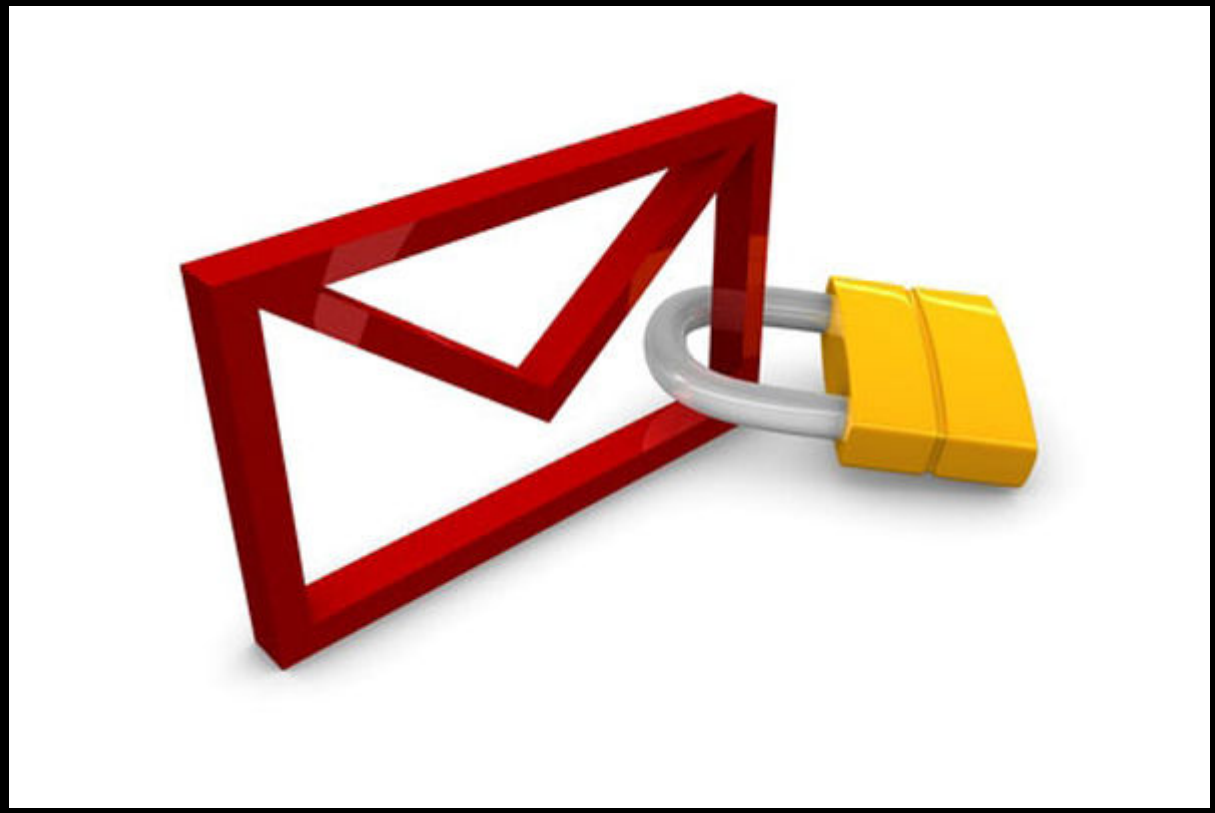
Encryption

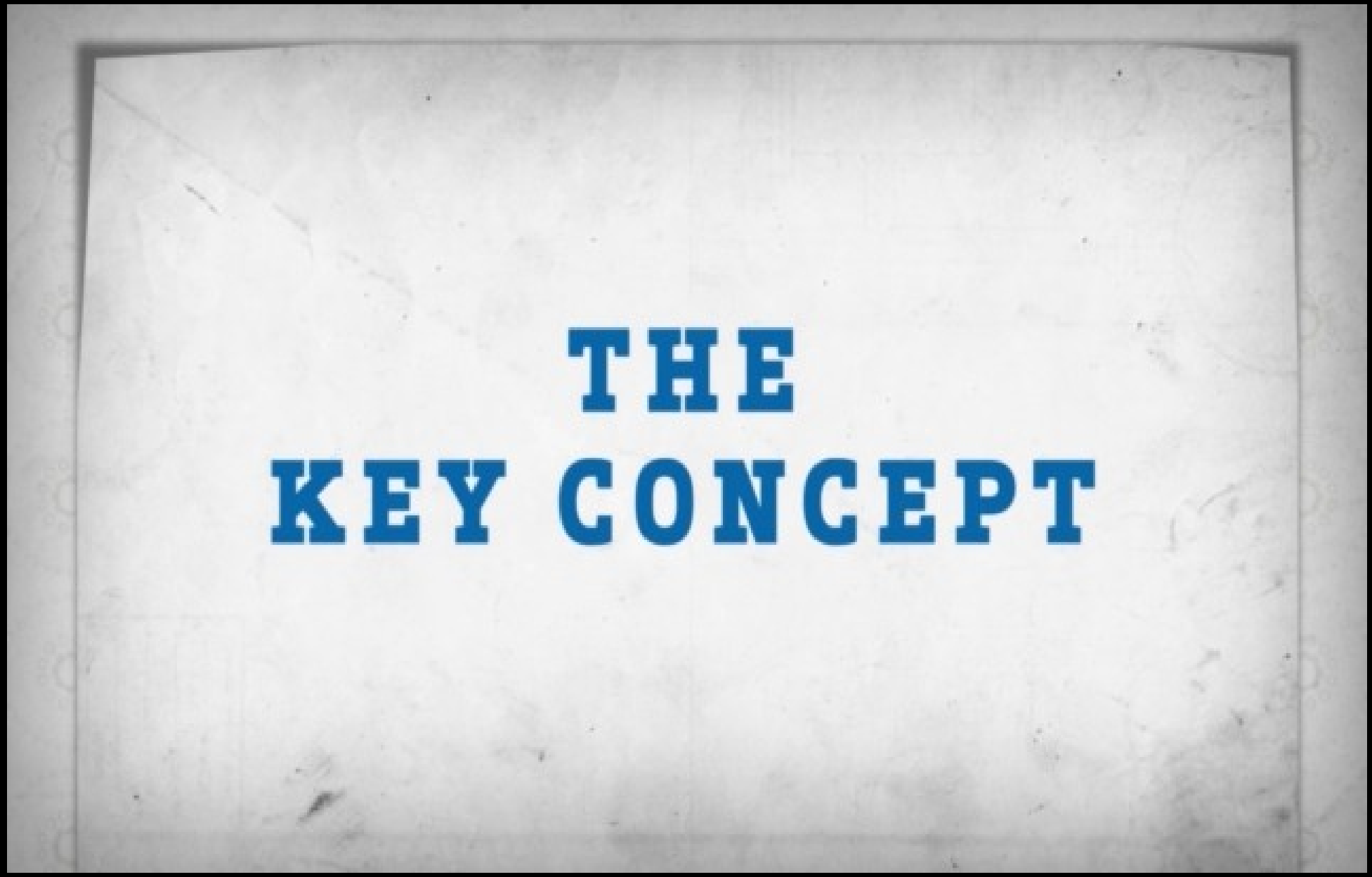
Sessions

- Email encryption
- File encryption
- Encrypting instant messages & VoIP calls

Session 1:
Email encryption



https://vimeo.com/134932244



Tools for email encryption

- **Thunderbird:** An open source email client for sending, receiving, and storing emails *without* a browser.
- **GNU Privacy Guard (GPG):** Open source software capable of **encrypting, decrypting, and digitally signing** messages and files.
- **Enigmail:** A Thunderbird add-on that allows you to use GPG for email encryption.

What can GPG do?

- **Encrypt** messages & files
- **Decrypt** messages & files
- **Digitally sign** messages & files
- **Manage keys**:
  - Create private & public keys
  - Manage a list of keys
  - Certify keys
  - Revoke or disable keys

CAUTION!

GPG does NOT hide who you are talking to, nor does it hide the fact that you are using GPG.

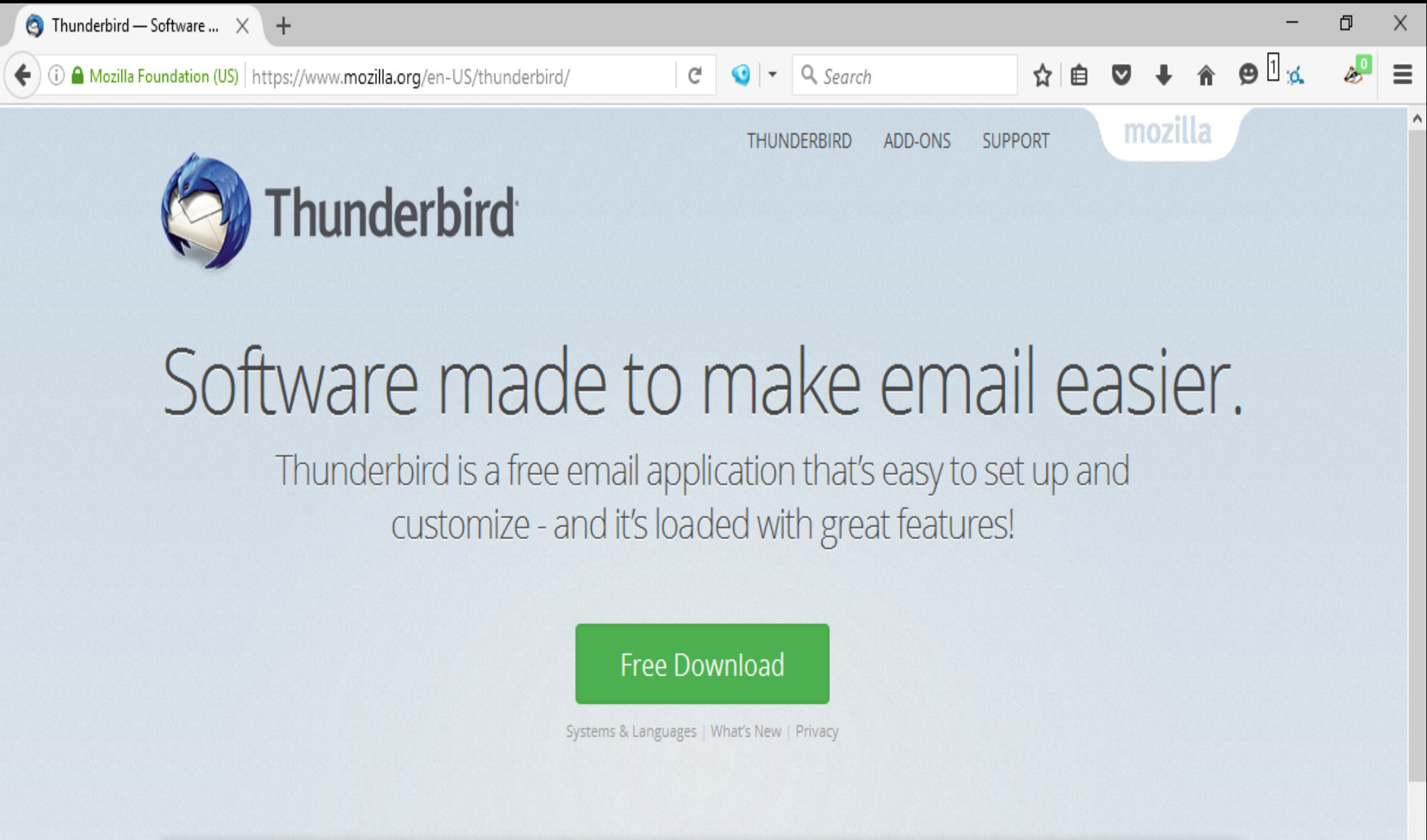
GPG keys

- **Private key:** A **passphrase** for **encrypting** and **decrypting** emails. This should be kept private!!!

- **Public key:** A string of numbers that can be made public (online), enabling others to send encrypted emails to you.

- Alice wants to send an email to Bob.
- She first acquires Bob's public key, so that she is able to send an encrypted email to him.
- She then uses her private key (passphrase) to **encrypt** her email to Bob's public key.
- Bob receives an encrypted email from Alice & uses his private key (passphrase) to **decrypt** it.

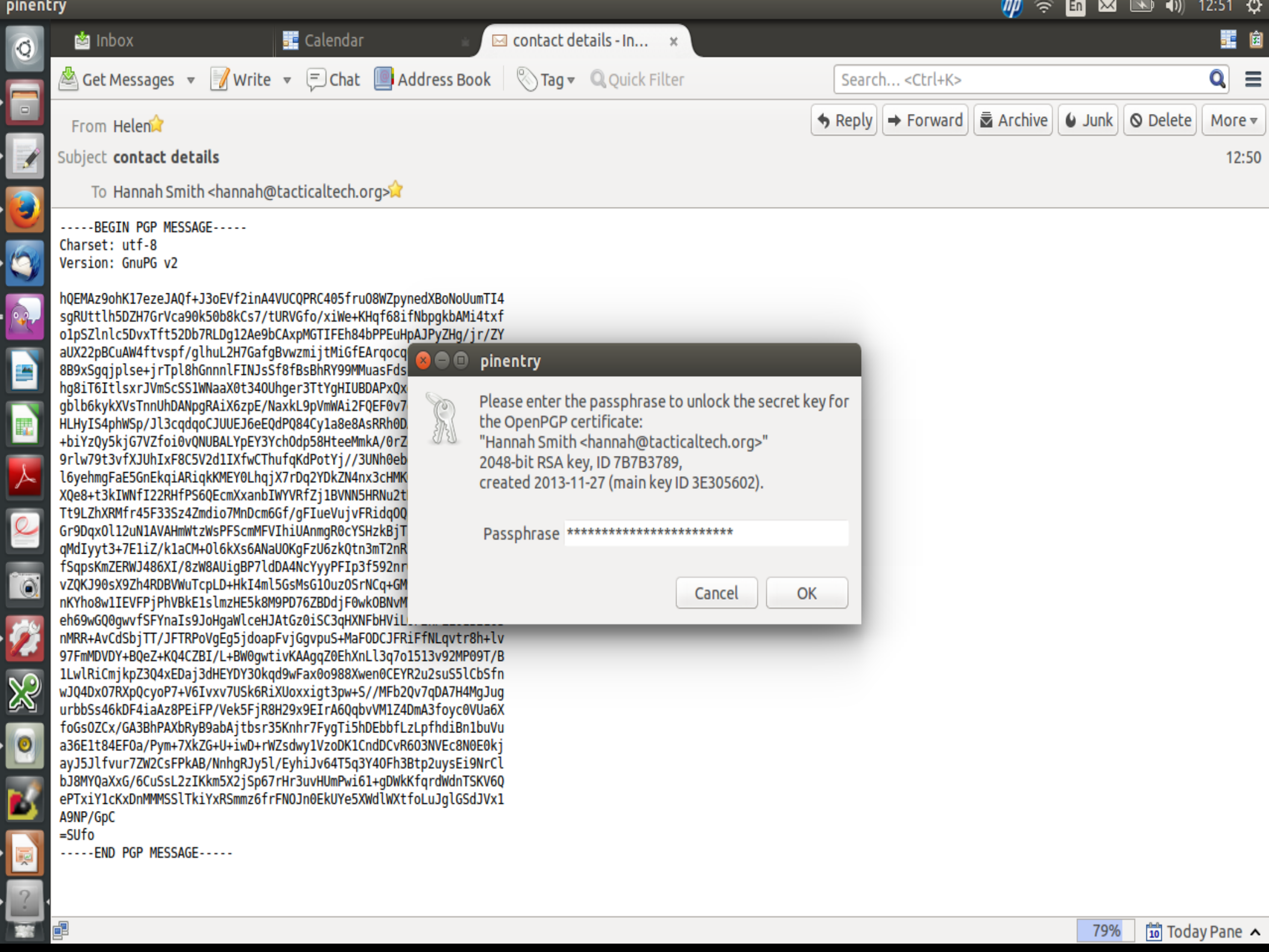
Install Thunderbird (and add an email account to it)



Install Gpg4win (Windows) or GPG Suite (macOS)

Enigmail

- **Install** Enigmail (via Thunderbird add-ons)
- Configure Enigmail to **generate GPG keys**
- Create a **Revocation Certificate**
- **Configure your email** to work with Enigmail (OpenPGP Security via Account Settings)


pinentry
12:51
Inbox
Calendar
contact details - In...
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Search... <Ctrl+K>
Reply
Forward
Archive
Junk
Delete
More
From Helen
Subject contact details
12:50
To Hannah Smith <hannah@tacticaltech.org>
-----BEGIN PGP MESSAGE-----
Charset: utf-8
Version: GnuPG v2
hQEMAz9ohK17ezeJAQf+J3oEVf2inA4VUCQPRC405fruO8WZpynedXBoNoUumTI4
sgRUttlh5DZH7GrVca90k50b8kCs7/tURVGfo/xiWe+KHqf68ifNbpgkbAMi4txf
o1pSZlnlc5DvxTft52Db7RLDg12Ae9bCAxpMGTIFEh84bPPEuHpAJPyZHg/jr/ZY
aUX22pBCuAW4ftvspf/glhuL2H7GafgBvwzmijtMiGfEArqocq
8B9xSgqjplse+jrTpl8hGnnnlFINJsSf8fBsBhRY99MMuasFds
hg8iT6ItlsxrJVmScSS1WNaaX0t34OUhger3TtYgHIUBDAPxQx
gblb6kykXVsTnnUhDANpgRAiX6zpE/NaxkL9pVmWAi2FQEF0v7
HLHyIS4phWSp/Jl3cqdqoCJUUEJ6eEQdPQ84Cy1a8e8AsRRh0D
+biYzQy5kjG7VZfoi0vQNUBALYpEY3YchOdp58HteeMmkA/0rZ
9rlw79t3vfXJUhIxF8C5V2d1IXfwCThufqKdPotYj//3UNh0eb
l6yehmgFaE5GnEkqiARiqkKMEY0LhqjX7rDq2YDkZN4nx3cHMK
XQe8+t3kIWNfI22RHfPS6QEcmXxanbIWYVRfZj1BVNN5HRNu2t
Tt9LZhXRMfr45F33Sz4Zmdio7MnDcm6Gf/gFIueVujvFRidqOQ
Gr9DqxOl12uN1AVAHmWtzWsPFScmMFVIhiUAnmgR0cYSHzkBjT
qMdIyyt3+7E1iZ/k1aCM+Ol6kXs6ANaUOKgFzU6zkQtn3mT2nR
fSqpsKmZERWJ486XI/8zW8AUigBP7ldDA4NcYyyPFIp3f592nr
vZQKJ90sX9Zh4RDBVWuTcpLD+HkI4ml5GsMsG1OuzOSrNCq+GM
nKYho8w1IEVFPjPhVBkE1slmzHE5k8M9PD76ZBDdjF0wkOBNvM
eh69wGQ0gwvfSFYnaIs9JoHgaWlceHJAtGz0iSC3qHXNFbHViL
nMRR+AvCdSbjTT/JFTRPoVgEg5jdoapFvjGgvpuS+MaFODCJFRiFfNLqvtr8h+lv
97FmMDVDY+BQeZ+KQ4CZBI/L+BW0gwtivKAAgqZ0EhXnLl3q7o1513v92MP09T/B
1LwlRiCmjkpZ3Q4xEDaj3dHEYDY3Okqd9wFax0o988Xwen0CEYR2u2suS5lCbSfn
wJQ4DxO7RXpQcyoP7+V6Ivxv7USk6RiXUoxxigt3pw+S//MFb2Qv7qDA7H4MgJug
urbbSs46kDF4iaAz8PEiFP/Vek5FjR8H29x9EIrA6QqbvVM1Z4DmA3foyc0VUa6X
foGsOZCx/GA3BhPAXbRyB9abAjtbsr35Knhr7FygTi5hDEbbfLzLpfhdiBn1buVu
a36E1t84EFOa/Pym+7XkZG+U+iwD+rWZsdwy1VzoDK1CndDCvR6O3NVEc8N0E0kj
ayJ5Jlfvur7ZW2CsFPkAB/NnhgRJy5l/EyhiJv64T5q3Y4OFh3Btp2uysEi9NrCl
bJ8MYQaXxG/6CuSsL2zIKkm5X2jSp67rHr3uvHUmPwi61+gDWkKfqrdWdnTSKV6Q
ePTxiY1cKxDnMMMSSlTkiYxRSmmz6frFNOJn0EkUYe5XWdlWXtfoLuJglGSdJVx1
A9NP/GpC
=SUfo
-----END PGP MESSAGE-----
pinentry
Please enter the passphrase to unlock the secret key for
the OpenPGP certificate:
"Hannah Smith <hannah@tacticaltech.org>"
2048-bit RSA key, ID 7B7B3789,
created 2013-11-27 (main key ID 3E305602).
Passphrase **********
Cancel
OK
79%
Today Pane

Resources

- Windows: https://securityinabox.org/en/guide/thunderbird/windows
- MacOS: https://securityinabox.org/en/guide/thunderbird/os-x
- Linux: https://securityinabox.org/en/guide/thunderbird/linux
- https://myshadow.org/resources/the-key-concept?locale=en

Session 2:
File encryption

Full disk encryption

- **Windows:** BitLocker (built-in software)
- **MacOS:** FileVault (built-in software)
- **Linux:** LUKS (upon installation of operating system)

VeraCrypt

- An electronic safe in which you can protect your files.
- Create encrypted “containers” (called “volumes”) to store your files.
- Create *hidden* volumes to hide the fact that you have certain files on your computer at all.

VeraCrypt volumes

- **Standard volume:** Protect your files with a passphrase that needs to be entered to access them.

- **Hidden volume:** Protect your *sensitive* files with two passphrases – the one opens the “outer volume”, and the other opens the “hidden volume”.

Install VeraCrypt

Resources

- Windows: https://securityinabox.org/en/guide/veracrypt/windows
- MacOS: https://securityinabox.org/en/guide/veracrypt/os-x
- Linux: https://securityinabox.org/en/guide/veracrypt/linux

Session 3:
Encrypting instant messages & VoIP calls

Off-the-Record (OTR): Protocol for encrypted IM

- **Encryption:** No one else can read your messages.
- **Authentication:** You are assured the correspondent is who you think it is.
- **Deniability:** No digital signatures that can be checked by third parties.
- **Perfect forward secrecy:** If you lose control of your private keys, no previous conversation is compromised.


OTR
RECORDS

Other User IP Addresses

[redacted]

Time (GMT)	From	To	Message
Mar 16, 2012 13:37:51	[redacted]		
Mar 16, 2012 13:37:59			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:08			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:12			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:24			[OC: No decrypt available for this OTR encrypted message.]
Mar 16, 2012 13:38:44	[redacted]		
Mar 16, 2012 13:38:57			
Mar 16, 2012 13:39:16			
Mar 16, 2012 13:39:23			
Mar 16, 2012 13:39:36			
Mar 16, 2012 13:39:53			

***

ZRTP:
Protocol for encrypted VoIP

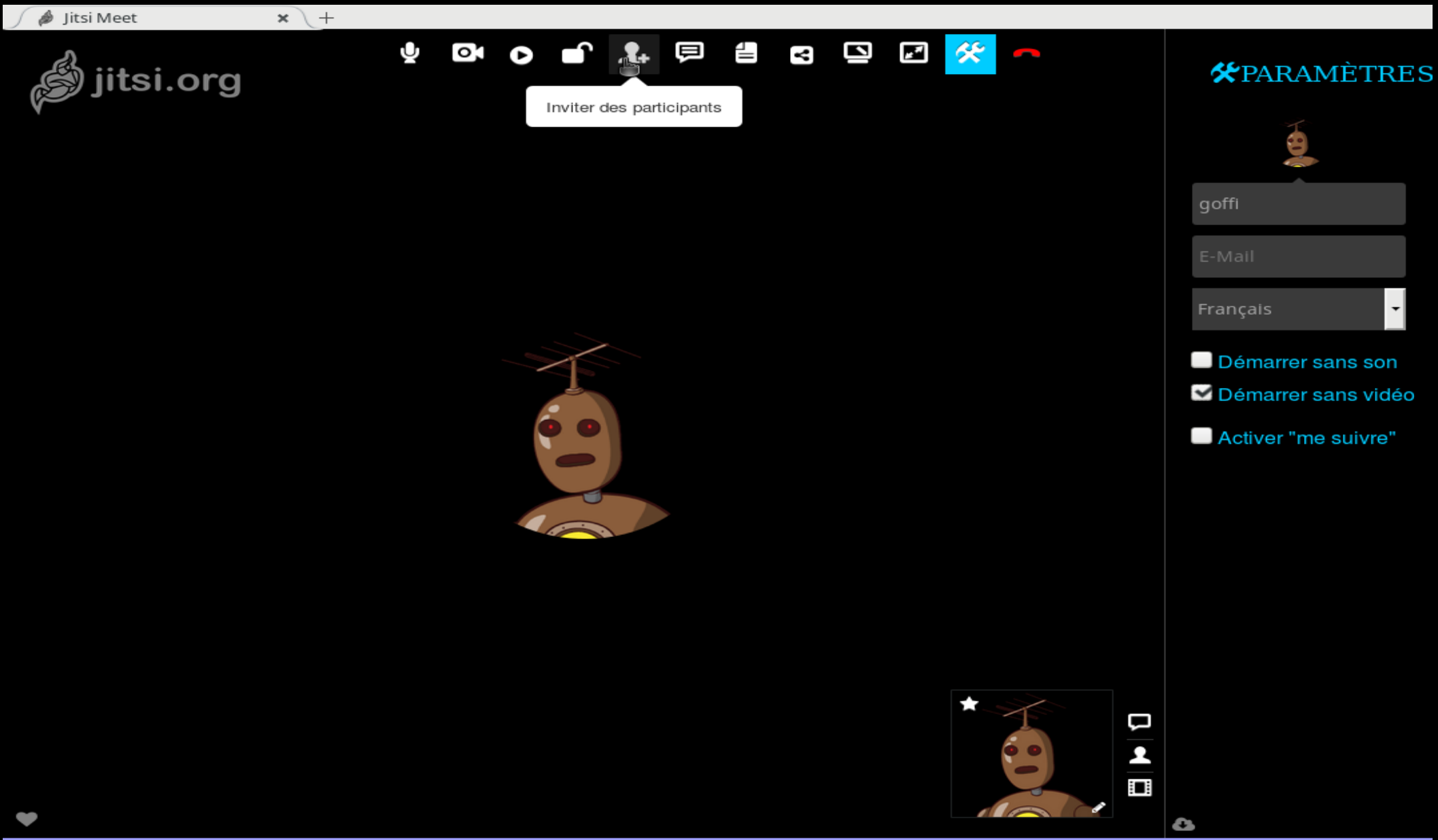
- Encryption
- Authentication (prevents man-in-the-middle attacks by requiring users to compare an authentication string)
- Perfect forward secrecy (the keys are destroyed at the end)


jitsi

Install Jitsi

Tor Messenger

Meet.jit.si


Jitsi Meet
jitsi.org
Inviter des participants
PARAMÈTRES
goffi
E-Mail
Français
Démarrer sans son
Démarrer sans vidéo
Activer "me suivre"
https://meet.jit.si/test [-]
[1/1]Top

Signal

Resources

- Windows: https://securityinabox.org/en/guide/jitsi/windows
- MacOS: https://securityinabox.org/en/guide/jitsi/os-x
- Linux: https://securityinabox.org/en/guide/jitsi/linux
- Signal: https://securityinabox.org/en/guide/signal/android
- https://meet.jit.si/
- https://blog.torproject.org/blog/tor-messenger-beta-chat-over-tor-easily