Name (eg, city)

localityName\_default        = Ho Chi Minh

organizationName            = Organization Name (eg, company)

organizationName\_default    = Hosting

commonName                  = Common Name (e.g. server FQDN or YOUR name)

commonName\_default          = mylocalhost.com

emailAddress                = Email Address

emailAddress\_default        = hotro@nmylocalhost.vn

[ x509\_ext ]

subjectKeyIdentifier   = hash

authorityKeyIdentifier = keyid,issuer

basicConstraints       = CA:FALSE

keyUsage               = digitalSignature, keyEncipherment

subjectAltName         = @alternate\_names

nsComment              = "OpenSSL Generated Certificate"

[ req\_ext ]

subjectKeyIdentifier = hash

basicConstraints     = CA:FALSE

keyUsage             = digitalSignature, keyEncipherment

subjectAltName       = @alternate\_names

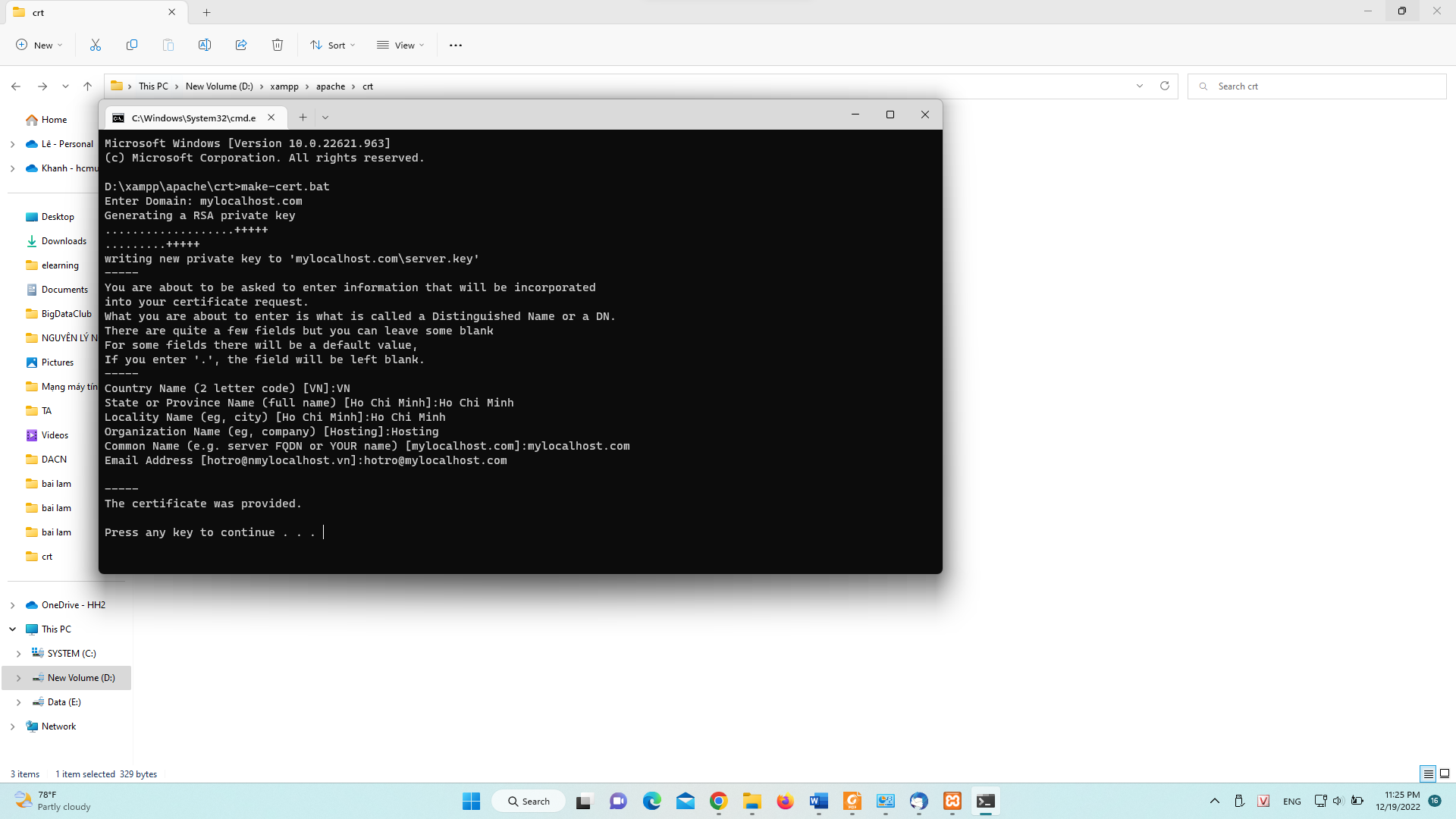
nsComment            = "OpenSSL Generated Certificate"

[ alternate\_names ]

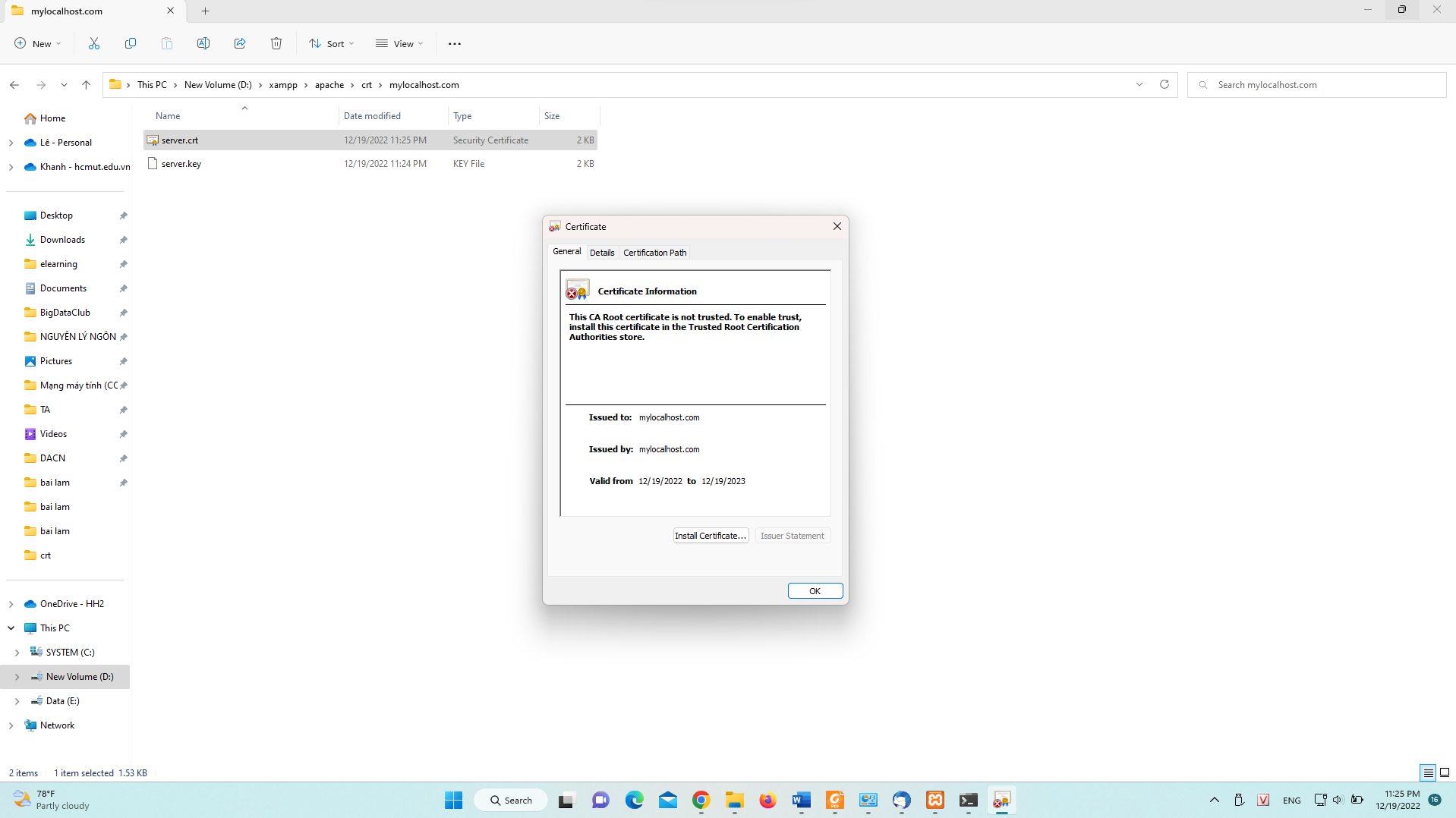
DNS.1       = mylocalhost.com

**+ 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**

Các bước thực hiện là:

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

**127.0.0.1 mylocalhost.com**

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

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

# mylocalhost.com

<VirtualHost: \*:80>

    DocumentRoot "D:/xampp/htdocs"

    ServerName mylocalhost.com

    ServerAlias \*.mylocalhost.com

</VirtualHost>

<VirtualHost: \*:443>

    DocumentRoot "D:/xampp/htdocs"

    ServerName mylocalhost.com

    ServerAlias \*.mylocalhost.com

    SSLEngine on

    SSLCertificateFile "crt/mylocalhost.com/server.crt"

    SSLCertificateKeyFile "crt/mylocalhost.com/server.key"

</VirtualHost>

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

**Tìm hiểu:**

* **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.**
* **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.**
* **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.**

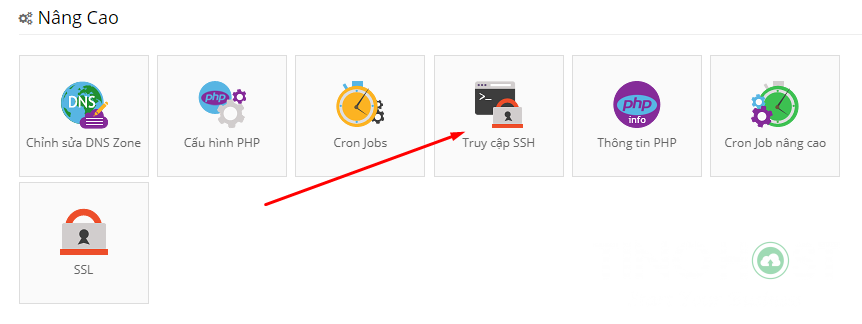
1. **Cho biết cách tạo và duy trì chứng chỉ SSL miễn phí từ Let’s Encrypt**

Let’s Encrypt là một lựa chọn hợp lý, miễn phí, hỗ trợ bảo mật domain của bạn khi bạn muốn test website. TinoHost sẽ hướng dẫn bạn cách để tạo chứng chỉ SSL/STL miễn phí trên cPanel.

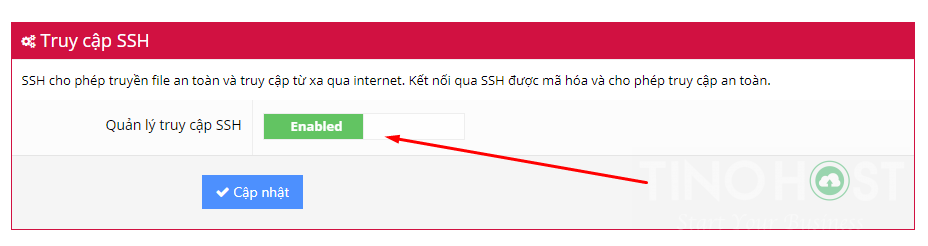
Một lưu ý nhỏ: Tùy vào mỗi nhà cung cấp hosting, bạn sẽ có một bản điều khiển riêng như cPanel hay DirectAdmin,… mỗi phiên bản cPanel sẽ khác nhau nên bạn chỉ cần tìm những thông tin và thao tác tương tự là ổn.

### ****Truy cập SSH****

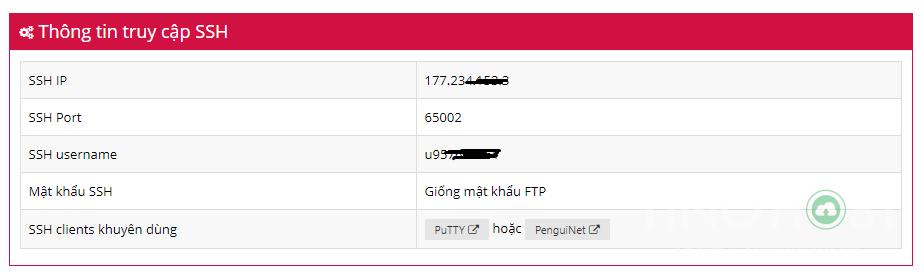
Vào **Control Panel** của tài khoản hosting, bạn chọn **Truy cập SSH.**



Tại đây bạn chọn **Enabled**, kế tiếp chọn **Cập nhật** để kích hoạt truy cập SSH



Những thông tin truy cập SSH như **IP, port, username, password,**bạn nên nhớ kĩ để sử dụng.



### ****Cài đặt ACME client và Composer****

Tiến hành kết nối SSH vào tài khoản của bạn: bạn sử dụng [PuTTY](https://www.putty.org/)điền các thông tin truy cập SSH bạn vừa có được và lần lượt chạy các lệnh sau trong cửa sổ command của PuTTY.

**git clone https://github.com/kelunik/acme-client**

**cd acme-client**

**php -r “copy(‘https://getcomposer.org/installer’, ‘composer-setup.php’);”;**

**php composer-setup.php;**

**php -r “unlink(‘composer-setup.php’);”;**

**php composer.phar install –no-dev**

**php bin/acme setup –server letsencrypt –email your@email.com**

**php bin/acme issue –domains yourdomain.com,www.yourdomain.com –path /home/username/public\_html –server letsencrypt**

Để phù hợp với tài khoản của mình, bạn cần thay đổi **your@email.com, yourdomain.com, username.**

Sau đó, bạn sử dụng trình File Manager di chuyển tới

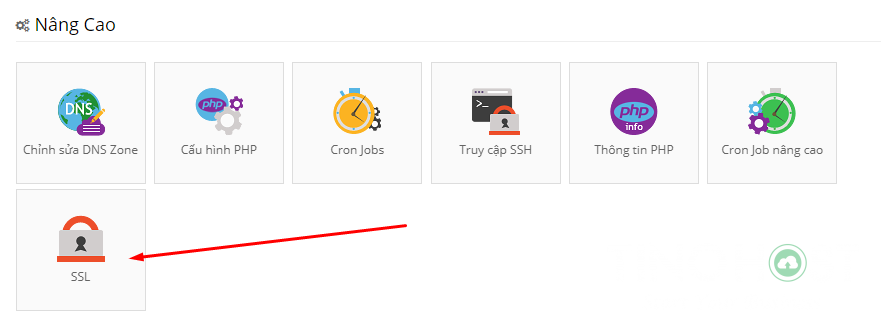
**/home/username/acme-client/data/certs/acme-v01.api.letsencrypt.org.directory/yourdomain.com**

Bước này sẽ tạo ra 2 file quan trọng trong tài khoản hosting.

* **fullchain.pem:** chứa thông tin certificate của bạn
* **key.pem:** chứa thông tin private key của bạn

### ****Cài đặt SSL từ Control Panel****

Sau khi đã có 2 files là **fullchain.pem** và **key.pem**, chúng ta sẽ vào mục **SSL** ở **Control Panel**



Bạn thực hiện các bước như sau:

Chọn domain cần cài đặt

Sao chép nội dung file **fullchain.pem** và dán vào Certificate: (CRT)

Sao chép nội dung file **file key.pem**và dán vào Private Key: (KEY)

Cuối cùng, bạn chọn **Cài đặt** để thực hiện. Giờ bạn chỉ cần đợi một chút để quá trình cài đặt hoàn tất, bạn nhấn **F5**để làm mới trình duyệt lại và xem trang web của bạn đã được lên HTTPS chưa.

Nếu có là bạn đã thành công rồi đấy! Tiếp theo, để SSL tự động gia hạn, chúng ta sẽ cài đặt Cronjob.

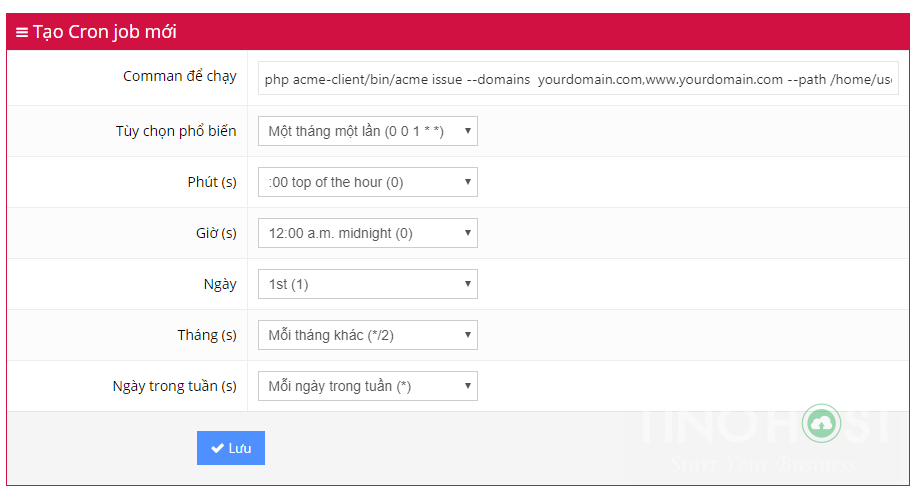
### ****Cài đặt Cronjob****

Do Let’s Encrypt chỉ cung cấp xác nhận bảo mật cho tên miền của bạn trong thời hạn **90 ngày** kể từ ngày tạo nên bạn cần thực hiện chạy [cronjob](https://wiki.tino.org/cron-jobs-la-gi/)để gia hạn SSL này một cách tự động và đỡ tốn thời gian hơn.

Vào **Control Panel**, chọn “**Cron Job nâng cao**”

Bạn nhập vào **Comman để chạy** bằng code sau:

**php acme-client/bin/acme issue –domains yourdomain.com,www.yourdomain.com –path /home/username/public\_html –server letsencrypt**



Sau khi hoàn tất, bạn nhấn **Lưu**để lưu lại quá trình