Passwords are the weakest link when it comes to secure communications, because an enemy will basically always guess a password before they break encryption. It is therefore important to have good password practice.

A strong password has at least twelve characters long and contain numbers, punctuation marks, and both upper-case and lower-case letters. It does not contain any words found in the dictionary, but words that have been rendered unrecognizable due to substitutions and distortion should be good. It is very important to use a unique strong password for every account that you can't be compromised. For things that don't matter, a simple generic password is fine.

It can obviously be difficult to remember numerous strong passwords, though it usually becomes easier after you've used them for a while. With this in mind, it is better to use a good password and write it down somewhere than to use a bad password that you'll remember. You can always destroy your note later on, once it's stuck in your head.

****

It is important to use encrypted communications as much as possible, because it defeats the purpose of encryption if only the “high-risk” information gets transmitted securely. It is ideal that all information, from elaborate schemes to grocery lists, look like the same mess of code to an outsider, so that it's totally impossible to know where to begin with further investigation.

****

This pamphlet does not deal with anonymity, because that is a separate subject from secure communications. High-profile super activists can, and should, communicate securely, for example. It is not pointless, as some people think, to use encryption with an email account with your legal name in it. The message will still be unreadable to anyone but the recipient and the sender.

****

None of these techniques are a guarantee of complete safety. There is no such thing as an impenetrable fortress. What we are doing is setting up obstacles. Eventually, with enough time and energy and ingenuity, any one obstacle can be overcome – but if the obstacles are endless, if they are everywhere, and if there's never any certainty that what's on the other side is even worth all this trouble, the enemy will often feel defeated and give up on their own.

****

You can contact us (about technical problems, with questions, etc.) at...

ats-mtl@riseup.net

And our website is...

ats-mtl.com

A SHORT GUIDE TO SETTING UP

ENCRYPTED ONLINE COMMUNICATIONS

BY ATS (ANARCHIST TECH SUPPORT COLLECTIVE)

Encrypted email.

Get a secure email account. We recommend using riseup.net because it's easy to use, their services are extensively documented and well-supported, and they are politically trustworthy. To get a riseup.net account of your own immediately, you will need invite codes from two different account-holders.

Download GnuPG. Once installed, this encryption protocol interfaces with Enigmail, an add-on for the open-source email client Thunderbird. If you have Windows, go to gnupg.org/download , scroll down to "Binaries", and select the "FTP" link for Windows (the one with the letter *B* next to it). If you have a Mac, go to macgpg.sourceforge.net, scroll down, and download the version "1.4.9" of GNU Privacy Guard, unless you have an older system.

Set up Mozilla Thunderbird. You can download Thunderbird from mozillamessaging.com. When you open the program for the first time, it will request information for an email account; give it the info for your secure account. There are two crucial add-ons to download: Master Password +, which provides an extra level of security, and Enigmail. Follow Tools menu -> Add-ons -> Get Add-ons -> Search All Add-ons. Search for both add-ons, hit Add to Thunderbird..., and once you have both, hit Restart Thunderbird.

Create a key pair. A key pair has two parts: the private key and the public key. The private key is kept only on your computer and possibly on a backup. The public key is distributed to those who you want to communicate with securely. To create a pair, follow OpenPGP menu -> Key Management -> Generate menu -> New Key Pair, then enter a strong password. Hit Generate key and, once that process is done, hit Generate Certificate in the notification window that comes up. Save that file to an external device, like a USB key or a CD. If a key pair is compromised, the revocation certificate can be used to disable it. To see it, check Display All Keys by Default in Key Management.

Signing and encrypting emails. When you compose a new email, you will see the icons of a pencil and a key in the lower-right corner of the window. Click the pencil to sign an email; this indicates that the email could only have been written by someone with your private key, which should only be you. To encrypt a message, click the key; doing so means the message can only be read by the person you designate as the appropriate recipient, i.e. the person in possession of the private key corresponding to the public key you choose.

Keyservers. A keyserver is an online database of public keys. If you upload your key there, others can download it from there directly without having to contact you. However, uploaded keys remain on the keyserver permanently. To upload a key, righty-click your key in Key Management and select Upload Public Keys to Keyserver. To download a key, follow Keyserver menu -> Search for Keys. The search bar at the top of the Key Management window searches among the keys already on your computer.

Exporting and importing keys. To send a public key to a friend, right-click it in Key Management and hit Send Public Keys by Email. To save a key elsewhere, such as a backup, right-click and hit Export Keys to File. It is useful to back up your own key pairs; when doing so, you should select Export Secret Keys in the notification window that comes up. To import a key from a file, follow File menu -> Import Keys from File.

It is also possible to render a key in textual form. To import a key like this, copy the key from the first dash to the last dash, no more no less, and follow Edit menu -> Import Keys from Clipboard in Key Management. To export a key in text form, right-click it and select Copy Public Keys to Clipboard, then paste it wherever you want to.

The web of trust. Right-clicking a key in Key Management, two of the options you get are Sign Key and Set Owner Trust. Signing a key is an indication that you have confirmed the key in question actually belongs to the corresponding person. Owner trust is an indication of whether you think the owner of a given key will sign the keys of others only after careful checking. It is not supposed to be an indication of how much you trust a person otherwise.

All of this is supposed to form an informal identity verification system called the web of trust. If your friend has signed a stranger's key, for example, you will be able to see that when that stranger contacts you. In fact, it is possible to be connected to people by several degree of separation in this way. None of this is necessary to encryption, and there is some concern that this makes it possible to map social networks if signed keys are posted on keyservers. It is possible to only use local signatures and only sign keys for your own recordkeeping.

Encrypted instant messaging.

Get Adium or Pidgin. Adium, an instant messenger client for Mac, can be downloaded at adium.im, and Pidgin, the equivalent on Windows and Linux, can be downloaded at pidgin.im. Both programs come with an encryption protocol called OTR built-in. For Pidgin, follow Tools menu -> Plugins -> find "Off-the-Record Messaging" in the long list and check it. Hit Configure Plugins and set the default settings to require private conversations and not log. This isn't necessary with Adium.

Get a Jabber account. OTR will work with GChat and MSN, but using these protocols does not hide who you communicate with and when. An XMPP account obtained at jabber.org is more secure. You can have more than one account if you want to keep using old accounts.

Encryption. In Adium, the OTR menu is in the form of a padlock. For others using OTR, click the padlock and set conversations to automatically encrypt. With Pidgin, it is easier to change the settings for those who *don't* use OTR by following Conversation menu -> More - Settings and changing it there. For encryption to be useful, it should be used as much as possible.