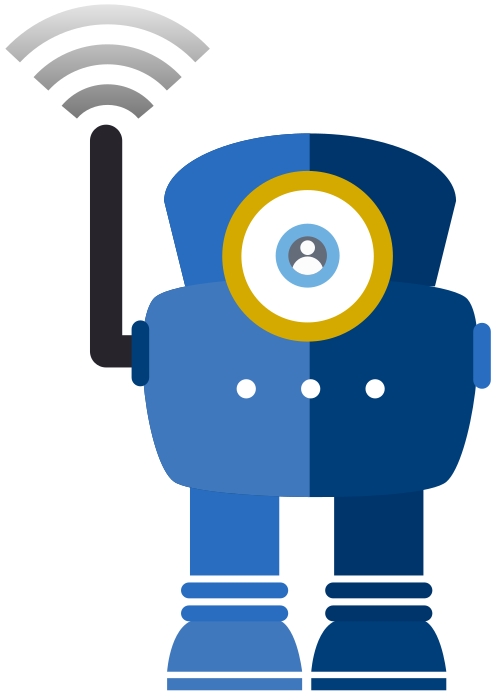
MARCH 30 • 5-7PM



Information Society Project
Yale Law School

MFIA
MEDIA FREEDOM & INFORMATION ACCESS CLINIC

DIGITAL

01111001011011110111010

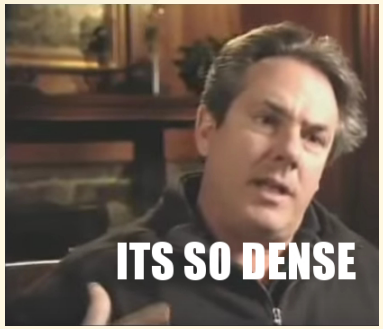
SELF-DEFENSE

Learn how to encrypt your e-mail with **PGP** and use secure text / audio / video chat like **Signal**. Workshop designed for YLS Clinic students.
Bring your laptops & mobile devices!

40 ASHMUN • A422

Facilitators: Sean O'Brien | Hannah Bloch-Wehba

These Slides are Detailed



Grab a copy of the presentation:
privacylab.yale.edu/slides/yls-clinics01

Refer back to it later, read it slowly, & click the links.

- If you don't do everything or fall behind, that's okay. **Learn 3 new things**.
- If you don't have a computer/phone, or it's acting up, make a friend in the room and follow along.

Sharing is Caring: Please copy, share, and remix!

Our Goals Today:

1. **Set up PGP-encrypted e-mail (GPG / GnuPG)**
   - Manage e-mail via Thunderbird & Enigmail
   - Back up and manage our public/private GPG keys.
   - Safely share our public GPG key.
2. **Browse and share anonymously via Tor**
3. **Try mobile apps like Signal / Noise, Kontalk.**
4. **Web-based audio/video chat via Jitsi Meet.**

Guiding Principles:

1. Trust is earned. Not bought, decreed, or promised.

2. Free and Open Source Software (FOSS) is an essential security requirement (not a guarantee).

3. Solutions must be both *libre* & *gratis* to reduce friction, encourage sharing, avoid discrimination.

4. Advertisements & surveillance go hand-in-glove.

5. Data is a toxic asset.

6. Centralization is dangerous.

Etherpad for Live Q & A

Let's name a new pad at pad.riseup.net

...this pad will self-destruct in 30 days.

- This is "Security by Obscurity".
  Do not type info in the pad you wish to remain private.
  If the pad name is guessed or shared, anyone can view it.
- Riseup.net hosts awesome services.
  Donate if you can, they almost had to shut down in 2016.

Other options: Riseup .onion Etherpad (Tor only)
Mozilla's public Etherpad | Try Ethersheet for spreadsheets

Intro to Encryption

How math can keep us secure.

Watch on YouTube ➡️

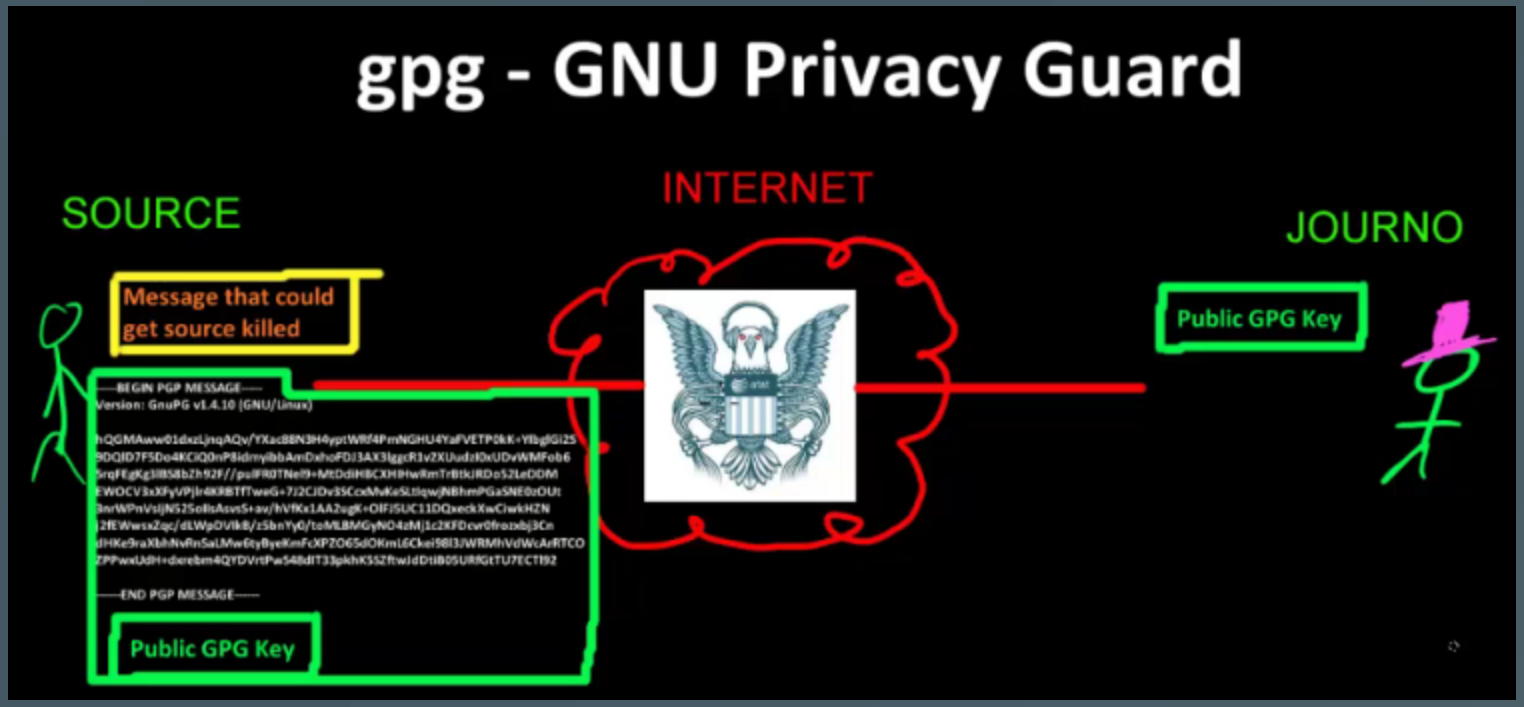
Demonstration:

Up and running with

Encrypted E-mail

GPG guide by anon108

Uploaded Jan. 6, 2013. Can you name the voice?



[Watch on Vimeo ➡️]

You Down with PGP? *Yeah, GnuPG!*

We say "GPG" because we're using the **GNU Privacy Guard** implementation of **Pretty Good Privacy**.

Download Thunderbird ➡️

Follow the EFF's guide for your operating system:

GNU/Linux | **MacOS** | **Windows**

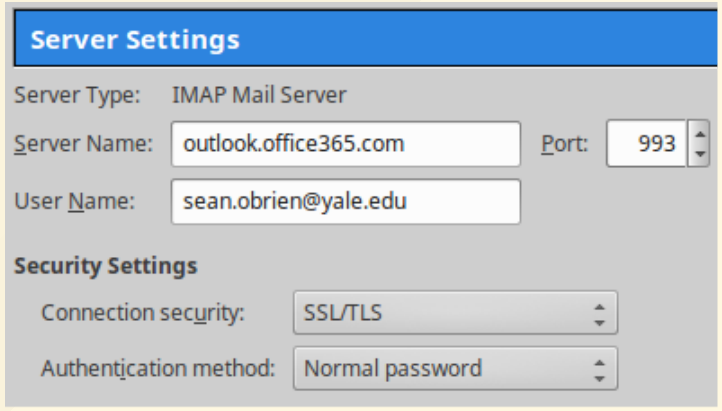
- You can use your existing e-mail account.
- Configuration guidance on the next slide.

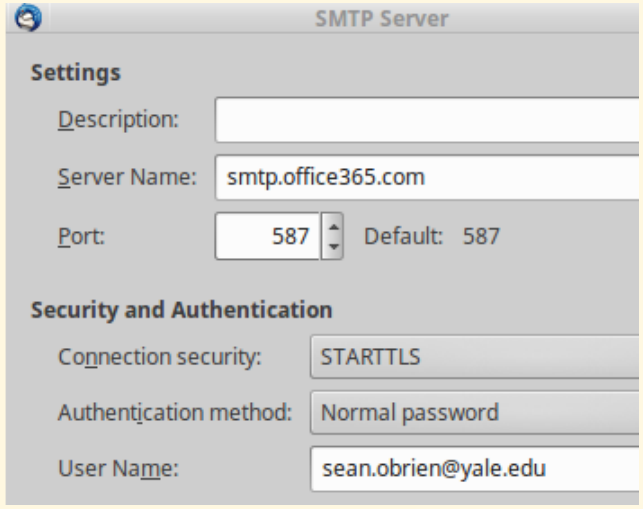
Find your IMAP & SMTP settings

- Thunderbird will guess settings for big hosts like Gmail.
- **@ylsclinics.org** settings:

		Server hostname	Port	SSL	Authentication
Incoming	IMAP	imap.secureserver.net	993	SSL/TLS	Normal password
Outgoing	SMTP	smtpout.secureserver.net	465	SSL/TLS	Normal password
Username		Your email address			

- **@yale.edu** settings:





Answers to Common Questions

- Metadata such as e-mail headers, DKIM signatures, and message Subject are **not private**.
- You use your friend's **public** key to encrypt for your friend. Your friend uses your **public** key to encrypt for you.
- You may publish your **public** key to the public keyservers, attach it to an e-mail to your friend, use sneakernet, or try OnionShare & Up1 over Tor (more on this later!).
- Your **private** key & revocation certificate should be stored in safe places, separately, perhaps even CD/DVD and paper.
- If you lose your **private key**, you lose messages encrypted with it. The public key will live forever on the keyservers.

More Answers, Tips & Tricks

- You should turn off HTML in your e-mail.
- Use the Key Management dialog to change your key settings (identity / e-mail accounts associated with it).
- Use Key Management to sign keys of your contacts, set the trust level of keys, and set per-recipient rules.
- Use Key Management to back up your key pair, generate a revocation cert, and download missing keys for contacts.
- In your Account Settings make sure your Draft and Trash messages are stored in local folders.

Even More Tips!!!!!!111

- To encrypt attachments, you must use PGP/MIME (the default). If you have issues with this, turn it on and off.
- GPG messages can't be checked by server anti-virus. This may result in "UNCHECKED" being appended to the subject by the e-mail server. If so, set Inline PGP as default.
- You should use GPG to verify identity by signing messages.

If all else fails, you can manually encrypt the message and copy/paste into the e-mail body, like Snowden in this video. Use GNU Privacy Assistant.

Options for Other E-mail Clients

- **Apple Mail:** You can use the GPG Suite. Your mileage may vary, and Apple Mail + GPG has a very rocky history.
- **MS Outlook:** You can use Gpg4win and the GpgOL plugin for Outlook.
- **Android:** Install F-Droid and use K9-Mail + APG.
- **iOS:** iPGMail and oPenGP are your best options, though they are not *libre* or *gratis*.

Making First Contact

Establishing a trusted connection

Privacy tools require trust and a shared secret. That secret could be a username, a URL, a passphrase, or an encryption key.

- Share a secret using tools you learn about today.
- Meeting in person may be the best method.
- Etherpads, pastebins/imagebins like Up1, and "burner" temporary e-mail accounts are good options.

Try to use Tor Browser or Orfox for first contact *(we'll cover this later)*.

Onion Routing via Tor

Be truly anonymous on the Internet.

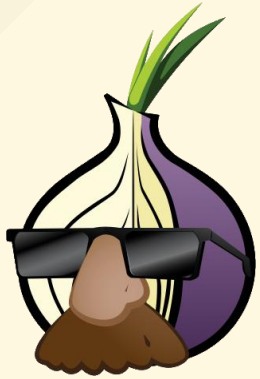
[Watch on YouTube ➡️]

Demonstration:

Try out

Tor Browser Bundle

Anonymous Web Browsing



We'll use Tor to share secrets, GPG keys.

Download Tor Browser Bundle ➡

It's Firefox, but anonymous! Security plugins pre-installed.

Download OnionShare ➡

Creates a temp Tor hidden service (.onion address)
for sharing files/folders with other Tor users.

6zc6sejeho3fwrd4.onion *Up1 filesharing and pastebin.*

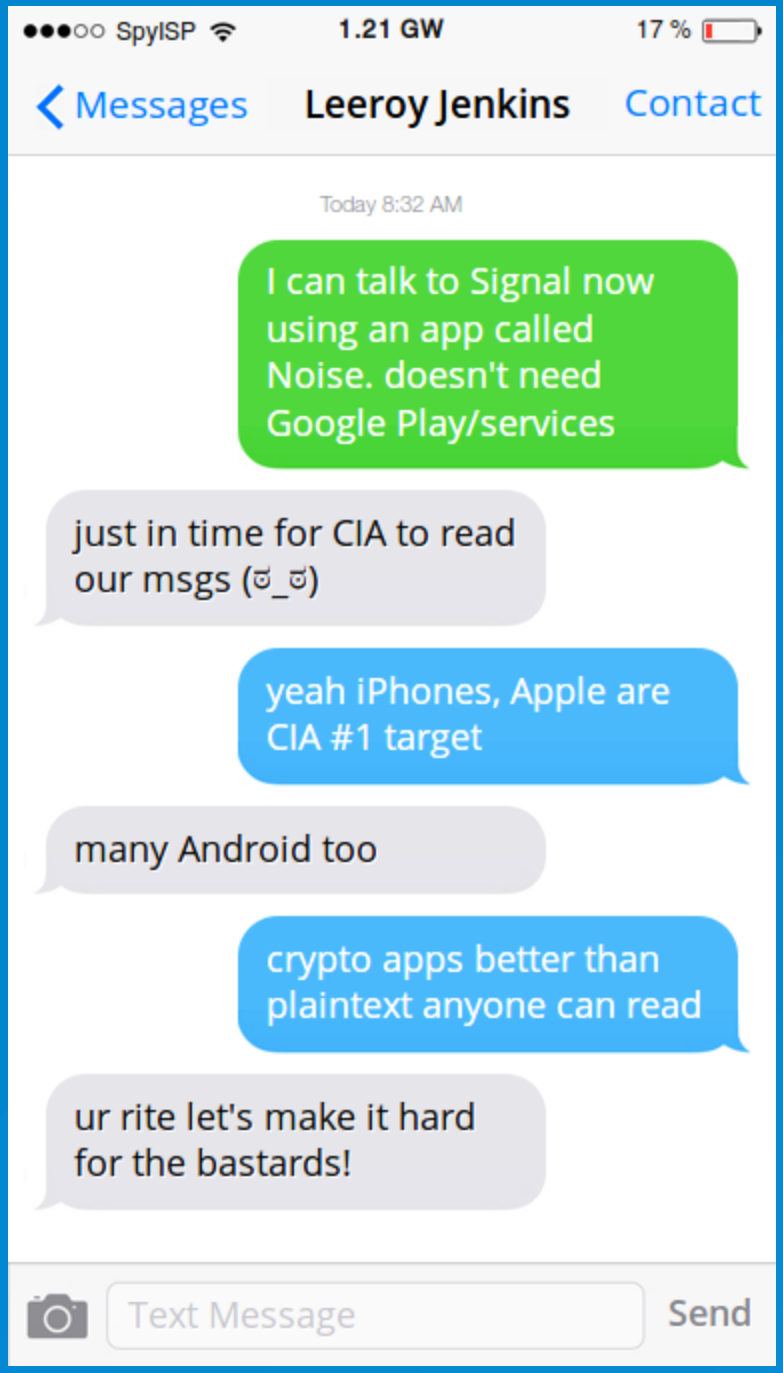
share.riseup.net in a non-Tor browser.

Onion Sites That Don't Suck

Tor anonymity is the gold standard

The Tor network thwarts the NSA's best efforts to break it (we know this thanks to Snowden).

- **However:** Using Tor is not a magic bullet. Vulnerabilities may occur over time, so **update often** (TBB will nag you!)
- **TBB Settings:** Go with the defaults. Customization makes you more susceptible to browser fingerprinting.
- **Bridges:** Use if Tor is blocked or you need extra protection.


●●●○○ SpyISP
1.21 GW
17 %
Messages
Leeroy Jenkins
Contact
Today 8:32 AM
I can talk to Signal now using an app called Noise. doesn't need Google Play/services
just in time for CIA to read our msgs (ಠ_ಠ)
yeah iPhones, Apple are CIA #1 target
many Android too
crypto apps better than plaintext anyone can read
ur rite let's make it hard for the bastards!
Text Message
Send

Did #Vault7 break Signal & WhatsApp?

There's no evidence the CIA broke the Signal protocol itself, which WhatsApp also uses.
No private chat app, Telegram or any other, has been mentioned as being cracked.

The underlying operating systems iOS and Android have been pwned. We don't know the full extent of the Android pwnage (all AOSP? just some firmware?)

- If your text, audio, and video are being recorded before a private chat app can encrypt them, what's the use?

This highlights the importance of controlling, upgrading, and switching your OS.

Mobile Devices

iPhones/iPads: The proprietary software in these is a security liability. Also, the CIA disproportionately targets Apple devices. **Covering some Threat Models is better than being wide open.**

Android: For similar reasons, stock firmware is vulnerable. Especially Samsung, popular models.

Everyone: Your current device may not allow you to "free" it. Keep freedom in mind for your next device.

iOS users should focus on installing Signal, which is like a more-trustworthy version of WhatsApp.

Android Recommendations

- Install F-Droid. This is an app store with only free software.
- Add the Copperhead OS F-Droid repository in F-Droid and install Noise (Signal without the Google dependency).
- Add the Guardian Project repository in F-Droid. GP offers privacy apps like ObscuraCam.
- Try Orfox and OrWall for Tor browsing.
- Install Silence for encrypted SMS and MMS texts.
- Try Kontalk for a **decentralized** alternative to Signal/Noise.

Demonstration:

Hands-on with

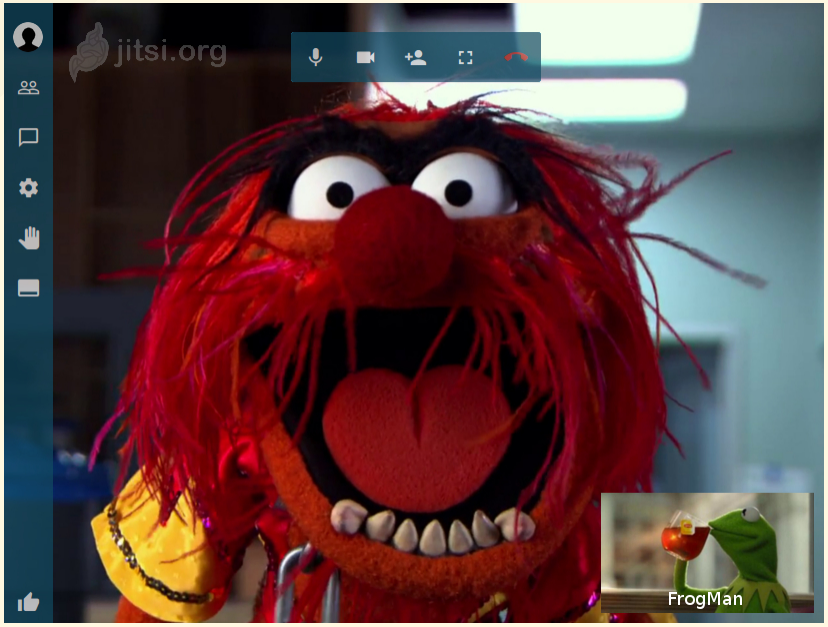
Jitsi Meet

Secure Audio/Video Chat

Let's name a new room at https://meet.jit.si

...this chat room will self-destruct when everyone leaves.

- Peer-to-Peer and End-to-End Encryption
- Password-protected rooms, no user limit, screen sharing
- Built-in Etherpad, text chat, optional YouTube streaming



Other WebRTC options: appear.in | Talky

Secure Comms Strategy

Make a plan and stick to it.

- The **What**: Choose a few crypto, sharing, & publishing tools.
- The **How**: Try these tools, figure out how they work.
- The **Where**: Find safe places to share secrets, on & offline.
- The **When**: Describe scenarios when you will use each tool.
- The **Why**: State clear reasons to use each tool.
- The **Who**: Identify "experts" who can help & teach others.

The Only Constant Is Change! Try new software, keep up on tech news & potential threats, and re-evaluate over time.

Resources

- Free Software Foundation: fsf.org
- Tor Project: torproject.org
- Electronic Frontier Foundation: eff.org
- Digital Security For Journalists

Cryptoparty | Riseup | Tactical Tech | PRISM Break

MayFirst | Encryption Works | Reset The Net

Digital First Aid | H-Node | DRM-Free

Digital Security Helpline: 24/7 multilingual support