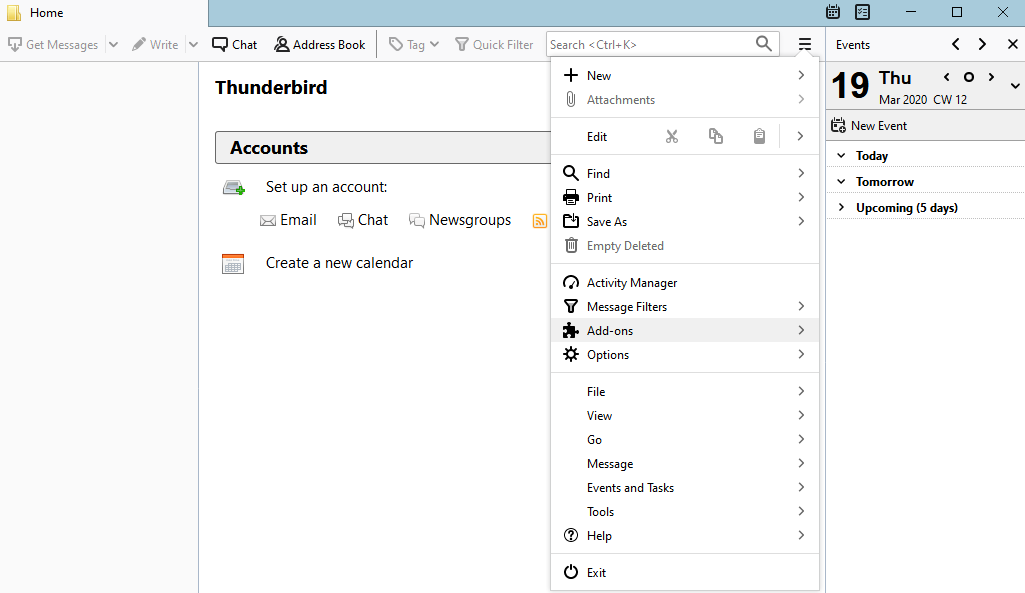
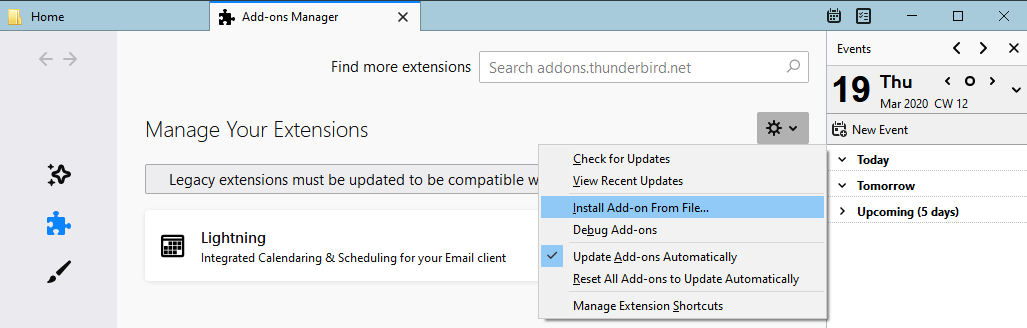
In this example I used Thunderbird as my email client.

**Installing Enigmail Extension for Thunderbird**

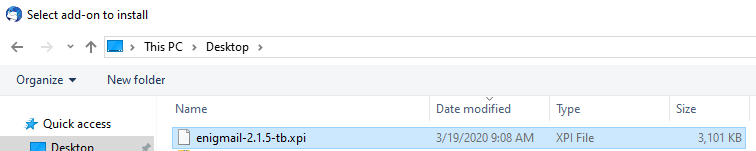
Step 1)

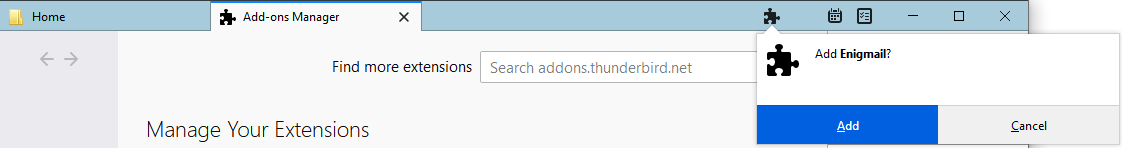


Step) 2

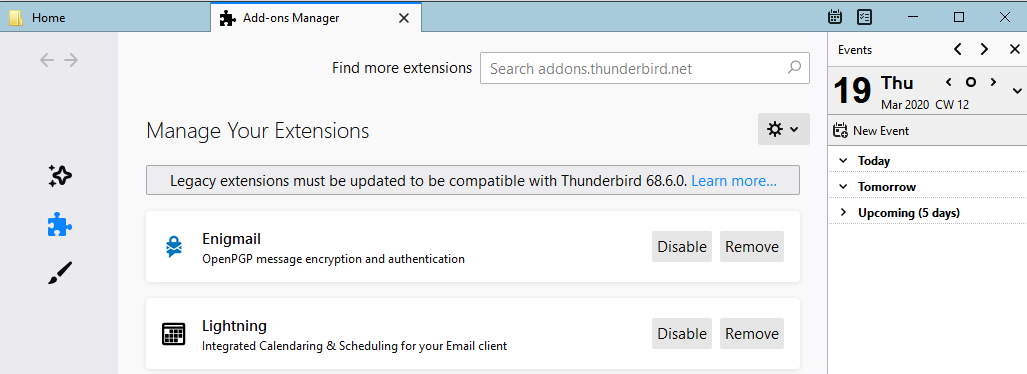


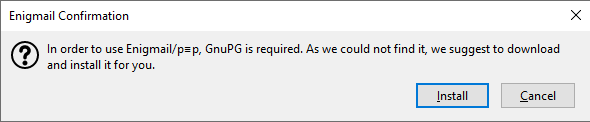
Step) 3



Step 4) 

Step 5)

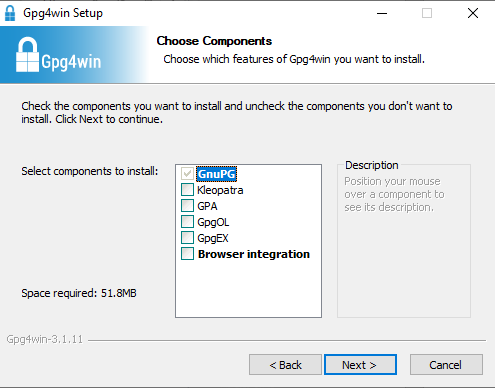


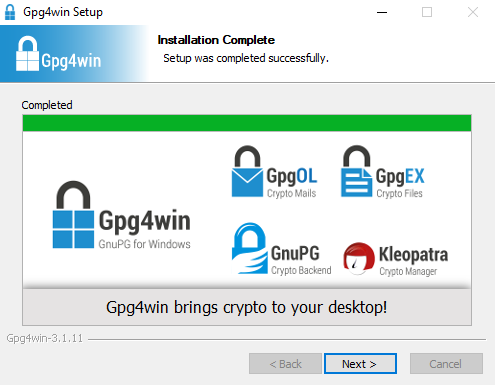
Step 6) 

Step 7)



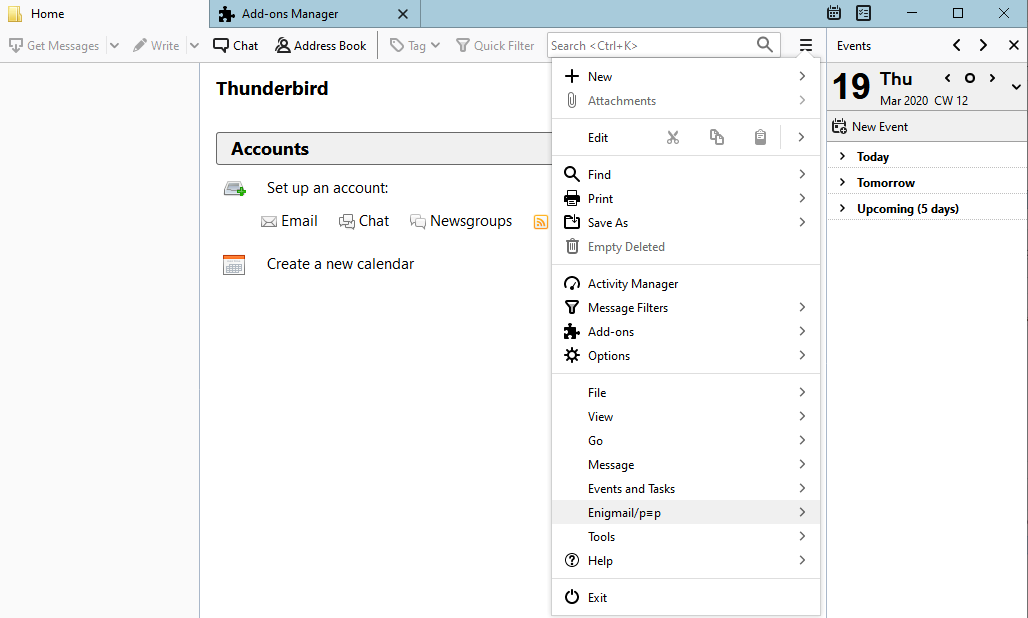
Step 8)



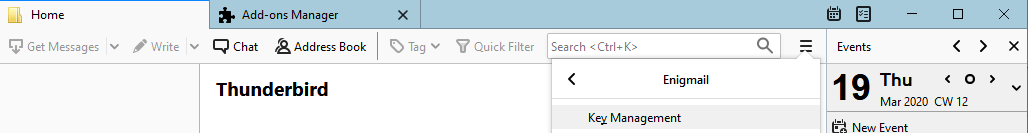


**How to send encrypted emails using Thunderbird**

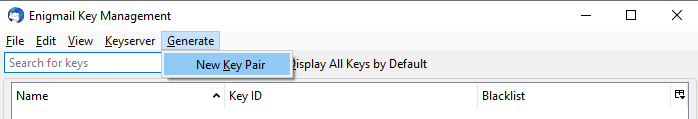
Step 1)



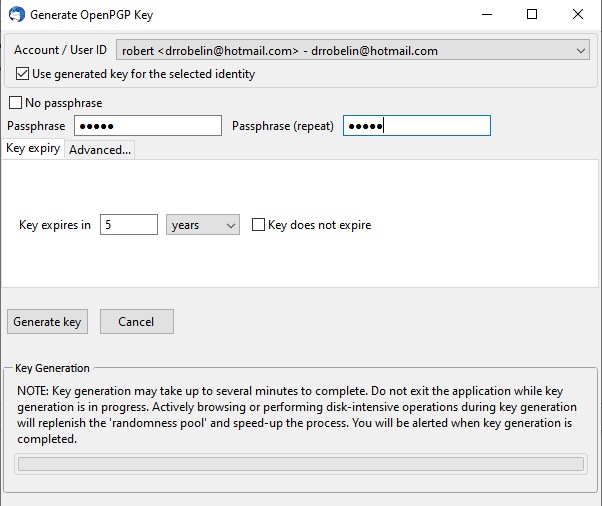
Step 2)

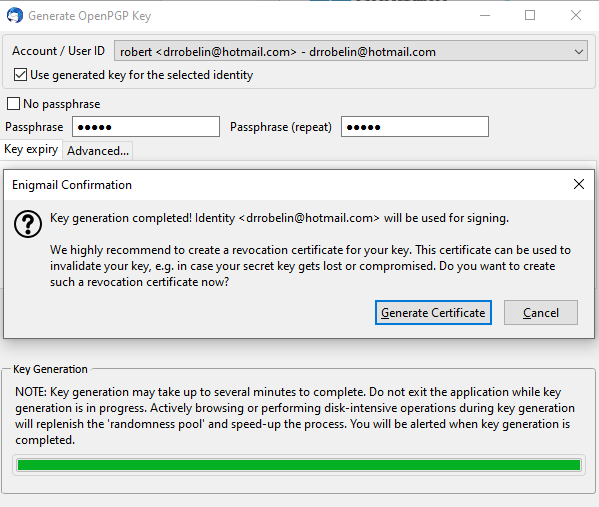


Step 3)



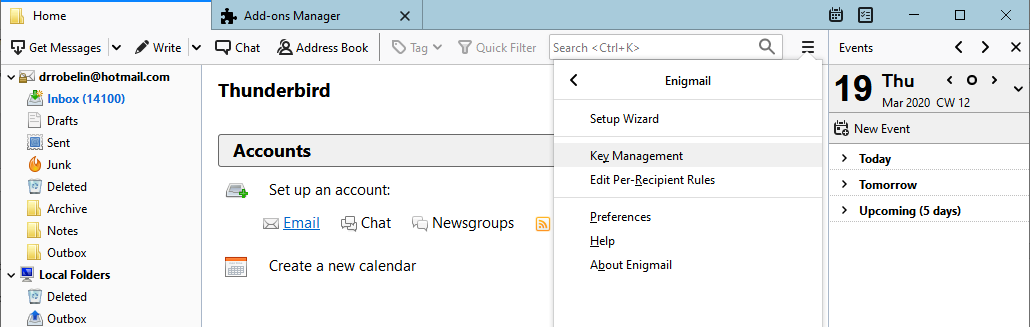
Step 4)



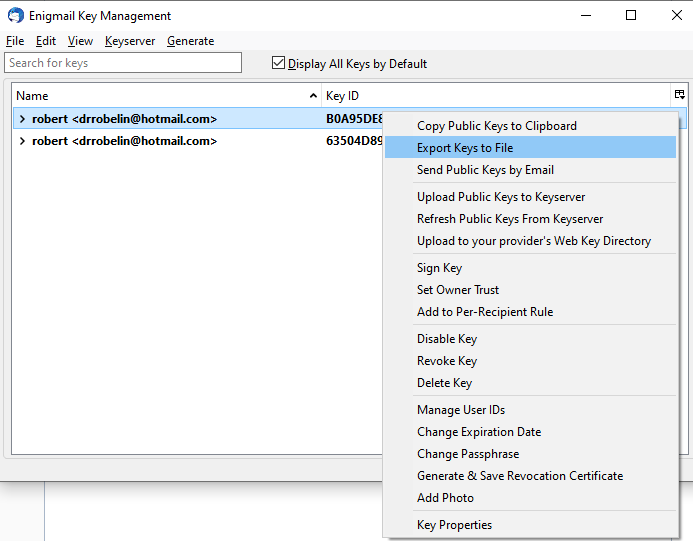


**How to save the Generate key for safe keeping**

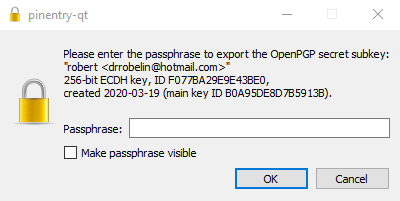
Step 1)



Step 2) Select the keys you want to save then select “Export Keys to File”

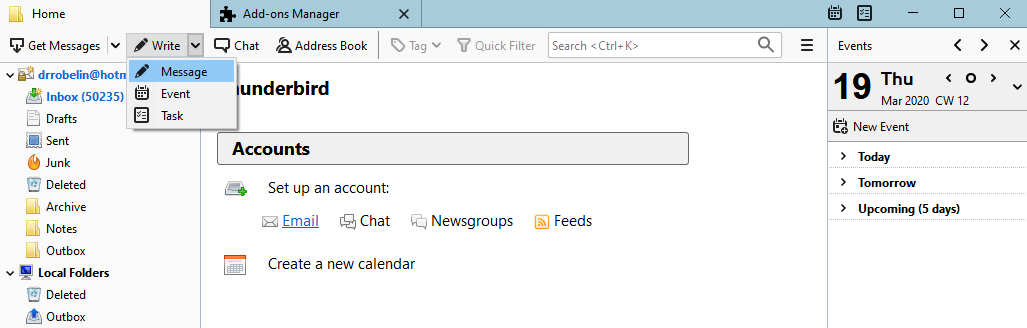


Step 3)

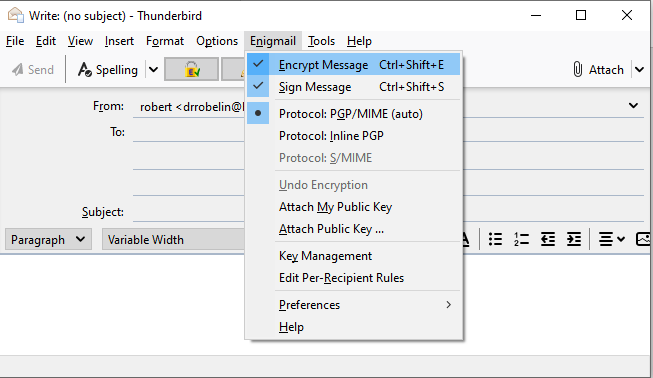


**How to send encrypted messages with Thunderbird**

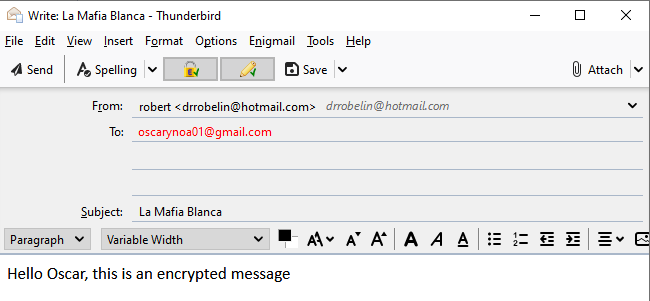
Step 1)



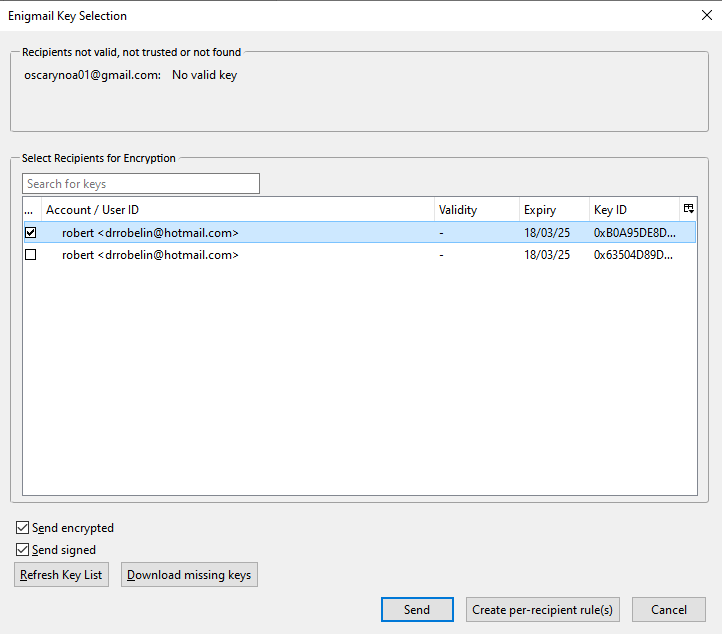
Step 2) Check “Encrypt Message” and “Sign Message”



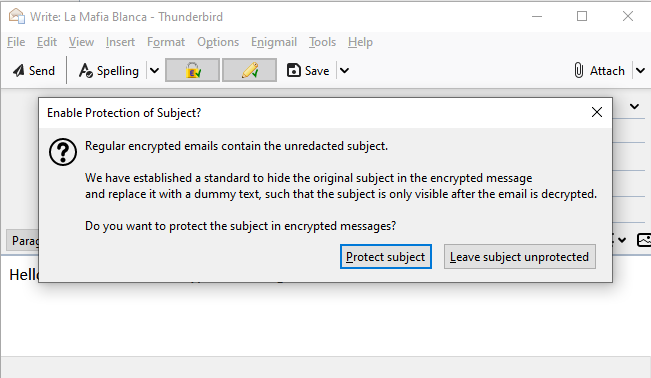
Step 3)

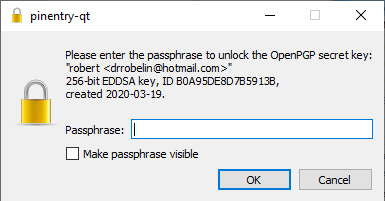
****

Step 4)



Step 5)





**Questions**

**Which service for encrypted email was easier to set up? Why?**

Both email clients do the same thing. However, Postbox is graphic interface is more intuitive and easier to use. I personally choose thunderbird in this example because is compatible with Linux and it’s from the same team that created the popular web browser Mozilla Firefox.

**Which one do you think is more useful? Why?**

As I said both of this email clients do the same for the average user. It’s about personal choice. They both use (IMAP) or the internet Message Access Protocol. For Receiving Email, they both use POP3.

The differences are that Thunderbird use Exchange Support and Postbox use SMTP. Exchange support use a Microsoft server as Outlook. In other words, a third-party server. SMTP sends the message from host to host without relying on an outgoing server. Thunderbird allows user to have multiple account. What I learned is that thunderbird is better for business because, it syncs your calendar, contacts based on the Exchange server, while SMTP must rely on the host.

**Is email considered private? Are there certain circumstances when that might change?**

No, your email isn’t private. Emails are stored in multiple locations thought the internet. Unless you set up your own private email server. The best way to make your email more secure is to use encrypted communications.

**Is it possible to have your private key be compromised?**

Yes, your private key can be stolen if you stored it in a computer. It’s important to store your private key on an external hardware.

**How secure is encrypted email? Are there are any negatives to using encrypted email (for both set ups you did in this lab)**

Nothing is safe at all, but encrypted message is safer than regular messages. It all depends on the sender and the receiver. The sender must be cautious when sending an encrypted message and where does he store the public keys. How secure is the sender computer? same thing goes for the receiver. There is so much variables that comes into play.

The negatives of using encrypted messages is that isn’t convenient as oppose of sending regular messages. The receiver must have some knowledge of how to open an encrypted message. They must have the same mail setup etc. Overall, encrypted message is not meant for the regular users.

**Is your phone encrypted? Why or why not?**

My phone isn’t encrypted. I’m an iPhone user. Encryption is only available for android users. What heard is that not every android phone can be encrypted.

**What are 3 pieces of information your phone collections (preferably ones you didn't know about before reading that article). Name and describe 3 ways you can be more careful with your phone and digital privacy.**

Your location, the way you’re holding your phone, your habits and more. The apps that you run in your phone is collection data about you. To see what data the app is collection about you, in the settings, find the app and see the permission you granted to it before installing. Must apps have access to your personal pictures, camera etc. Most of them collect every piece of usage in your phone. A phone has a GPS, it tracks your location every where you go.

The best way to be more careful is to encrypt your phone. Do not store personal pictures or important data in your phone. Second turn off the phone GPS. Do not give access to application to go into the root of the phone. Do not give them access to the picture library or camera. Read the terms and services of such apps.

**Talk to one person who isn't aware of how technology can affect their privacy, make sure to include information about why it might be important to them, and help them find 1 way to stay safer online either through a computer or their phone.**

I always tell my family that phones are not secure. All of them use iPhone to stay connected with each other. They don’t know the implications that a piece of technology as a phone can bring to them. Phones are not secure, but they are very convenient, and most them use it to stay in touch with family members across the country. My responsibility is to tell them how to stay safer while using such device. In the past, I have told them to never use public Wi-Fi. I have told them to never download free apps, because free apps have a malicious purpose. I told them about the GPS, but they prefer to have that option on. The GPS allow them to see each other, and according to them is a must have for children. Be able to see the location of your children is a safe feature measure for most parents that wants to track their children location.

**pick an app ( I recommend Signal but you can pick any top-rated app, TOR chat is new and not on the list but a good choice too) and try it out, find someone else either in class or in your life who can also use it and send some messages. How did it go? Was it noticeably slower?  What type of encryption does it use? Is it safe? How safe? Why would it be important to have a secure message service?**

For this example, I use TorChat. It is an instant messenger client that makes encrypted, anonymous chat and file sharing with your friends incredibly easy.

TorChat was a bit slower compared to the popular chat WhatsApp. It was 3-5 second slower. But overall, the experience wasn’t bad.

The type of encryption that TorChat use is a peer to peer instant communication. It uses the same type of encryption as Tor browser. It uses the “Onion Router”. The data is sent to different host in the TOR network until it reaches the desirable destination. Each node only knows the IP address of the previous nodes and the IP of the next nodes. Nothing in the internet is safe at all, the last node in the data is completely decrypted. It’s important to have secure message service, because you don’t want someone to altered or read your personal information.