

Secure email with OpenPGP

9/20/14

Noelani Kamelamela

Why encrypt emails?

- Privacy is a right
- Don't expect it, but protect it
- Keep your private business private

OpenPGP: GnuPG, Mailvelope, etc...

- Use public key cryptography
- These solutions are free

GnuPG/Mailvelope download details

GnuPG (G/Hot/Yahoo!mail)

Mac

<https://gpgtools.org>

Windows

<http://gpg4win.org>

Linux

possibly pre-loaded, can install
with package manager

**Mailvelope (G/Yahoo! mail,
Outlook, GMX)**

Firefox

[https://github.
com/toberndo/mailvelope/releases](https://github.com/toberndo/mailvelope/releases)

Chrome

[https://chrome.google.
com/webstore](https://chrome.google.com/webstore)

search for “Mailvelope”

Public key encryption

User generates a keypair: one public, one private

- A message can be encrypted with the public key and decrypted with the private key to provide security
- A message can be encrypted with the private key and decrypted with the public key to provide signatures

Common work on all platforms

- Generate a keypair (remember password)
- Configure mail program to receive/send encrypted email
- Send an encrypted email
- Ideally, we have a keysigning party in 5 minutes!

GnuPG: keypair

- Generate a key

```
gpg --gen-key
```

Choose RSA, RSA. Use the longest key possible. Remember your passphrase!

- Upload key to keyserver

```
gpg --send-key KEYID
```


- Download my public key

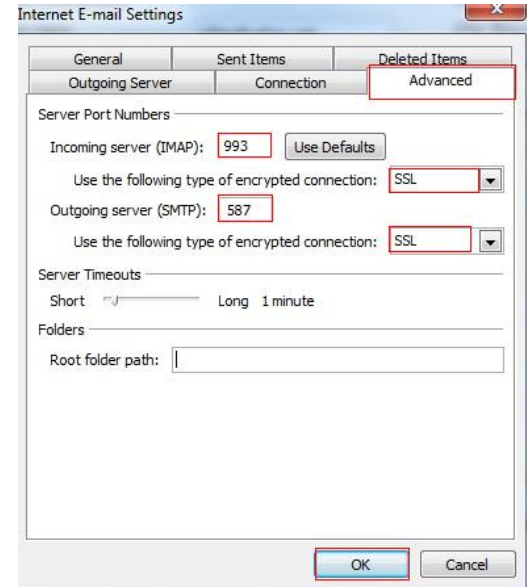
```
gpg --recv-key 358758A8
```

KEYID ← last eight characters of a key fingerprint

```
gpg --fingerprint KEYID ← gpg --fingerprint jdoe@example
```

GnuPG: G/Hot/Yahoo!mail Configs

- Must enable IMAP or POP first in web interface
- Gmail 
 - Send: smtp.gmail.com, port 587, use SSL
 - Receive: imap.gmail.com, port 993, use SSL; OR pop.gmail.com, port 995, use SSL
- Yahoo
 - Send: smtp.mail.yahoo.com, port 587, use SSL
 - Receive: pop.mail.yahoo.com, port 995, use SSL; OR imap.mail.yahoo.com, port 993, use SSL
- Hotmail
 - Send: smtp-mail.outlook.com, port 587, use TLS
 - Receive: imap-mail.outlook.com, Port 993, use SSL; OR pop-mail.outlook.com, port 995, SSL



GnuPG: How to send


```
gpg -ea -r "recipient" -o -filename | mail s "subject" recipient@example.com
```

Graphical User Interfaces vary: closed lock signals encryption or “to encrypt” and open lock means decrypted or “to decrypt”

Make the file and then encrypt, must have the public key of recipient for simple encryption, the recipient must have your public key for signing to work

Mailvelopers get ready

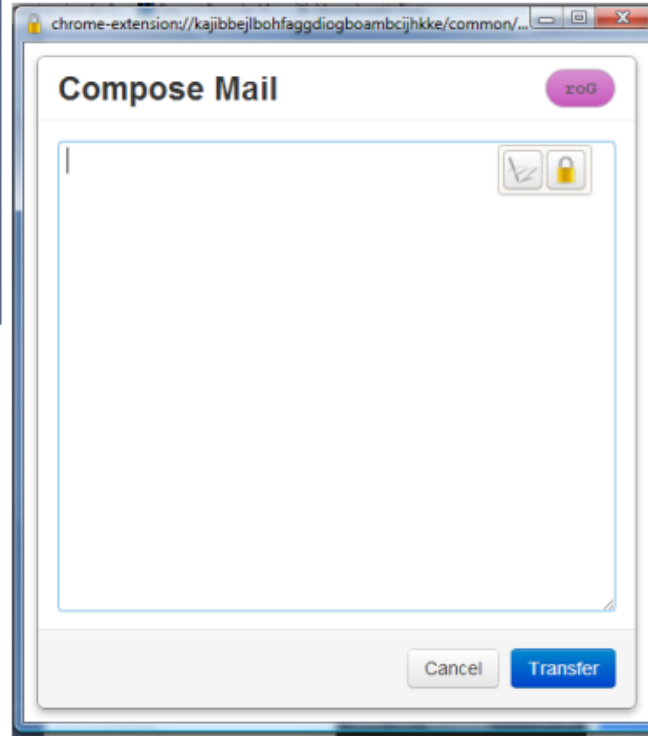
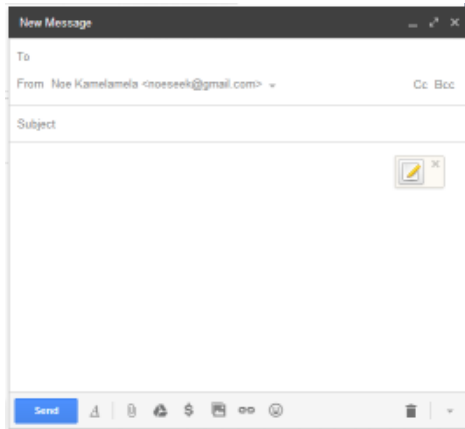
Mailvelope: generate keypair

- Click on Mailvelope's lock icon 
- Select "Options"
- Under "Key Ring" select "Generate Key"
- Click on "Advanced >>" to set Algorithm (RSA/RSA), Key Size (longest) and Expiration Date
- Must enter Name, Email and Passphrase

Mailvelope: set-up?

- No need to configure for Gmail, Yahoo, Outlook or GMX
- Caveats
 - Only a browser extension for Firefox or Chrome
 - Cannot currently revoke keys

Mailvelope: How to send



1. Make New Message
2. Click on icon
3. Write email in pop-up
4. Encrypt by clicking Lock symbol and using settings
 - a. must have public key of receiver
 - b. use your public key to sign
5. Transfer encrypted message back to New Message (can also copy and paste)

Send and receive

- Send me an encrypted message
 - Find and Import my public key
 - pgp.mit.edu-->Search String: “noeseek@gmail.com”
 - KEYID=1C434302
- Open Sent Mail folder, make sure you can read the email you sent
- I will reply, you should be able to download and decrypt my message

Key safety

- Back up your private key
 - Export private key to safe place
- Revoke unsafe private keys
 - GnuPG: generate revocation certificate and then upload certificate to a keyserver
 - `gpg -a --gen-revoke KEYID > pgp-revoke.asc`

Keyserver

pgp.mit.edu

<http://pool.sks-keyserver.net/>

PGP resources

- GnuPG: <http://gnupg.org>
- gpg4win: <http://www.gpg4win.org>
- Mailvelope: <https://www.mailvelope.com>
- Cryptoparty handbook: <https://www.cryptoparty.in/documentation/handbook>

Additional Questions

Multiple emails on one keypair:

Add user ID

Mailvelope does not support multiple user IDs

Mailvelope keyring on another computer:

Export all of your keys into a file

Import the file into your other computer's
keyring