certificate'. Save it in a safe place. Enigmail will ask about a 'revocation is. Get a cup of coffee or tea! Yum. two, depending on how fast your machine Key generation might take a minute or you'll also need to enter this passphrase. eucrypted with your unique public key for your email - in order to read email least). This is an extra layer of protection email and computer password, at the keypair (make sure it's different from your Choose a secure password for your sharing part in a bit).

exchange secure email (we'll get to the bublic' key, which we'll share with folks to key (which stays on your computer), and a pair': as we said earlier, this is a 'private' On the next screen we'll create a 'key Create a Key Pair

.'noiferugifnoo screen select 'l prefer a standard Start setup now', and then on the next configuration will be totally fine, so click pop-up. For most folks the 'standard' installing Enigmail a set-up wizard should When you first open Thunderbird after Set-up Enigmail:

Sharing your public key:

In order for someone to write an encrypted email to you, they need to have a copy of your public key on their computer. You can share your key in a variety of ways, but the easiest ways are probably over email, and by uploading to a keyserver.

Click the hamburger:

Find Enigmail -> Key Management. This will show you the public keys saved on your machine, and let you do various things with them.

Right click on your key!

something like Alice ⟨axyridis@riseup,net⟩

If you click 'Send Public Keys by Email' you can share your key with anyone whom you trust. Make sure you get their key too, and then all of your correspondance will be safe!

If you click 'Upload Public Keys to Keyserver' your public key will be uploaded to a server. This means that other people will be able to find your public key, simply by looking for a key has your public key can verify that the associated with your email address. Neat!

keypair. It's super handy! importing public keys, as well as making your own this, and provide tools for managing, signing, and installing the other software (GnuPG) that we need to do and decrypt emails encrypted with GPG. It will automate Enigmail is a plugin that will allow Thunderbird to send find version 1.8.2. Install it!

for a plugin called Enigmail. You should

Search all add-ons we want to: corner: 🚍 and then find 'Add-ons'. Now Click on this button in the upper right

https://support.mozilla.org/en-US/products/thunderbird See https://en.wikipedia.org/wiki/GNU_Privacy_Guard for so you may want to check out the documentation at Thunderbird is a powerful, but simple to use program, well you should be presented with your email! Riseup, and most common email providers). It all goes address. It usually gets this right (it will for Gmail, server settings to download and send email using your recommended) and Thunderbird will try to guess the next screen you'll see options for POP or IMAP is address, and the password you use to log-in. On the you first run it. This will ask for your name, email Thunderbird should pop-up a 'new account' wizard when

Set up your email account

on your computer. that we have access to the GPG private key we'll store browser (as Gmail does). We need a local mail client so computer as a separate application instead of in a web Thunderbird is a local mail client, so it runs on your install with your package manager (Linux) 1. Visit https://getthunderbird.com or

Ok let's go!

for more details.

Sending Encrypted Mail:

OK, so we've made a key, we've shared it with our trusted friends, and maybe they've shared their keys back. How do we actually write an encrypted email to someone?

Well, it's pretty easy! Enigmail takes care of almost all of the work. If you write an email to a friend (say her email is sarah@example.com), and you Sarah's public key on your computer, Enigmail will automatically encrypt your mail message with Sarah's key, so only she can read it. Nice!

You can be sure an email is going to be encrypted when the following appears in the 'compose' window:

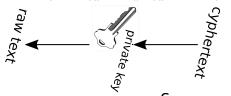
Enigmail:

This message will be signed and encrypted signing is different encryption. Signing uses your private key to digitally sign the message because of the pairing between your public and private keys, a recipient who message came from you.

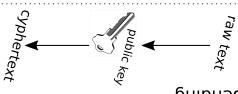
- An hour or so! - An internet connection version of Linux) - A computer (Mac OS, Windows, or any Forwarding and POP/IMAP -> Enable is preferable (for gmail users: Settings -> - An email account! One with IAMP access

What you need:

more details on how GPG encryption works.



Receiving



guibne2

That's the basics! For more:

- https://emailselfdefense.fsf.org/en/
- https://www.cryptoparty.in/brief#email
- https://ssd.eff.org/en
- https://tech.safehubcollective.org/cyber

All files related to this zine can be found here:

https://github.com/aliceriot/PocketGuide Improvements, suggestions, and corrections are most welcome! Contact info for the author at https://aliceriot.github.io/contact

creative

This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. To view a copy of this license, http://creativecommons.org/licenses/by-nc-sa/4.0/.

> Please print and share! **Encryption works!**

in practice! complicated, but it works and is simple corresponding private key. This sounds only be decrypted (for reading) by the encrypted with a user's public key can key is shared widely. An email key stays on one device, and the public private) which are paired. The private cryptographic keys (one public and one works with a 'key pair', a set of two except the intended recipient, GPG that they are unreadable by anyone (GPG), which can encrypt emails so software called Gnu Privacy Guard We're going to set-up a piece of How does it work?

Mhy encrypt?

to use software to prevent that! text. This sucks, but anyone can learn traveling across the internet in plain eucryption your correspondance is you're not currently using strong government agencies. In any case, if out of surveillance imposed by a lawyer, maybe you just want to opt-Maybe you're an activist, maybe you're



resist the surveillance state!