BÀI THỰC HÀNH SỐ ????

Môn: MẬT MÃ & AN NINH MẠNG

-o0o-

**Họ tên: Lương Hữu Phú Lợi**

**MSSV: 1911545**

**Nhóm: L02**

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

1. *Cài đặt Mozillla Thunderbird*

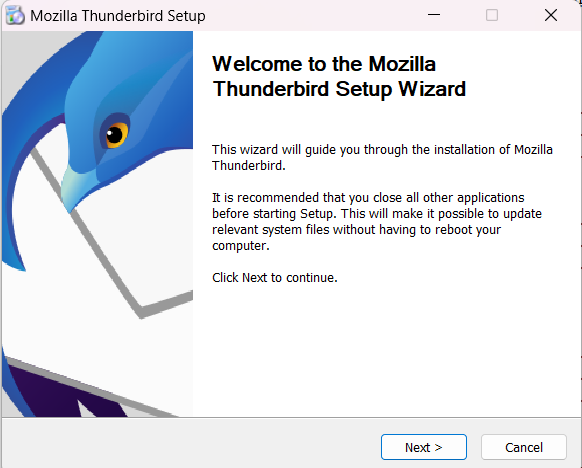
****Mozilla Thunderbird**** là chương trình miễn phí, nguồn mở hoạt động trên mọi nền tảng hệ điều hành giúp quản lý việc nhận, gửi và lưu trữ thư điện tử. Một phần mềm quản lý thư điện tử phía người dùng là một chương trình giúp bạn tải về và quản lý thư điện tử mà không cần sử dụng trình duyệt Internet.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

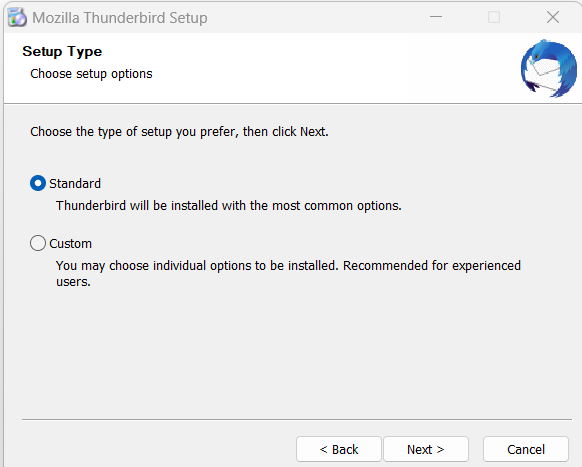
Các bước ngắn gọn để cài đặt Thunderbird**:**

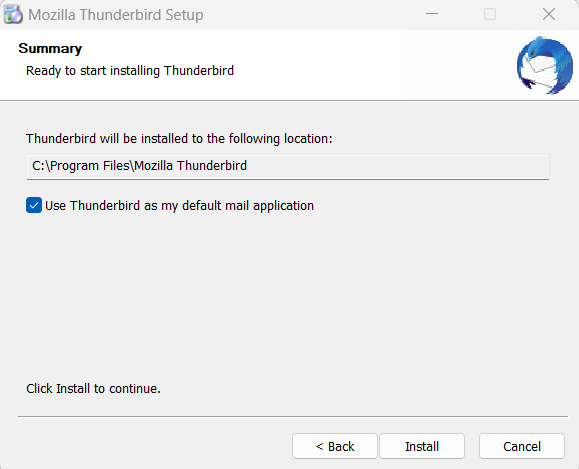
**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………**

**…………………………………………………………………………………………………**



**Chọn Standard**



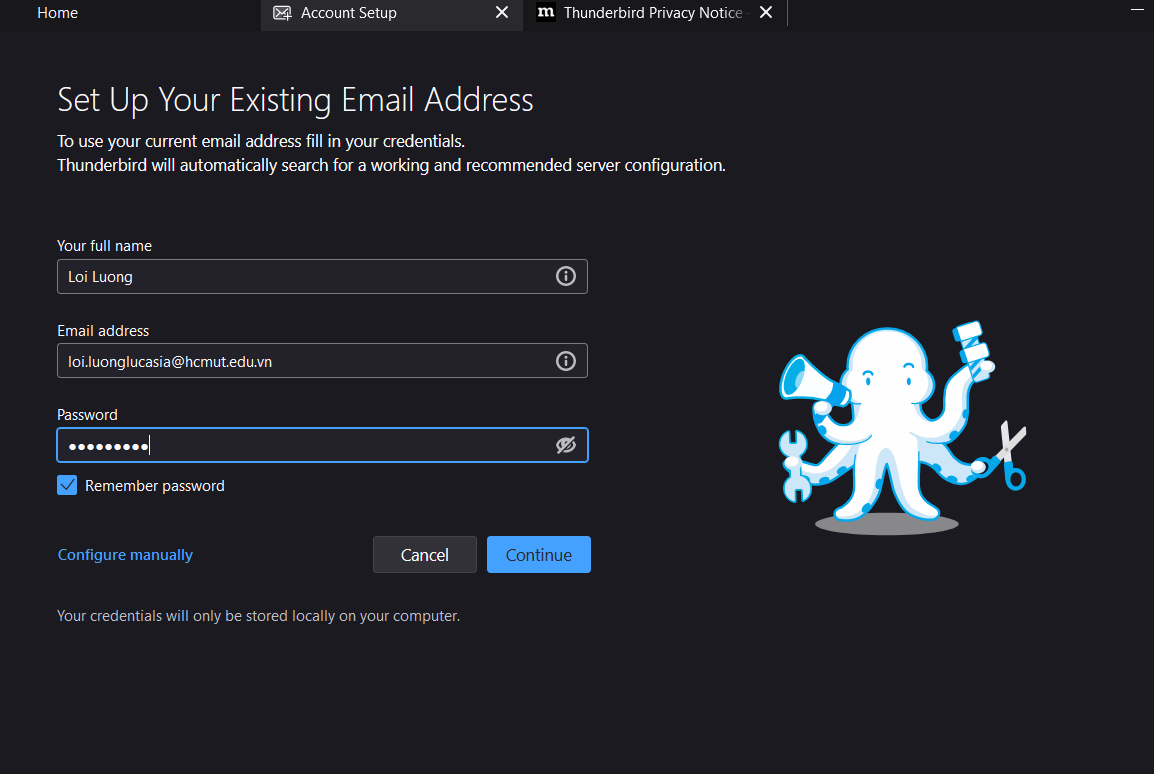
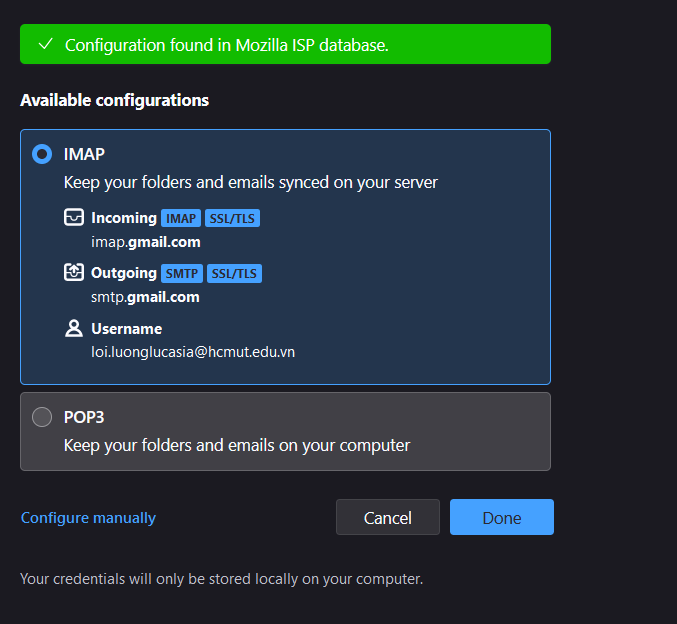


1. *Đăng ký một tài khoản thư điện tử vào Thunderbird*

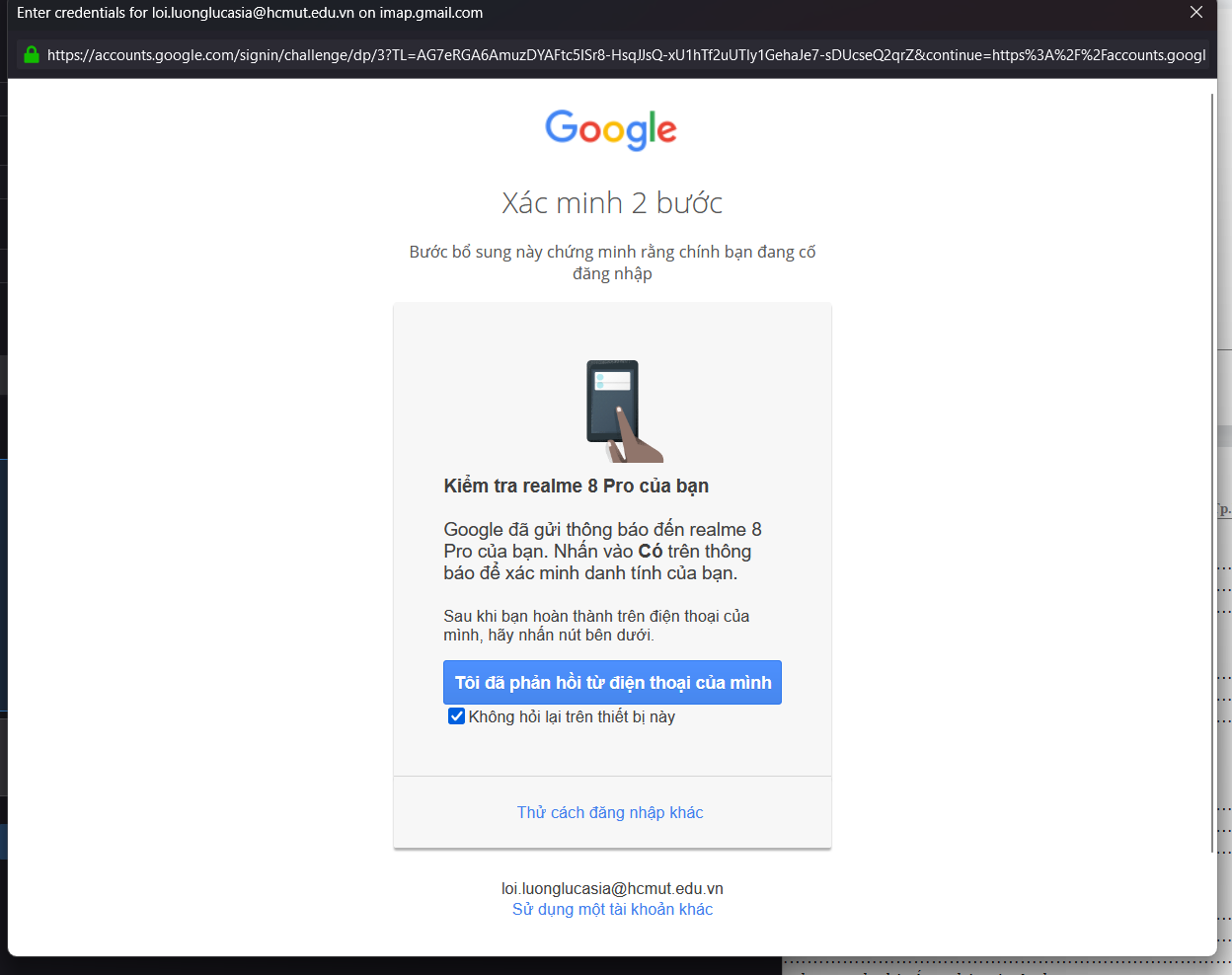
Các bước ngắn gọn để đăng ký một tài khoản thư điện tử của bạn vào thunderbird:

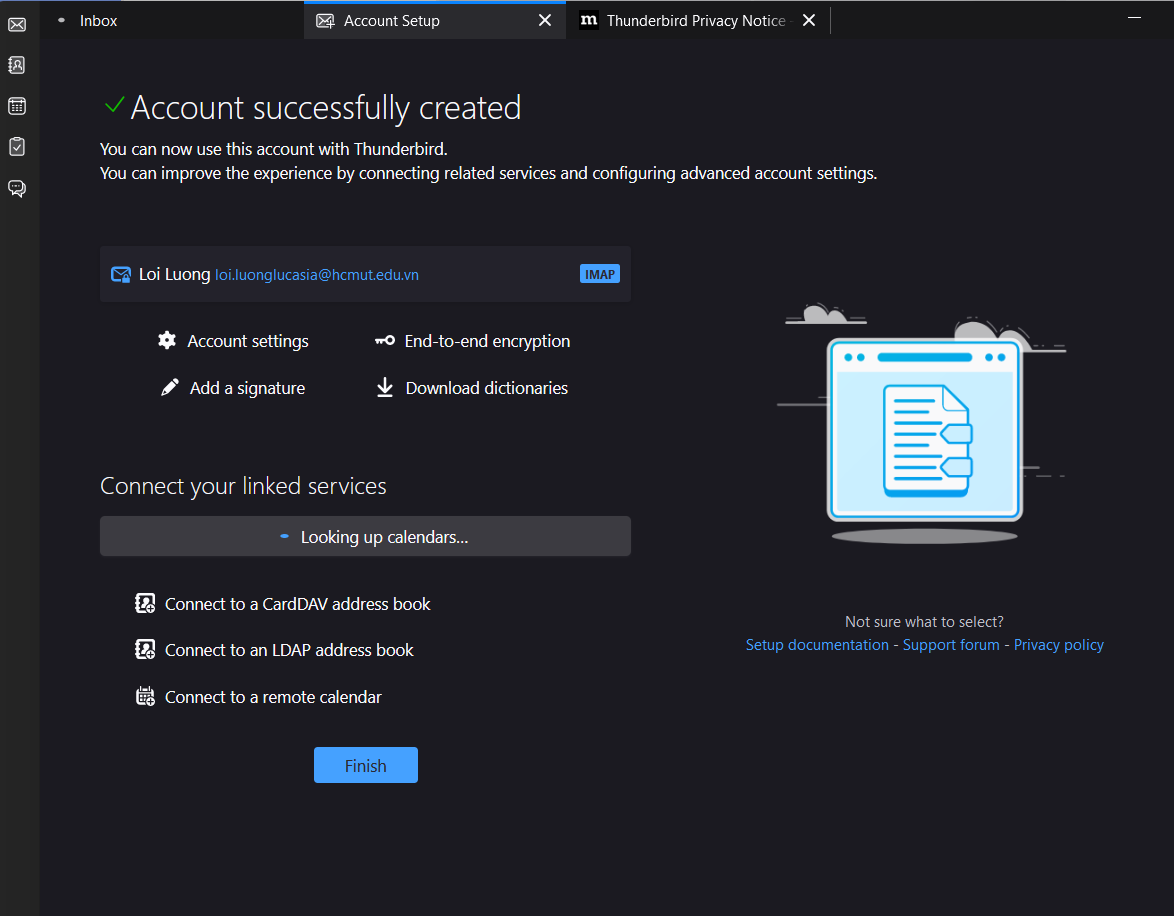
**……………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………**

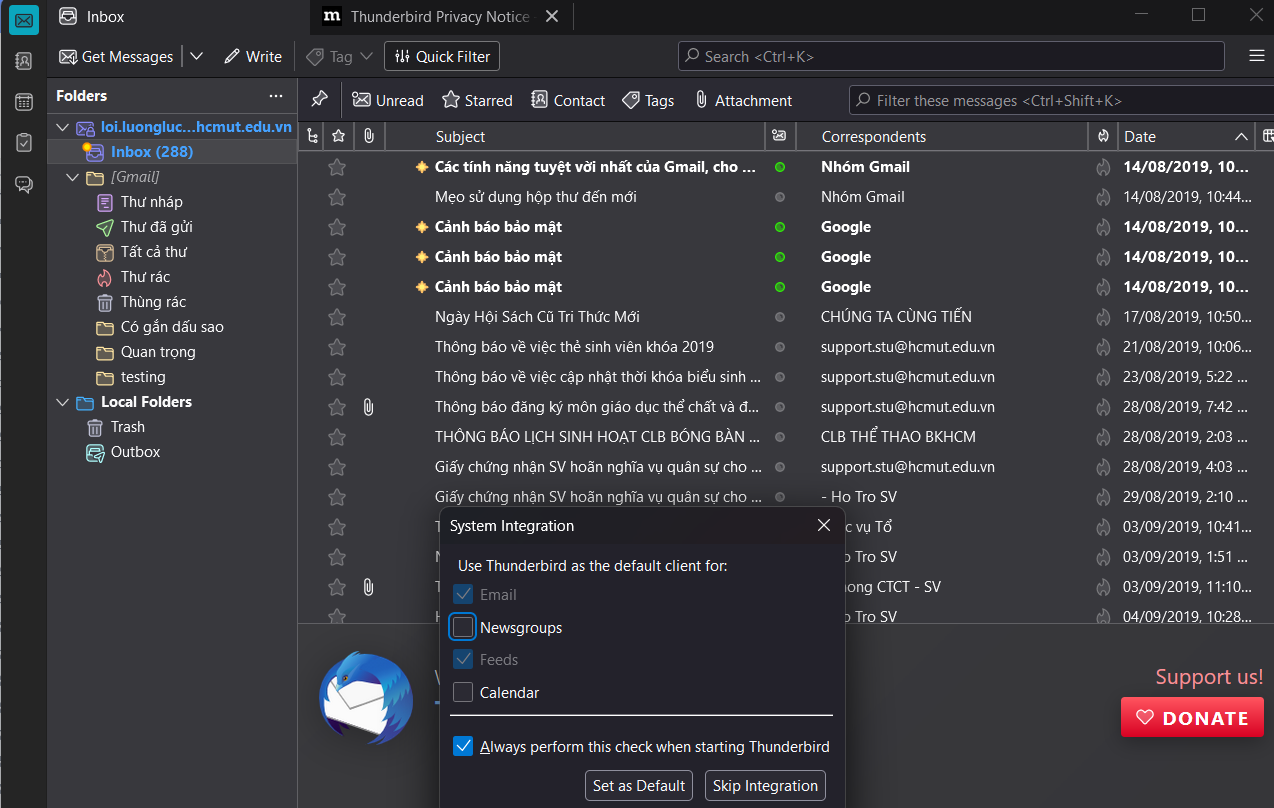
**…………………………………………………………………………………………………**

Chọn **Done** sau đó sẽ đăng nhập vào tài khoản gmail







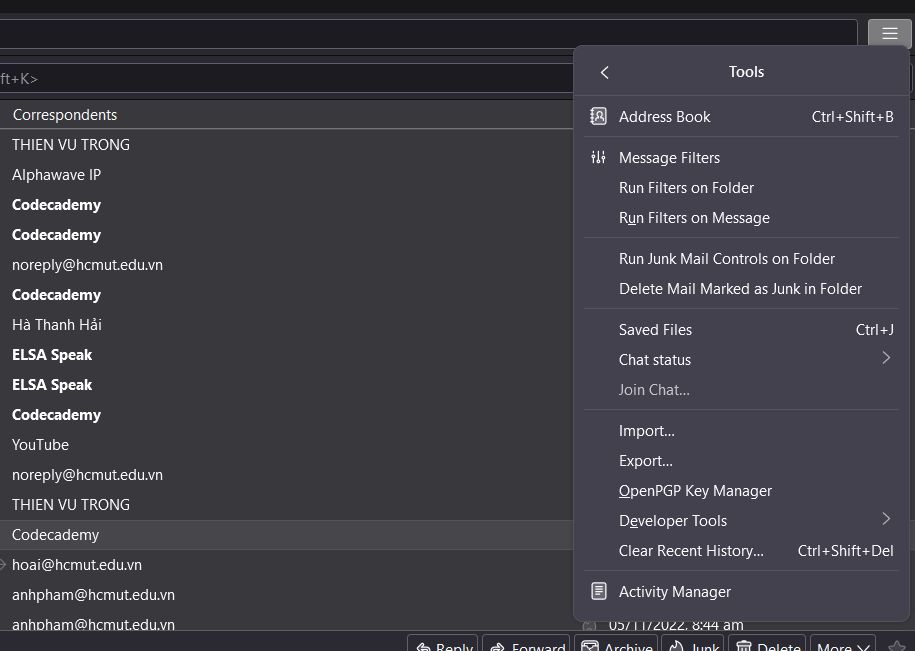
1. *Tạo cặp khóa từ OpenPGP Key Manager*

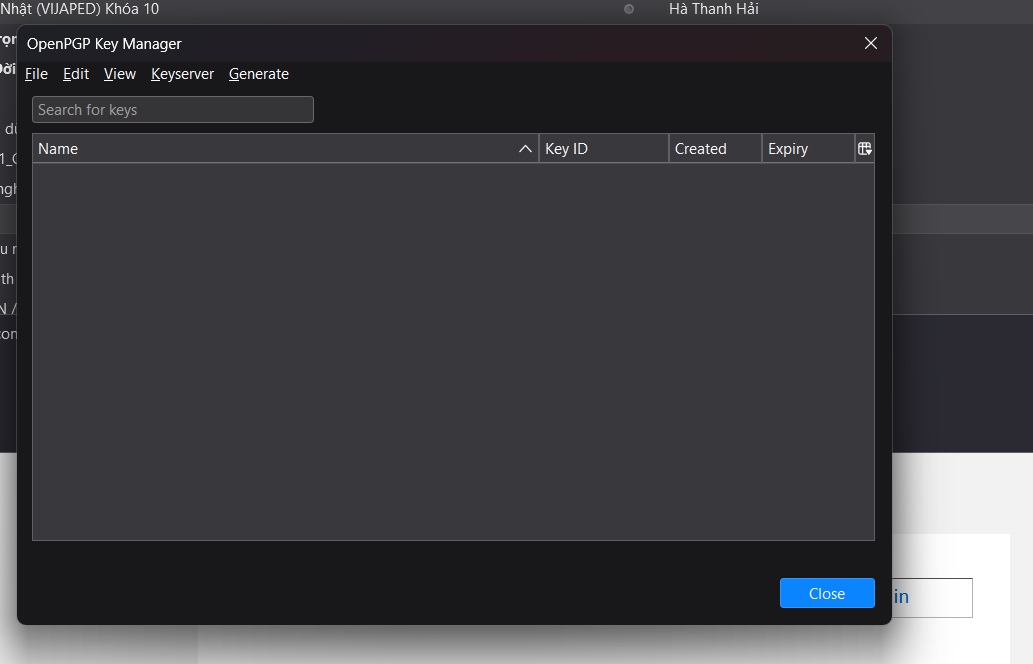
Từ **Tools-> OpenPGP Key Manager**, cửa sổ hiện ra là:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**



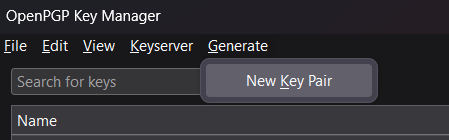


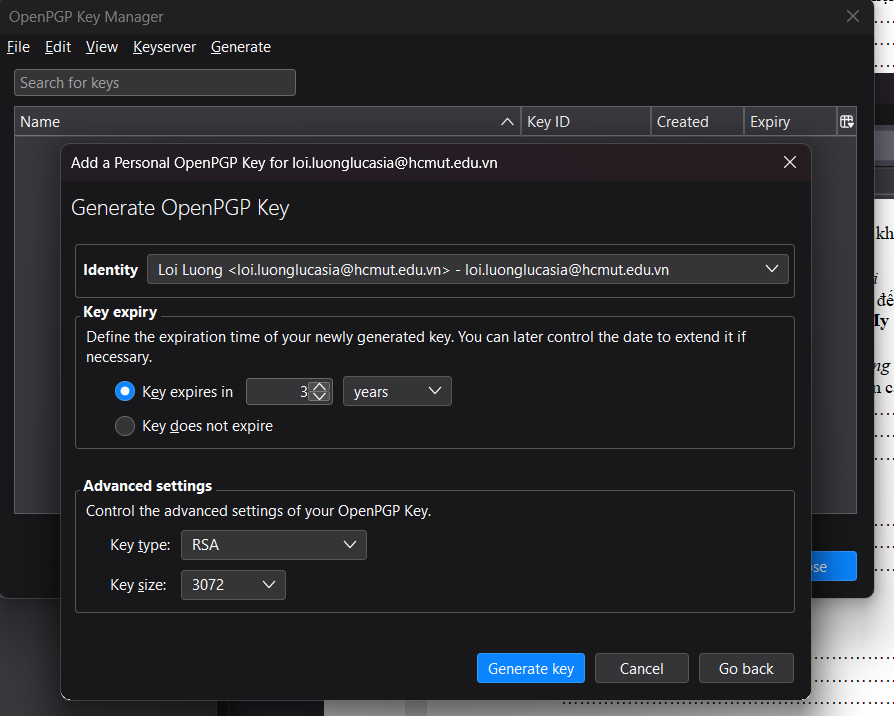
**Chọn **Generate -> New Key Pair,** cửa sổ hiện ra là:**

**…………………………………………………………………………………………………**

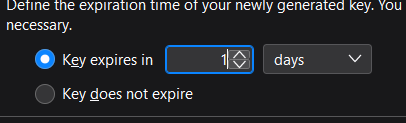
**…………………………………………………………………………………………………**

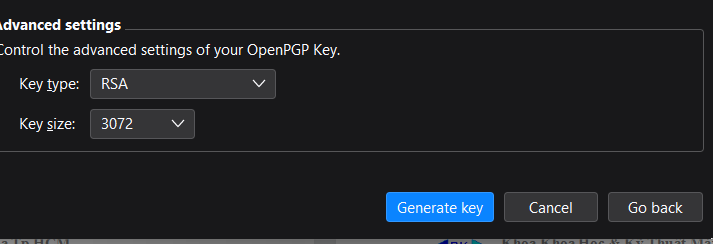
**…………………………………………………………………………………………………**



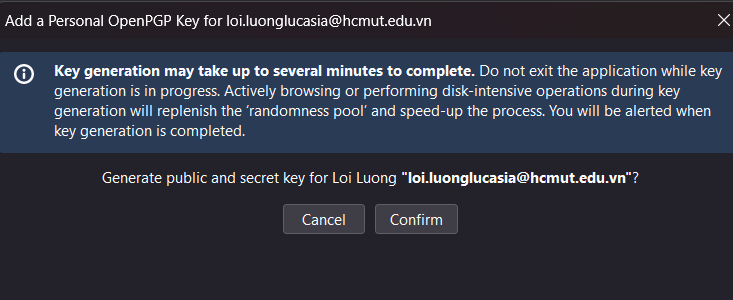


Thực hiện các bước tiếp theo để tạo cho tài khoản của mình một cặp khóa.

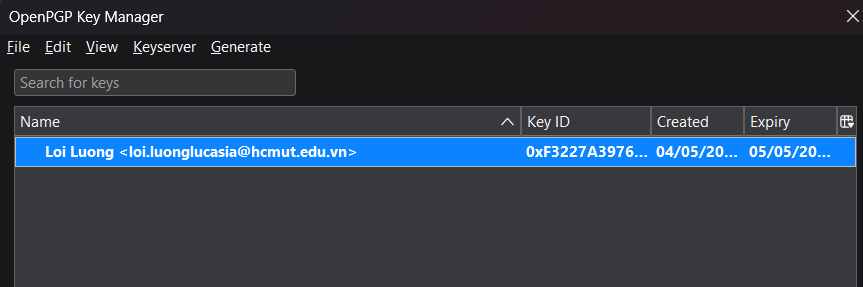




Chọn **Generate**

A

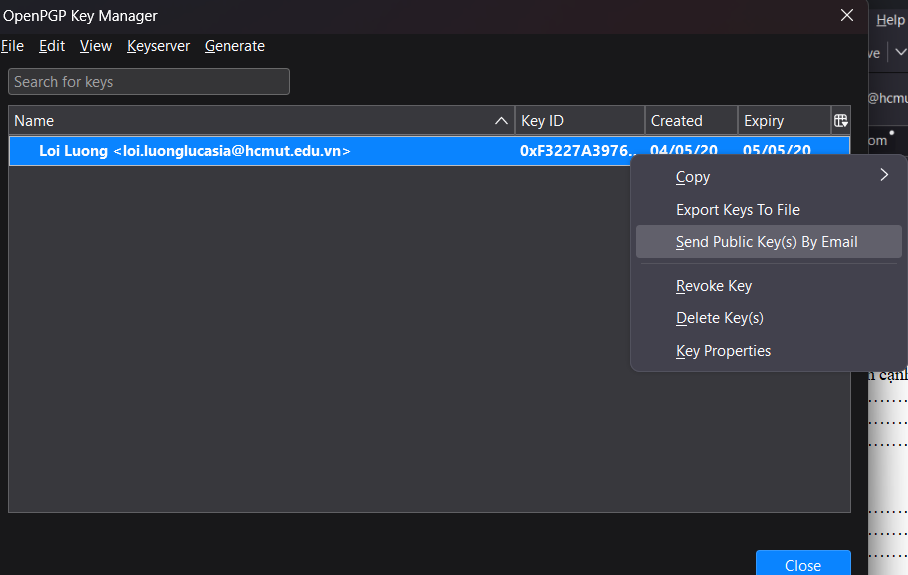
Chọn **Confirm**a



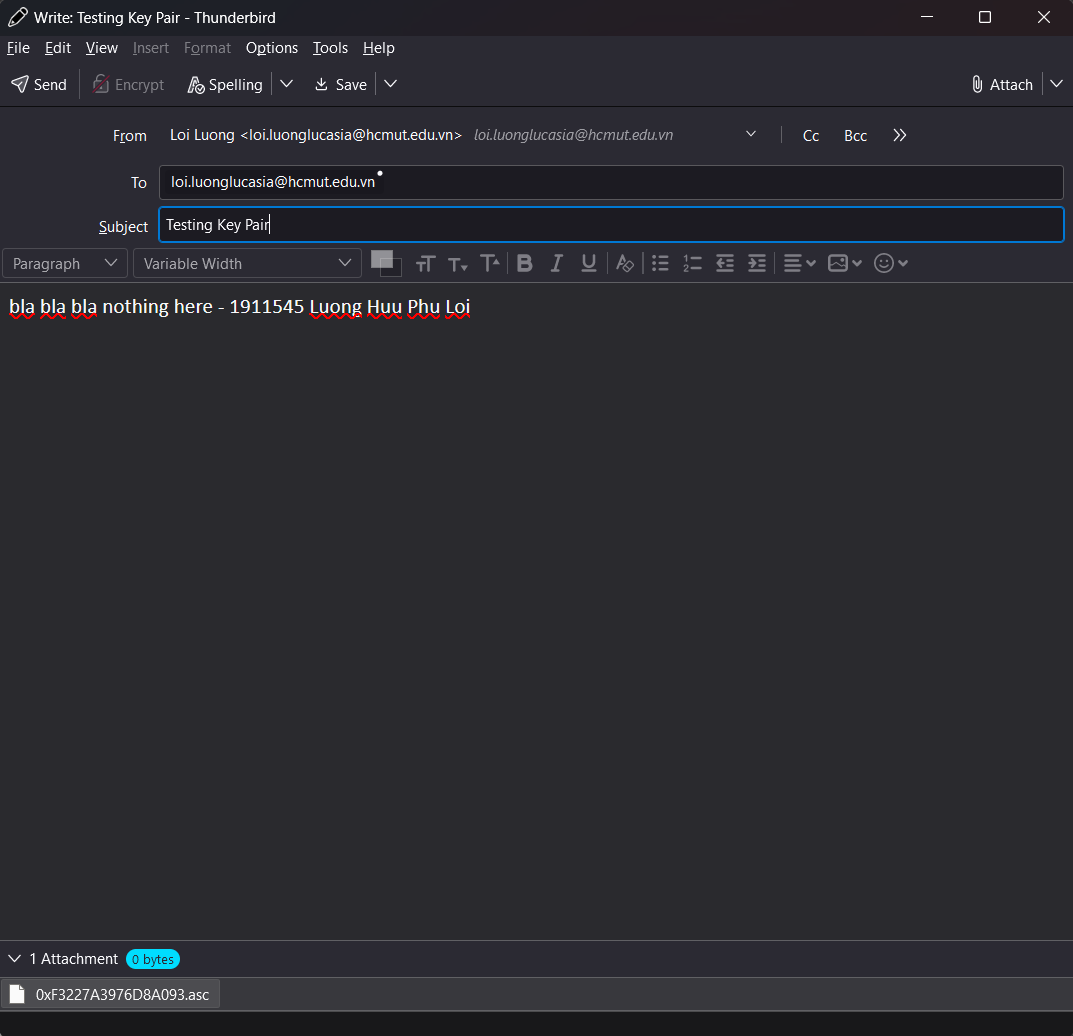
1. *Tạo thư và gởi đính kèm khóa công khai*

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**).**

**Bấm chuột phải vào key vừa tạo**



Chọn Send Public key By Email



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:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**- Ấn Save để lưu file chứa khóa công khai của người gửi**

**- Chọn thư mục muốn lưu rồi ấn Save**

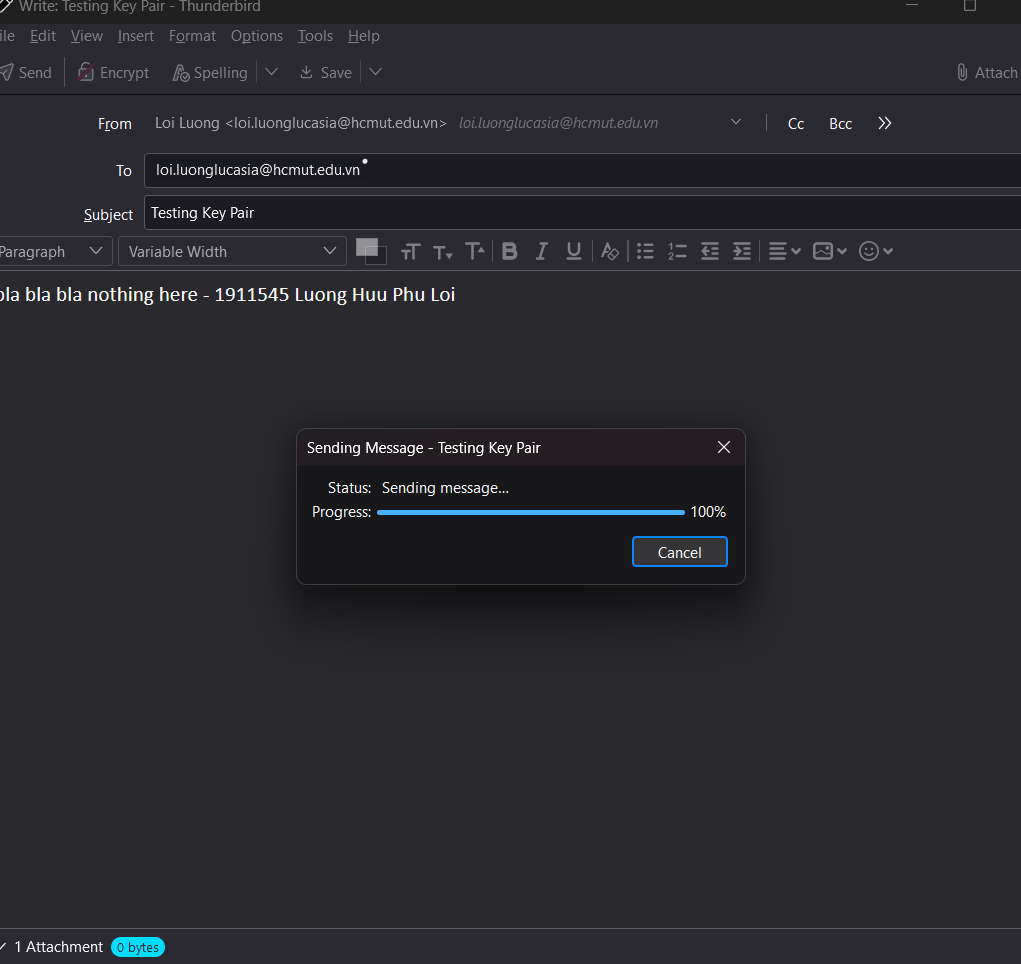
1. *Tạo thư, mã hóa và gửi đi*

Các bước thực hiện là:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**



1. *Nhận thư. giải mã, đọc thư*

Các bước thực hiện là:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**- Sau khi nhận được thư thì ấn vô mục**

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

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

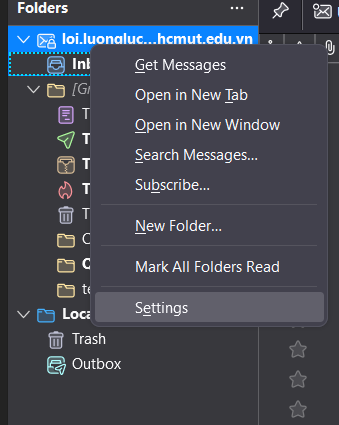
1. *Tạo thư, tạo chữ ký số, mã hóa và gửi đi*

Các bước thực hiện là:

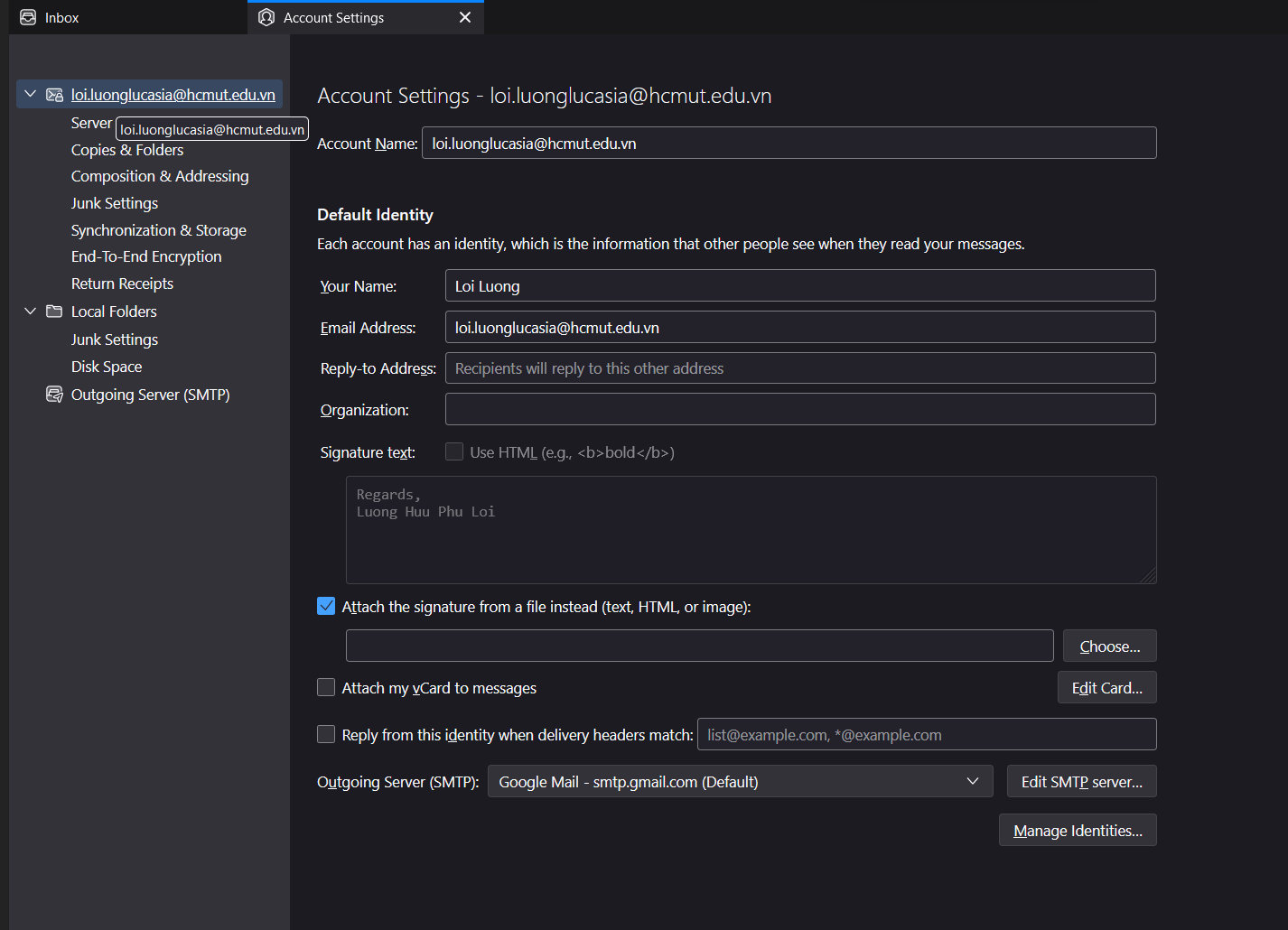
**…………………………………………………………………………………………………**

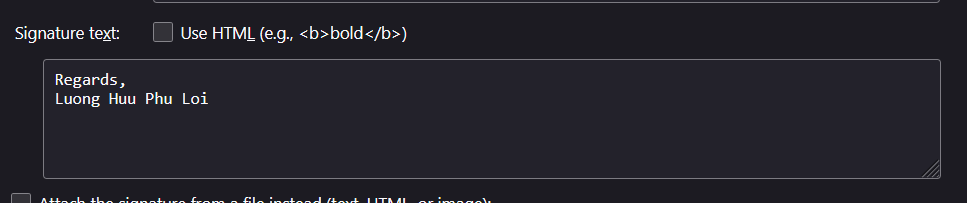
**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

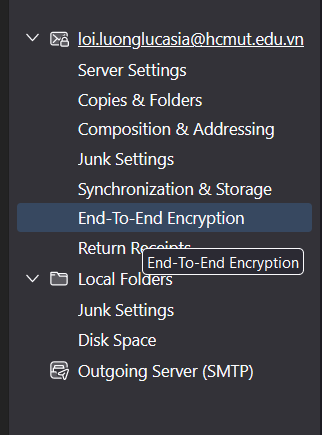


Bấm vào **Setting**

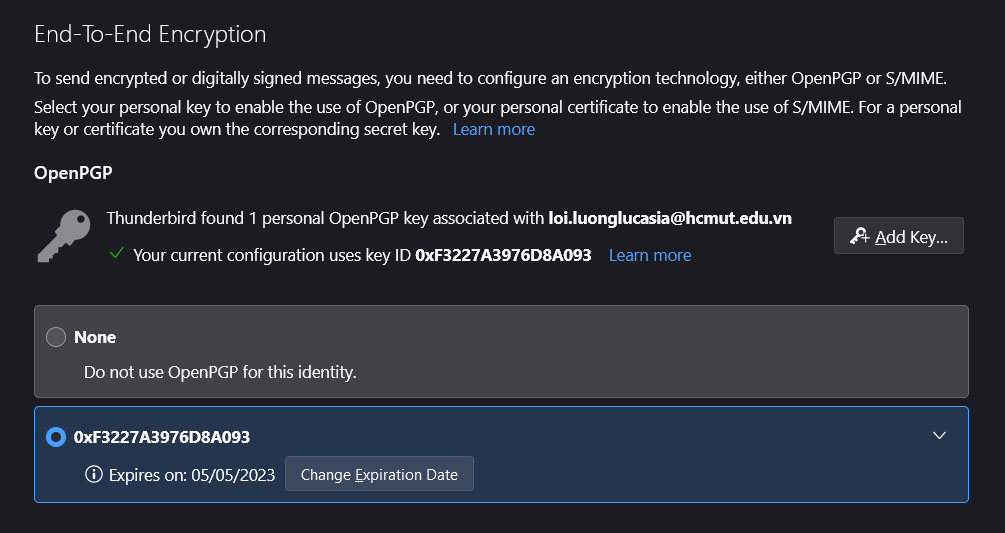




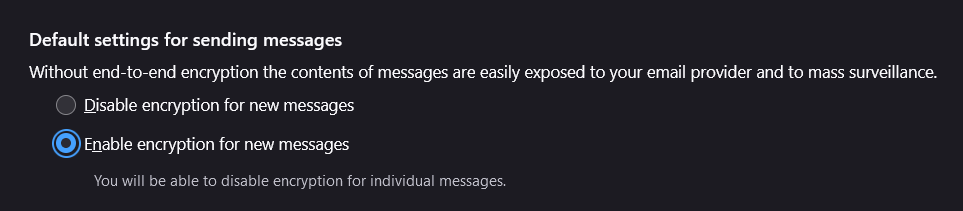
Tiếp theo



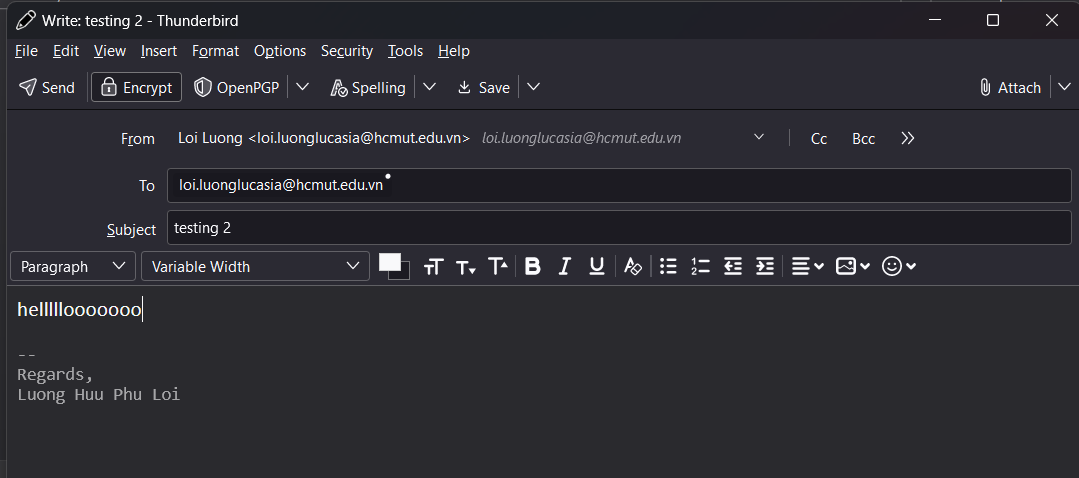
Chọn **End To End Encryption**

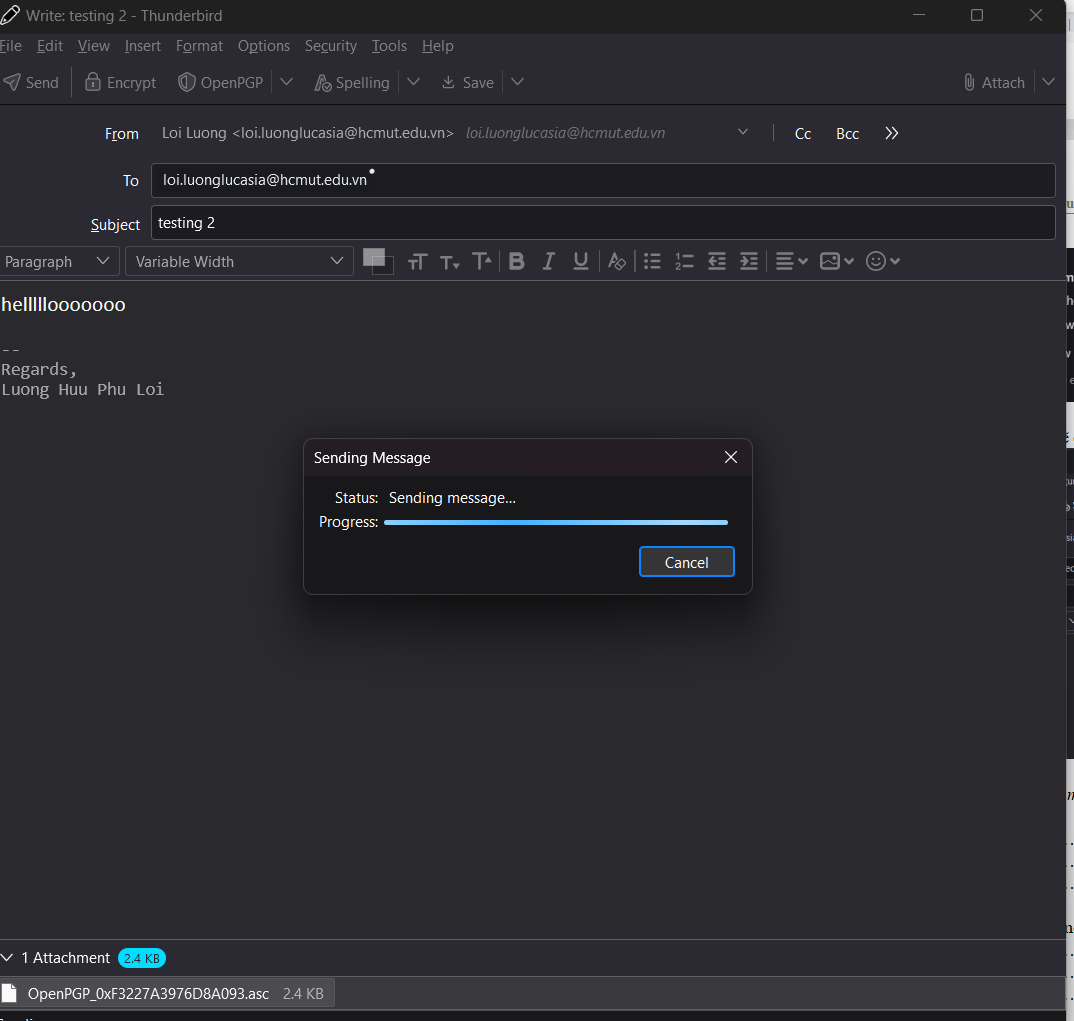


Chọn phần key vừa tạo



Lúc này, khi viết 1 mail mới sẽ có thể encrypt





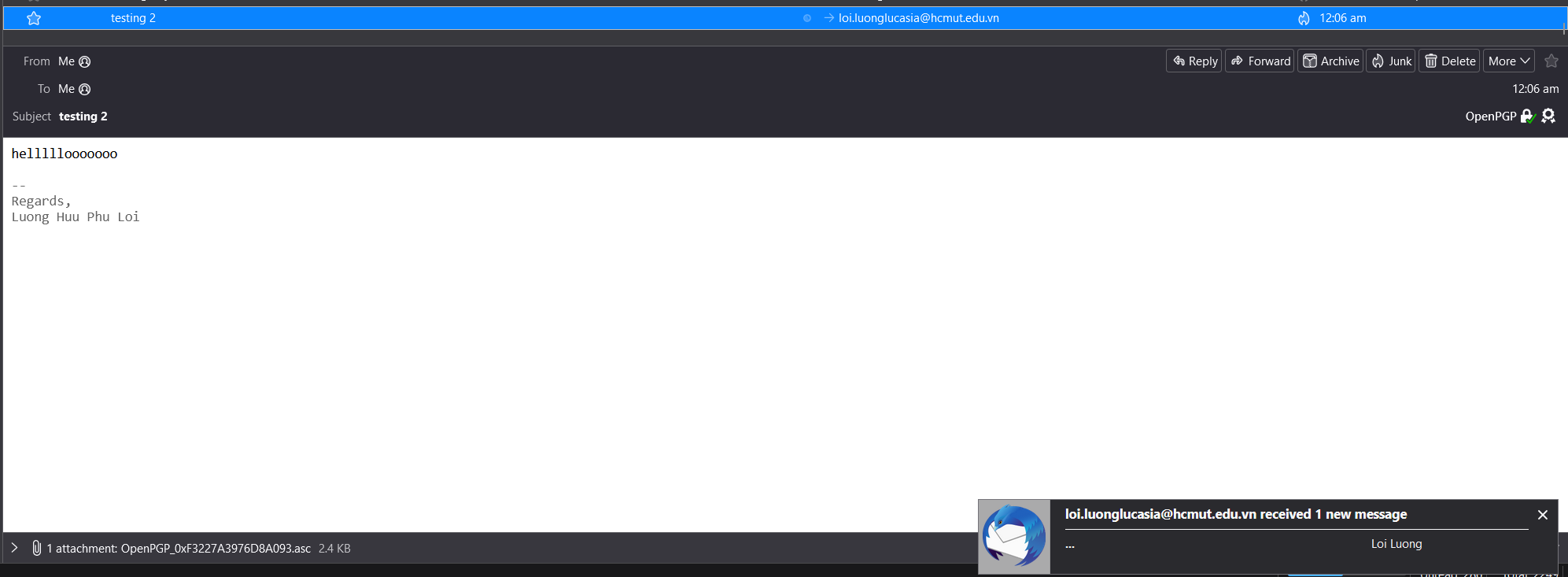
1. *Nhận thư. giải mã, xác minh chữ ký số, đọc thư*

Các bước thực hiện là:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**



**- Sau khi nhận được thư thì ta ấn vô thư và đọc thư.**

**- Phần chữ ký sẽ hiện phía dưới của nội dung thư**

**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**:**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**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:

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**…………………………………………………………………………………………………**

**………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………………………………………………**

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

Các bước thực hiện là:

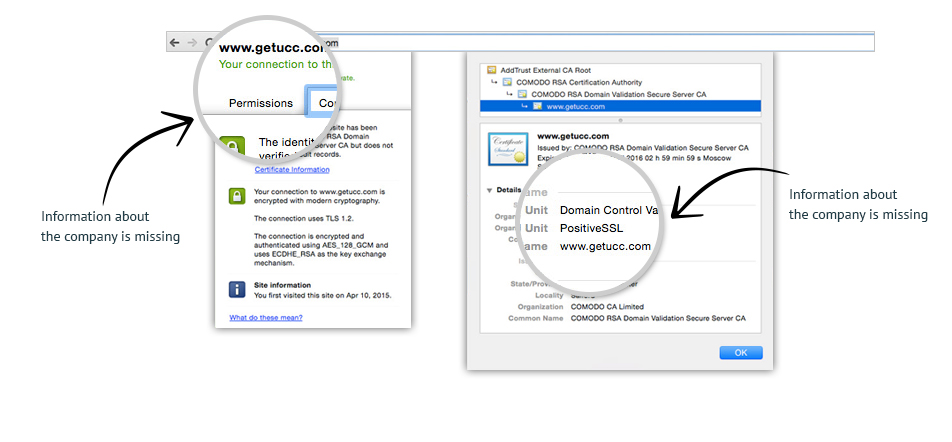
**………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………………………………………………**

**………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………………………………………………**

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

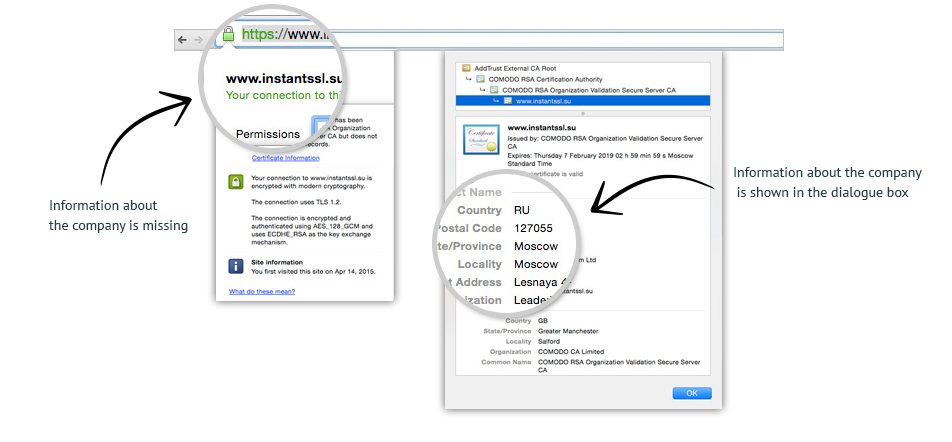
**………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………………………………………………**

**- Chứng chỉ SSL(DV):** Chứng chỉ DV (Xác thực tên miền). Đây là cấp độ xác thực SSL cơ bản nhất. Cơ quan chứng nhận (CA) chỉ đảm bảo rằng chúng ta là chủ sở hữu của một tên miền cụ thể bằng cách sử dụng thông tin có trong WHOIS.Loại chứng chỉ này cho phép mã hóa dữ liệu an toàn trên trang web, nhưng nó không xác minh rằng chúng ta là chủ sở hữu của một doanh nghiệp hợp pháp.



Chứng chỉ DV vẫn ổn khi bảo mật không phải là vấn đề đáng lo ngại: Tuy nhiên, kẻ tấn công cũng có thể sử dụng chứng chỉ DV trên các trang lừa đảo.

- Chứng chỉ SSL(OV): **Chứng chỉ OV (Xác thực tổ chức- Organisation Validation)** là bắt buộc đối với các công ty và tổ chức nơi người dùng phải nhập thông tin nhạy cảm (số thẻ tín dụng, thông tin liên hệ, v.v.) Đặc biệt, chúng rất hữu ích cho các trang web thương mại điện tử hoặc bán hàng trực tuyến. Chứng chỉ OV xác thực chủ sở hữu trang web và yêu cầu thông tin kinh doanh hợp pháp cho công ty đó. Quá trình xác nhận cho các chứng chỉ này dài hơn và chi tiết hơn. Tổ chức chứng nhận không chỉ xác minh thực tế rằng bạn sở hữu tên miền mà còn thực tế rằng bạn là chủ sở hữu của công ty. Công ty phải ở trong cơ sở dữ liệu đăng ký kinh doanh và trong một thư mục trực tuyến đáng tin cậy (ví dụ: dnb.com). Kẻ lừa đảo không thể có được chứng chỉ OV vì tổ chức của họ không thể được xác nhận.



**- Chứng chỉ SSL(EV):** Chứng chỉ SSL EV (Extended Validated) là loại SSL được khuyến nghị nhất vì nó hiển thị thanh địa chỉ màu xanh lá cây cùng với tên doanh nghiệp trong URLnhằm cho biết tính hợp pháp của doanh nghiệp và đảm bảo người dùng không thể truy cập được thông tin mà họ chia sẻ. Nó cung cấp mã hóa mạnh mẽ lên đến 256-bit giúp tăng sự tin tưởng và niềm tin của người dùng vào trang web.

Để cấp chứng chỉ EV SSL, nhà phát hành cần gửi các tài liệu kinh doanh quan trọng theo yêu cầu của cơ quan chứng nhận. Phải mất tới 10 ngày để cấp Chứng chỉ SSL EV.

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

**………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………………………………………………**