PLEASE COMMENT ON THE DOCUMENT TO MAKE IT BETTER.
WE WILL BE MOVING DIGITALLY SIGNED VERSIONS TO GITHUB & MEDIUM.
PLEASE NOTE THAT COMMENTS MAY BE VISIBLE TO ANYONE WHO READS THE DOCUMENT.
PROTIP: You can view this link from a logged out google account for some anonymity & comment as an “Anonymous” animal.

(TBD: table of contents)
(TBD: table of contents by need/concern)

Written originally
in: english.
This is the
translation to:
english.

information
expires/ best by:
August 19th, 2018

FIRST THINGS FIRST!

Watch this 8 minute video! It is worth the short investment of 8 minutes before you move on.

THE INTERNET

ENCRYPTION & PUBLIC KEYS

[**THE INTERNET: Public Keys & Encryption https://www.youtube.com/watch?v=ZghMPWGXexs**](https://www.youtube.com/watch?v=ZghMPWGXexs)

Watch this 1 minute video! It's worth the short investment of 1 minute, promise

INTERNET SECURITY

PGP

PGP: Pretty Good Privacy
https://vimeo.com/184962576

<u>Password: (password hint, it’s all lower case, it’s three letters, & it’s the same as the three letters above the play logo above), pgp</u>

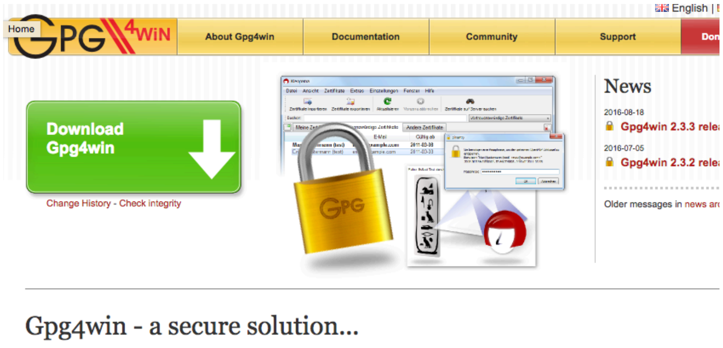
EDITORS NOTE: Email encryption is not a magic bullet. Email encryption is not a ‘get out of jail free’ card. It is however simply math, NOT centralized, nor run by no one person or company. It is the best we have. Encryption doesn’t “save you”, but it does buy you time. Days, weeks, months, years, decades, centuries. It is still a great idea to be careful what you send via email. If you need to send a message because someone is too far away to whisper into their ear, we recommend encrypted mobile messaging apps. Still email isn’t going anywhere. Current events teach us it is a matter of WHEN not IF your email or your organization’s email gets breached, read, & dumped.

SELF CARE NOTE: It takes the average person a little over an hour to complete these steps. Give yourself the time you need. Take a break, hydrate, and return to things if you need. Once you learn the steps try to teach someone else along with this guide. It is the best way to cement your learning. Be patient. You got this!

YOUR COMPUTER DOESN'T COME WITH WHAT YOU NEED TO ENCRYPT EMAIL. YOU WILL NEED TO… <u>DOWNLOAD THIS FIRST!</u>

Download the GPG binary and wrapper for your system:

ON A PC:



News

2016-08-18
Gpg4win 2.3.3 rele

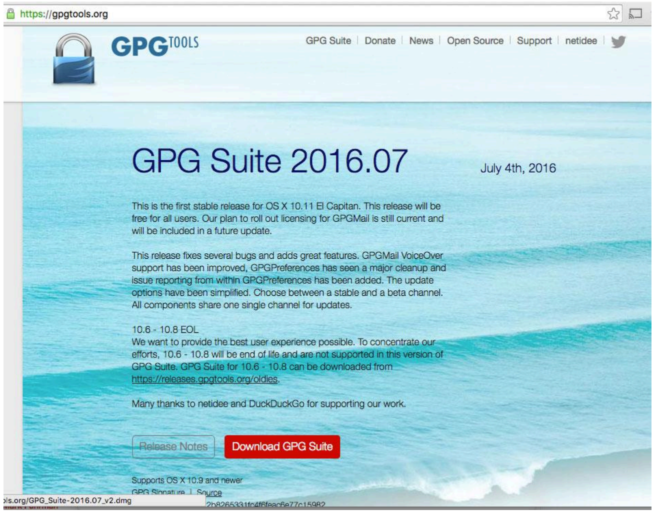
2016-07-05
Gpg4win 2.3.2 rele

Older messages in news arc

Gpg4win - a secure solution...

Download the largest GPG4WIN, it should be 26MB approximate size. Get it here: https://www.gpg4win.org/download.html

ON A MAC:


https://gpgtools.org
GPG TOOLS
GPG Suite | Donate | News | Open Source | Support | netidee |
Release Notes
Download GPG Suite
ols.org/GPG_Suite-2016.07_v2.dmg

GPG Suite 2016.07

July 4th, 2016

This is the first stable release for OS X 10.11 El Capitan. This release will be free for all users. Our plan to roll out licensing for GPGMail is still current and will be included in a future update.

This release fixes several bugs and adds great features. GPGMail VoiceOver support has been improved, GPGPreferences has seen a major cleanup and issue reporting from within GPGPreferences has been added. The update options have been simplified. Choose between a stable and a beta channel. All components share one single channel for updates.

10.6 - 10.8 EOL
We want to provide the best user experience possible. To concentrate our efforts, 10.6 - 10.8 will be end of life and are not supported in this version of GPG Suite. GPG Suite for 10.6 - 10.8 can be downloaded from https://releases.gpgtools.org/oldies.

Many thanks to netidee and DuckDuckGo for supporting our work.

Supports OS X 10.9 and newer
GPG Signature | Source
2b8265331fc4f6feac6e77c15982

Download the latest GPGTOOLS from here: https://gpgtools.org/

Optional steps in gray: VERIFYING THE DOWNLOADS (recommended for activists, dissidents, & journalists)

All security apps have a method to prove the file is what you think it is and has not been tampered with. GPG has a .sig file you can view on their website. If you want to verify the download you can:

ON A PC (this step is OPTIONAL):

1. *Download File Checksum Validator https://www.microsoft.com/en-us/download/details.aspx?id=11533*
2. Go to: Start > All apps > Windows System > Command Prompt
3. *Install this program, When asked put the application in your Downloads folder .*
4. *If the file you downloaded from http://gpg4win.org was called* ***gpg4win-231.exe*** *you would type (this is one line, there is a space after "exe" and*

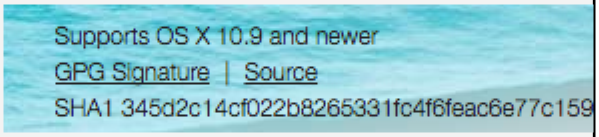
after "-sha1"). Depending on the version you might need to change the end of the command a bit from 2.3.1 to something else:

```
fciv.exe -sha1
~/Downloads/gpg4win-2.3.1.exe
```

On A MAC (this step is OPTIONAL):

1. Use spotlight (command key + spacebar) and type: **TERMINAL**
   (*Then press the ENTER key*)
2. Once you press enter a little box appears. type: **cd ~/Downloads**
   (*There is a space after the "cd" , the squiggle thing is in the upper left corner, then press ENTER! :))*
3. *Start typing but don't hit return yet:* ***openssl sha1 GPG_***
4. ***Then press the TAB key twice****, it should enter the rest of the filename for you.*
5. ***Then hit enter.***
6. *Assuming the file you downloaded is called GPG_Suite-2016.07.dmg you should have something that looks like*
   (make sure it ends in .dmg):

   ```
   openssl sha1 GPG_Suite-2015.09.dmg
   ```
7. *Press* ***ENTER***
8. *Compare what is displayed from the command you typed with what is on the website http://gpgtools.org for the version of GPG you downloaded.*



Supports OS X 10.9 and newer
GPG Signature | Source
SHA1 345d2c14cf022b8265331fc4f6feac6e77c159

It should be an exact match. ***WE ARE VERIFYING THE KEY,*** **PROVING THIS IS THE** **<u>REAL</u>*!***
We do this because it IS possible for someone to control the network you are on and point you to a fake version of GPG (basically it has a hole in it). But even the smallest change to the file will give it a TOTALLY DIFFERENT list of characters in SHA1. Because someone could also be showing you a mock up of the actual website its a good idea to ask in a public forum (like twitter) if the SHA1 for the version of the software you downloaded is what you are expecting it to be.

Close TERMINAL *(MAC)or* ***Command Prompt*** *(WIN) when you are done.*

GETTING SET UP!

ON A PC: Install **GPG4WIN,**
Be sure to check the "GPA" & "KLEOPATRA" option during installation.

ON A MAC: Install **GPG Suite from your Downloads folder**
(*by double clicking on it then clicking INSTALL)*
Follow the steps. Continue-> Install -> (enter your password) -> Close
(for MAC & PC just go with the default settings the installer shows you.

ON A CHROMEBOOK: install this extension MAILVELOPE (https://www.mailvelope.com/)
1. Click on this link https://chrome.google.com/webstore/detail/mailvelope/kajibbejlbohfaggdiogboambcijhkke
2. Click ADD TO CHROME button then ADD EXTENSION to add this extension to chrome.

IF YOU HAVE A MAC, PC, OR LINUX MACHINE WE DO NOT RECOMMEND MAILVELOPE OVER WHATS AVAILABLE. MAILVELOPE has the ability to accidentally lose your private key & public keys, if you clear all data from your browser. Also Mailvelope does not have a good way to encrypt files or decrypt files, which makes handling encrypted attachments very difficult & problematic for you.

F

MAKE YOUR KEY!

We are going to make a new key with the highest level RSA encryption length of 4096 (bits or higher).

ON A PC (**skip over this part if you are on a mac **):

1. WINDOWS icon-> All Apps -> GPG4WIN-> Kleopatra. In KLEOPATRA, choose FILE-> NEW CERTIFICATE. Then pick the "CREATE A PERSONAL OPENGPG KEYPAIR"
2. Choose ADVANCED SETTINGS....
3. under the TECHNICAL DETAILS tab where it says KEY MATERIAL, change the 2,048 bits default to 4,096 bits.
4. under the TECHNICAL DETAILS tab where it says CERTIFICATE USAGE check "VALID UNTIL" and set this to 2 years from today.
5. click OK

you can create your new key. name, comment, and email address. leave the comment field blank. write your name as others might search for it, It's ok to use your nickname. for email you will put the email address you expect to receive encrypted mail under, most people are fine putting your normal email address. Your most known/public email address is recommended. Others will need to find your public key and this will be the email they will be searching for. When you are done choose CREATE KEY. you may now be asked to move your mouse around or type some random keys to finish making your key.

Leave comment field blank and set expiration to 2 years (or less). When the time comes enter in the passphrase you came up with.
When your key is created. close KLEOPATRA.|

ON A MAC:

1. After you install GPGTOOLS the program automatically starts. If it doesn't go to

Applications and run GPGKEYCHAIN

2. If you have never had a GPG KEY before it automatically clicks NEW KEY for you. *(If you are making a key but had one before click KEY-> NEW*).
3. **Lets being by filling out the form:** Full name, and email address fields should be filled in. It’s ok to use your nickname. For email you will put the email address you expect to receive encrypted mail under, most people are fine putting your normal email address. Your most known/public email address is recommended. Others will need to find your public key and this will be the email they will search be searching for. Its totally ok if your email is owned by a megacorp like a gmail address :)
4. DO **NOT** CLICK upload public key (we will get to that step later once we verify you know your passphrase).
5. Click on Advanced Options…
6. Be a pro and leave **comments** blank, for **key type** RSA and RSA (default) is fine, for key length be sure 4096 is set, for expiration date change to two years from today.
7. For passphrase read the section below ** **MAKE A PASSPHRASE!** ** then
8. Enter a PASSPHRASE (from the paper you wrote it on with pen & pad)
9. Click on **Generate key‘**

ON A CHROMEBOOK:

1. Open CHROME browser
2. Click on the MAILVELOPE icon
3. Click OPTIONS (with the wrench icon)
4. Click GENERATE KEY
5. Enter a NAME and EMAIL (the email you most commonly use is fine)
6. Read the section below ** **MAKE A PASSPHRASE!** ** then
7. Enter a PASSPHRASE where it says enter password (from the paper you wrote it on with pen & pad)

MAKE A PASSPHRASE!:

Every time you sign or decrypt something you will be asked to enter a passphrase. It’s not a password, it’s a phrase so make it long but memorable. If your secret encryption key is compromised this phrase is all that stands between your encrypted info and an attacker. We recommend using at least a **7-10 WORD** long passphrase (replace spaces with a special character like a number, symbol, or dash). If you need help in coming up with a secure passphrase we also recommend diceware passphrases*. https://entima.net/diceware/ a good explainer on diceware is http://world.std.com/~reinhold/diceware.html. and to use a die (singular for dice) check out http://www.diceware.net)

We highly recommend if you use a song lyric or phrase from a published work that you change a key part of it. Because these passwords are often found online in archives of stolen passwords from data breaches. If you are curious if any of your passwords may be in a stolen password archive check out the site https://haveibeenpwned.com (a video about this phenomena https://www.youtube.com/watch?v=CiqRYwRl9EE)

Regardless of how you come up with a passphrase, never store it in anywhere electronic. WIth a pen and paper write down your passphrase somewhere secure, we will need it soon. Once you have entered this passphrase about 22-100 times you can celebrate. Destroy (burn) the paper and celebrate. You can change your passphrase later but only if you know it. You can never request your passphrase if you forget it.

Every time you want to decrypt or digitally sign a message you will be entering this passphrase. So make it good. This is the hardest part of encrypted email, picking a good passphrase. You can change your passphrase to something else at any time, AS LONG AS YOU HAVE THE CURRENT ONE !!!

Once you come up with a great passphrase you wrote it down to a piece of paper. **FROM THE PAPER** you wrote it down on (this rules out any errorr) enter the passphrase you came up with into your GPG program, letter by letter. From your paper into that form.

CREATE A WAY TO "DELETE" (REVOKE) YOUR KEY

There is no way to delete your public key from the keyservers we will be sending it to. However there is a way to stamp your key as revoked. This basically tells others not to use it. This can be because your key is fake, compromised, or simply because you forgot the passphrase to it. In order to revoke your key you just need its certificate. Let's make that now so you can use it in the future if something happens to your key. Its just a file that you save, somewhere (on your computer) or even better onto a USB you store securely. You also will get some practice typing in your passphrase.

ON A PC:

1. *Open the Kleopatra app*
2. *Highlight your public key from the main window of Kleopatra*
3. *Choose Certificate from the toolbar*
4. *You will be given an option to create backup*

On A MAC:

1. Open the GPGkeychain app
2. Highlight your public key from the main window in GPGkeychain
3. Choose Key from the toolbar
4. Choose Generate Revocation Certificate…

Its a good idea to keep a copy of your certificate on this machine & another on a usb you store somewhere safe. This way if the machine is broken, lost, or stolen - you can still revoke your key. Revoking a key happens automatically when a key reaches its expiration date. At that time make a new one.

SOME IMPORTANT CHANGES TO YOUR SYSTEM!

Adding some cool services: allowing you to encrypt, decrypt, and sign messages & files by right clicking on them & picking the option from services.

ON A MAC *lets make GPG part of your Services:*

1. To make encrypting and decrypting part of your mac:
2. On your screen, click on the in the upper left corner.
3. go to **System preferences**->
4. Choose **keyboard**-> In the middle choose

shortcuts-> look for the column that says **Services**

5. **In the larger white box that appears. Put a check mark** in all the options that begin with "**OpenPGP:"** (there will be some on top the list that are automatically checked to begin with, **scroll further down** to see some that need to be checked. Look for the one called "OpenPGP: DECRYPT" to make sure it's checked).
6. When you are done you can close this window.

Changing the way textedit behaves:

preventing it from autosaving your message before you encrypt it and stuff like that.

ON A MAC *lets make textedit behave more like an encryption workspace/clipboard:*

- ***Press*** the **command** key + ***space*** bar and then type **TERMINAL** (this program allows us to hack OSX a bit), **press ENTER.**
- A box will appear with a cursor in it. This is TERMINAL, a way to access your mac's inner workings & system.
- **We will feed some lines into terminal. Commanding it to do one thing or another. These "commands" are moved or "run" when you press Enter. Run these terminal commands** to make sure (textedit never autosaves, that textedit uses a formatting called utf-8, and that textedit always uses plain text mode).
- **note:**The commands are programming messages to terminal. You are "commanding" it in what to do. All the commands begin with the word "defaults" and should be entered exactly as you see below (in italics). For each one just copy and paste it in, then hit enter. Nothing will appear to happen. When you get to the last option it will actually ask for a password. It wants the password you enter to get into your mac. You wont' see
- that it's registering your keystrokes but it is (that's a little TERMINAL security trick ;))

  HEY, ARE YOU USING THE DIGITAL
  VERSION OF THIS MANUAL? SWEET!
  WE RECOMMEND THAT YOU COPY AND
  PASTE THESE COMMANDS IN !

1. ***Turn off autosave in text edit with this***

terminal command (copy and paste this line below into TERMINAL then press enter):

```
defaults write com.apple.TextEdit
ApplePersistence -bool no defaults
write com.apple.TextEdit
ApplePersistence -bool no
```

2. ***Turn off autosave another way to be sure.***

   ```
   defaults write -app 'textedit'
   ApplePersistence -bool no
   ```

3. ***Turn off autosave after a certain time delay***

   ```
   defaults write -app textedit
   AutosavingDelay -int 0
   ```

4. Let's force ***Textedit to use plain text mode for new TextEdit documents (copy and paste this line below into TERMINAL then press enter):***

   ```
   defaults write com.apple.TextEdit
   RichText -int 0
   ```

5. ***Let's force Textedit to Open and save files as UTF-8 in TextEdit (copy and paste this line below into TERMINAL then press enter):***

   ```
   defaults write com.apple.TextEdit
   PlainTextEncoding -int 4
   ```

6. ***Let's force Textedit to use plain text encoding (copy and paste this line below into TERMINAL then press enter):***

   ```
   defaults write com.apple.TextEdit
   PlainTextEncodingForWrite -int 4
   ```

7. ***THIS ONE IS A LITTLE DIFFERENT -> Let's prevent revisions of TextEdit docs. (copy and paste this line below into TERMINAL then press enter)***
   This last command will ask for your password. It's the same one you use to login to your mac. You will not see the cursor move when you use it.This

command below is one line.

```
sudo mv
/.DocumentRevisions-V100/db-V1
/.DocumentRevisions-V100/db-V1_off
; sudo touch
/.DocumentRevisions-V100/db-V1;
sudo killall revisiond
```

Remember the cursor will not move as you enter the password that you use to get into you MAC (then press enter)

8. **GREAT**!!! IF I WASN'T A GPG step by step manual, I would give you a high five!!! You can now **close** the **Terminal** app

To make sure everything works let's open TEXTEDIT !

1. Press command + space and type: **TEXTEDIT**
2. **Then press enter**
   2a. **If you get a bouncing Textedit icon in your dock then it goes away something is wrong**
   2b**. If the Textedit program opens pat yourself on the back then exit textedit. Everything is working correctly.**

IMPORTANT! IF TEXT EDIT CLOSES SOON AS YOU OPEN IT...
then one of the commands above was typed in incorrectly. Start over again from the top. "Changing The Way Textedit Behaves" just copy paste directly from this

<u>YOUR VERY FIRST ENCRYPTED MESSAGE:</u>

ON A PC (skip over this part if you are on a mac **)**

1. in **GPA** app **click CLIPBOARD** icon in the upper right
2. **Type some text** in the clipboard window.
3. **click on ENCRYPT** (envelope icon)
4. click on your username
5. click OK.
6. Copy & paste this encrypted text to whatever comms program (gmail, twitter dm, facebook

msg, etc.). We recommend sending a message for you to yourself using your webmail or other account.

ON A MAC

1. Open TextEdit (press command + spacebar and type TEXTEDIT into spotlight)
2. A white box should show up for you to type into.
   If you don’t see a white box to type into, go to the upper right corner of the **TEXTEDIT** window and click on **FILE --> New**
3. **Write some text** (whatever you want!) to Text Edit.
4. **Select all** of the text you wrote.
5. **Right click** (or CTRL+click) on what you typed.
6. choose **Services**: **OPENPGP: ENCRYPT SELECTION** *(or just use the shortcut SHIFT+COMMAND+E)*
   4b. If you dont see that try OPENPGP: ENCRYPT
7. A GPGTools box pops up. The “**CHOOSE RECIPIENTS”** modal that pops up, check then uncheck the “select all” checkbox, to make sure nothing is autochecked from previous use. Once you have a lot of keys in here, this will keep you from encrypted message to the wrong person or people.
8. **Choose who this message is for by clicking on the box next to their name** (this is whose public keys to encrypt w/) When you start you only have your own public key and that of the GPGTools team. **Check the box next to your name**.
9. **Choose** which of **your public keys** to use under “your key” (if you only have one public key it will always be the default)
10. **Click Sign** to digitally sign the message. (This is recommended, but there are times for plausible deniability you might not want to)
11. **NEVER EVER EVER EVER** click “Encrypt with passcode” (it will cause confusion and some people wont be able to open their messages)
12. **Click OK**..
13. In the GPGTools a modal will pop up for you to enter your passphrase. **REMEMBER: DO NOT SAVE IN YOUR KEYCHAIN**

Voila. done! CONGRATULATIONS! Your message is encrypted.

ON A PC AND ON A MAC

LETS RUN A SIMULATION!!!! SEND YOURSELF A MESSAGE WITH THIS CYPHERTEXT

1. copy & paste this encrypted message, including --- BEGIN PGP --- all the way and including --- END PGP ---
2. To whatever communication program (gmail, twitter dm, facebook msg, etc.).
3. I recommend sending a message from you , to yourself using your webmail or other account.
4. QUIT QUIT QUIT!
   MAC people, if you do use this textedit based workflow be sure to CLOSE TEXTEDIT **DO NOT SAVE!** often. it has a undo feature that will show encrypted text as its original plaintext. encrypt a message, then click undo, to see what i mean.

DECRYPTING YOUR MESSAGE!

ON A MAC

1. **Copy the encrypted text**, from an email, facebook msgs, twitter DM, etc. Include the entire thing beginning with: "-----BEGIN PGP MESSAGE----- and ending with -----END PGP MESSAGE-----"
2. Open TextEdit (press command + spacebar and type TEXTEDIT into spotlight)
3. **Paste that encrypted text that you emailed yourself,** to Text Edit, select all, **right click** or (CTRL+click) on it
4. choose **Services**: **OPENPGP DECRYPT SELECTION** *(or just use the shortcut SHIFT+COMMAND+D)*
   4b. If you dont see that try OPENPGP: DECRYPT
5. In the GPGTools a modal will pop up for you to enter your passphrase. **REMEMBER: DO NOT SAVE IN YOUR KEYCHAIN**
6. **Click OK**.
7. COOL! YOU DID IT!!!

ON A PC (skip over this part if you are on a mac **):**

1. **Copy the encrypted text**, from an email, facebook msgs, twitter DM, etc. Include the entire thing beginning with: “-----BEGIN PGP MESSAGE----- and ending with -----END PGP MESSAGE-----”
2. In **GPA** app **click CLIPBOARD** icon in the upper right
3. **Paste your encrypted text** in the clipboard window.
4. **click on DECRYPT**
5.

Voila. done! CONGRATULATIONS! Your message is decrypted so you can read it!!!

GETTING AN ERROR WHEN YOU TRY TO DECRYPT?

1. Try removing that entire line that has the comment on it (if you see one) Its not important and just tells you how they encrypted message was made or delivered.
2. Make sure your key is the one the message is encrypted for. Send a copy of your public key or a link to your key on a keyserver to the sender and ask them to try again.

IF YOU WANT TO RECEIVE A MESSAGE FROM SOMEONE THEY NEED YOUR PUBLIC KEY. THE EASIEST WAY TO PROVIDE THIS IS TO LEAVE A COPY ON A PUBLIC KEY SERVER.

UPLOADING YOUR KEY TO A KEY SERVER:

At this point you can create encrypted text for yourself but what about if someone wants to send you an encrypted message? They will need your public key! There are a few ways to get it to them but the easiest

by far is to post your public key on a key server for others to find it.
Here is how to do that.

IMPORTANT: Using a simple keyserver.

For the purpose of this class/demo **we will use a simple keyserver: hkp://pgp.mit.edu.**
Your program starts out using an hkps:// keyserver like hkps://hkps.pool.sks-keyservers.net

WE ARE USING PGP.MIT.EDU TEMPORARILY. WHEN YOU ARE TOTALLY DONE WITH THIS MANUAL, BE SURE TO SWITCH BACK TO AN HKPS:// (note the "s") keyserver. This is the hkps:// keyserver you should switch back to, when you are done with this manual.:
hkps://hkps.pool.sks-keyservers.net

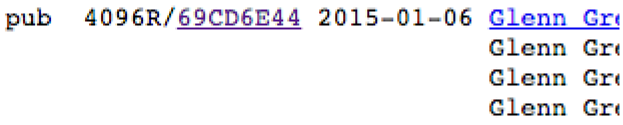
ON A MAC:
Lets make sure you are running our gpg keychain program.

1. Run spotlight by **click**ing on the ***COMMAND*** KEY + ***SPACE*** BAR and type: **GPG KEYCHAIN**
2. In the upper left on the tool bar, under **GPG KEYCHAIN**->**preferences->Key Server.** By default it uses a secure keyserver like: hkps://hkps.pool.sks-keyservers.net (for demos & teaching we will use "pgp.mit.edu" because its a cleaner page layout for searching, etc, be sure to switch back once you are done).
3. **Choose:** hkp://pgp.mit.edu from the dropdown menu
4. DO NOT show revoked and expired keys.
5. You can **CLOSE** preferences now. :)

ON A PC (**skip over this part if you are on a mac **):
in GPA Edit->Preferences->Check "Show advanced options" under Default key server: type the following: hkp://pgp.mit.edu

ON A MAC

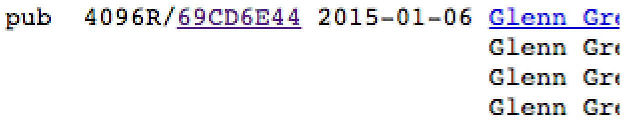
1. **Open you web browser and go to this website: https://pgp.mit.edu**
2. On the website is a box that says “Search String”. Search for your key by typing in your email address. (if you never had a key before, no results should be found).
3. **In GPG KEYCHAIN,** select your name from the list of keys on your system. It is highlighted blue.
4. Way up top in the toolbar select **KEY** -> **Send Public Key to Key Server**
5. There is no UNDO when it comes to sending stuff to Key Servers so the program ask if its ok, **click OK**
6. **Go to https://pgp.mit.edu**
7. In the field search for your key by entering your email address. THERE YOU ARE!



```
pub  4096R/69CD6E44 2015-01-06 Glenn Gr
                               Glenn Gr
                               Glenn Gr
                               Glenn Gr
```

ON A PC (**skip over this part if you are on a mac **)

1. **Open you web browser and go to this website: https://pgp.mit.edu**
2. On the website is a box that says “Search String”. Search for your key by typing in your email address. (no results should be found).
3. **In GPA,** select **WINDOWS -> KEYRING MANAGER**
4. Find your name & email from the list of keys on your system. It is highlighted.
5. Way up top in the toolbar select **SERVER** -> **Send Keys**
6. **click OK**
7. **Go to https://pgp.mit.edu**
8. In the field search for your key by entering your email address. THERE YOU ARE!



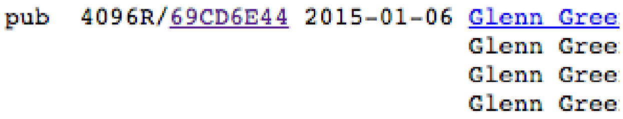
```
pub  4096R/69CD6E44 2015-01-06 Glenn Gr
                               Glenn Gr
                               Glenn Gr
                               Glenn Gr
```

ADDING SOMEONE ELSE’S PUBLIC KEY FROM A KEY SERVER:

The best part about being able to encrypt and decrypt messages is sending private and secure messages to people. For this to work you will need that person's public key. The fastest way would be to ask them for their keyid or a link to their public key. But what if they are not around, or if they are not online when you are? You can ask the keyserver for it! Then you will add that public key to your machine.

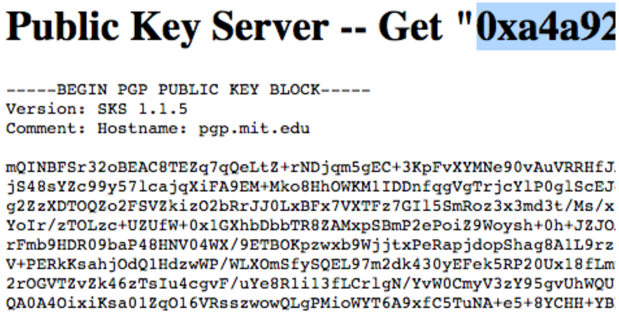
1. **Open you web browser and go to this website: https://pgp.mit.edu**
2. On the website is a box that says "Search String". Search by entering the email address of the person you are looking for. (in this example we typed Glenn.Greenwald@theintercept.com)

3. You should see something that looks like this:



```
pub  4096R/69CD6E44 2015-01-06 Glenn Gree
                               Glenn Gree
                               Glenn Gree
                               Glenn Gree
```

4. The first link will allow you to see the full public key. On the top of that page after the word GET is the KEYID for this person in quotes. Select the keyid.



Public Key Server -- Get "0xa4a92

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.5
Comment: Hostname: pgp.mit.edu

mQINBFSr32oBEAC8TEZq7qQeLtZ+rNDjqm5gEC+3KpFvXYMNe90vAuVRRHfJ
jS48sYZc99y57lcajqXiFA9EM+Mko8HhOWKM1IDDnfqgVgTrjcYlP0glScEJ
g2ZzXDTOQZo2FSVZkizO2bRrJJ0LxBFx7VXTFz7GIl5SmRoz3x3md3t/Ms/x
YoIr/zTOLzc+UZUfW+0x1GXhbDbbTR8ZAMxpSBmP2ePoiZ9Woysh+0h+JZJO
rFmb9HDR09baP48HNV04WX/9ETBOKpzwxb9WjjtxPeRapjdopShag8A1L9rz
V+PERkKsahjOdQ1HdzwWP/WLXOmSfySQEL97m2dk430yEFek5RP20Ux18fLm
2rOGVTZvZk46zTsIu4cgvF/uYe8R1il3fLCrlgN/YvW0CmyV3zY95gvUhWQU
QA0A4OixiKsa01ZqO16VRsszwowQLgPMioWYT6A9xfC5TuNA+e5+8YCHH+YB
```

ON A MAC

1. In GPG KEYCHAIN choose **KEY -> Lookup key on key server**
2. Paste in the KEYID from the pgp.mit.edu site and click **SEARCH KEY** (you should see it appear in the result box)
3. Check the box to the left of the key and choose **RETRIEVE KEY**
4. Next time you choose ENCRYPT option, the public key for this person will show up.

ON A PC (**skip over this part if you are on a mac **):

1. In KLEOPATRA choose **File -> Lookup certificates on server**
2. Paste in the KEYID from the pgp.mit.edu site and click **SEARCH** (you should see it appear in the result box)
3. Check the box to the left of the key and choose **IMPORT**

VERIFYING SOMEONE'S PUBLIC KEY, ESPECIALLY IF THEY ARE A WELL KNOWN FIGURE:

Sometimes you will find many keys associated with the same email address and name. It can be a little confusing as to which one is the correct one to add. This is why verifying someone's public key is important. The easiest way to do this is to ask them for their keyid through a secure channel, e.g an encrypted mobile messaging app like Open Whisper System's SIGNAL app. This doesn't always work if the person can't prove to you which keyid is yours you will need to figure it out yourself. Here are some tips::

An example of the problem you may face with people w/ multiple keys (old keys) and public personalities (fake keys)

1) **Open you web browser and go to this website: https://pgp.mit.edu**
2) In the search field you can **enter a person's full name** or email address. Let's type in: Glenn Greenwald
3) Whoah many results come back, and worst of all not all of them have anything to do with Glenn.

One way we can figure out which key is the one we want is by checking who else has "signed" each key:

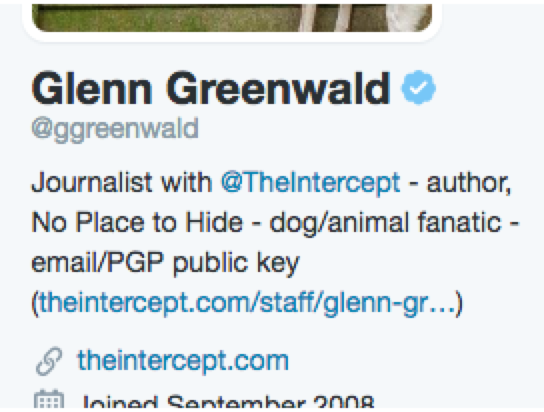
1. **Open you web browser and go to this website:** https://pgp.mit.edu
2. In the search field you can **enter a person's full name** or email address. Let's type in: Glenn Greenwald
3. Click on the link of their name and email: `Glenn Greenwald <Glenn.Greenwald@theintercept.com>`
4. You will see a list of everyone who has signed

that they believe this key to belong to this person.

5. **DO YOU KNOW THESE PEOPLE?** If these signees look familiar this is a good indication that this is the real key of the person.

Another way to is checking twitter to verify a keyid:

1. Find the person whose key you want to verify on twitter https://www.twitter.com.
2. Look for a keyid ,fingerprint, or link listed under PGP or GPG in their bio and/or location



Glenn Greenwald
@ggreenwald

Journalist with @TheIntercept - author, No Place to Hide - dog/animal fanatic - email/PGP public key (theintercept.com/staff/glenn-gr…)

theintercept.com

Joined September 2008

   a. If you don't see one consider sending a tweet out to the internet asking for the correct GPG/PGP info for the individual.

ON A MAC

If you find a link to a keyfile (.asc) or a link to open the public key on your screen

1. I recommend NOT downloading the asc file,
2. Instead open this asc file in it your browser and **select everything** including ---BEGIN to END --- Remember you have to have every character selected for this to work even those dashes before and after the words BEGIN & END.
3. Then right click and **import key selection**

If you have a problem with the import

follow the following steps

1. Open this asc file in it your browser and **select everything** including ---BEGIN to END ---
2. Copy what you have selected and open an editor (TextEdit or Notepad)
3. Paste the encrypted text into the editor
4. Save this page as filetype ***.asc** or ***.txt**
5. In your encrypted key manager (GPA on PC or GPG Keychain on MAC) import the file you saved.

If you find a GPG or PGP fingerprint or signature

1. Make sure the fingerprint/signature has two spaces between the first 5 set of numbers so you can look for an exact match online.
2. Check the box labled “Show PGP fingerprints for keys” on https://pgp.mit.edu and before puttng the person you are looking fors email or full name in the search field. .
3. Now in the results you will see a fingerprint under each key. You can use your browser’s find in page to see if there is a match.

If you find a a keyid

1. You can Lookup the keyid as seen in ADDING SOMEONE ELSE’S public key

ON A PC

If you find a link to a keyfile (.asc) or a link to open the public key on your screen

1. I recommend NOT downloading the asc file,
2. Instead open this asc file in it your browser and **select everything** including ---BEGIN to END ---
   Remember you have to have every character selected for this to work even those dashes before and after the words BEGIN & END.
3. Then right click and **import key selection**

If you have a problem with the import follow the following steps

6. Open this asc file in it your browser and **select everything** including ---BEGIN to END ---
7. Copy what you have selected and open an editor (TextEdit or Notepad)
8. Paste the encrypted text into the editor
9. Save this page as filetype ***.asc** or ***.txt**
10. In your encrypted key manager (GPA on PC or GPG Keychain on MAC) import the file you saved.

If you find a GPG or PGP fingerprint or signature

4. Make sure the fingerprint/signature has two spaces between the first 5 set of numbers so you can look for an exact match online.
5. Check the box labled "Show PGP fingerprints for keys" on https://pgp.mit.edu and before puttng the person you are looking fors email or full name in the search field. .
6. Now in the results you will see a fingerprint under each key. You can use your browser's find in page to see if there is a match.

If you find a a keyid

2. You can add that as seen in ADDING SOMEONE ELSE'S public key

Another place you can verify someone's key is the site keybase:

6. Go to https://www.keybase.io
7. In the search type the person's twitter account by typing in their username.

SIGNING KEYS AND WEB OF TRUST:

As you begin to add public keys there is a way you can sign/certify that the key is the correct one. This helps others who are looking to validate the key. It also links your key and their key in the key server showing you stand behind the fact this is the key of the person it claims to be. To do this you sign the key and then if you want republish the key with your digital GPG signature! This also raises the TRUST level the system has in this key.

On A PC:

1. In the GPA app click the key you want to sign so its row is highlighted blue
2. In the GPA task bar click on KEYS then click on SIGN KEYS...
3. You will be asked to check the box on to Sign Locally or not.
    a. Signing is public and sent to the server, for everyone to see. your name will be listed in the list of people who signed on that this key is owned by the person listed. We recommend this.
    b. Sign locally, if you don't want this. You may not want to have a public connection to the key and only want your computer to know you have verified the key owner is legit. The box you can check on allows this
4. Click on SIGN

ON A MAC:

1. In the GPG KEYCHAIN app click the key you want to sign so its row is highlighted blue
2. In the GPG KEYCHAIN, **RIGHT CLICK** (or press CTRL and CLICK) **on that person's name.**
3. You will be asked to choose which of your keys you sign with.
4. You will also be asked to choose the level of

certainty you have that this key is owned by the person listed. I recommend you choose no higher than “I have done casual checking” unless you are looking at the person’s id.

5. Click on GENERATE SIGNATURE
6. You will be asked for your PASSPHRASE and now this person’s key is signed
7. If you want to share your signature with the world, right click on this person’s name and choose “SEND **PUBLIC KEY** TO KEY SERVER**”**

YOU ARE DONE! TEST YOUR SKILLS

The ultimate test is to send an encrypted email &/or file and then receive one. The next ultimate test is to teach someone else how to do this. yay!

SOME ADDITIONAL THINGS TO THINK ABOUT (Advanced ideas you should understand): Mandatory reading for journalists & activists

WHEN TO SIGN A MESSAGE? WHEN TO INCLUDE YOUR PUBLIC KEY AS A RECIPIENT?

it's important to realize that it's very hard to deny a message that is signed with your one and only private key. it is also hard to claim a message isn't somehow related to you when your public key is bundled in the ciphertext. there are times where you will want to send a message (perhaps from a one-time-use email address, or a throw away mail.com or hushmail.com account from a made up username not associated to you). in these cases and many others you would not want to SIGN the message NOR include your key as a recipient. just remember that only the recipient can decrypt the message. once you encrypt it you can't decrypt it (because it's associated with ONLY the recipient's public key). confused yet? :) its an advanced subject so ask around.

DEALING WITH ATTACHMENTS:

A big part of email messaging is attachments. Personally we suggest using tools like ONIONSHARE (https://www.onionshare.org) to send files. However it works only when you and the person you are sending a file to are both online at the same time.

Sometimes you have to add a file to an email. How do i add a file?

ON A MAC:

1. Right click on a file from your deskop or in finder.
2. Under services choose ENCRYPT FILE
3. Choose who to send the file to.
4. Its recommended tha you sign the file. (it will begin zipping and encrypting).
5. An encrypted copy of the file is now in the same directory but with a different ending (.GPG) and an icon that looks like a LOCK on a page.
6. We recommend then **renaming the file** to something like **file.gpg** since the filename might give away its contents.
7. Attach the encrypted file to a message. There are a few more advanced ways to handle this but we'll leave it at that. try sending yourself an encrypted attachment of an image and then decrypting it to get a feel for this workflow.

DECODING ATTACHMENTS WHEN THEY ARE IN THE MIDDLE OF YOUR DECRYPTED MESSAGE:

After you decrupt a message you may see in the decrypted text an email attachment. If it looks like:

Hey how are you doing hope you get this important file

Content-Transfer-Encoding: base64
*Content-Disposition: attachment; filename="**2009 California Cup Schedule (Black&White).pdf**"*

JVBERi0xLjQKJcfsj6IKMSAwIG9iajw8L1R5cGUvQ2F0
YWxvZy9QYWdlcyAzIDAgUi9QYWdlTGF5
b3V0L09uZUNvbHVtbi9PcGVuQWN0aW9uWzQgMCB

*SL0ZpdF0+PgplbmRvYmoKMiAwIG9iajw8L1By
b2R1Y2VyKEJsdWViZWFtIEJyZXdlcnkgNS4wKS9Dc
mVhdGlvbkRhdGUoRDoyMDA5MDEyOTIzMTky
...*

Now what? The attachment you need isnt a familiar paper clip attached to your email. It is somehow fused into the text iteself? Don’t stress this is how you turn that chunk of text into the file you are expecting.

1. Copy the entire text beginning at “Content-Transfer-Encoding: base64” and paste this into your text editor and save as with the file extension (ending) ,UUE. When you click on this UUE file your system should automatically decode it. Just be sure that there are not several of these base64 encoded attachments stacked together. They all must be saved as their own UUE file.
2. **On a mac** you would need software like Stuffit Expander to open the uue (http://my.smithmicro.com/stuffit-expander-mac-download.html?submissionGuid=f19ade7f-213e-4c18-8530-cda815640577) **On a PC** you would can get Stuffit Expander here (http://my.smithmicro.com/stuffit-expander-win-download.html?submissionGuid=9a7faa4d-0038-4ceb-ac56-dc609454c844)

There is another method for MAC & PC using only Chrome browser. This also works on a Chromebook or to use Google Chrome to open these kind of inline base64 encoded attachments you would Open a new tab

Paste the follow in the location bar:
data:text/plain;base64, and append just the text part of your base64 string

Here is an example
data:text/plain;base64,SGV5IGd1eXMhIEhvcGUgeW91J3JlIGRvaW5nIHdlbGwu

1. Then go to FILE-> SAVE PAGE AS…

   Give the page a name and file name, for example the one listed right before the garbled base64 encoded letters & numbers: ***2009 California Cup Schedule (Black&White).pdf***

   When you open the file it will be the

attachment you received.

TTC6) EXTRA: your very important private key is located in ~/.gnupg We recommend coughing up $50 & some time. to get it onto a yubikey neo (https://www.yubico.com/products/yubikey-hardware/yubikey-neo/) instead. another quick solution for someone who uses a mac encrypts/decrypts a lot is a nifty drive (http://minidrive.bynifty.com/), or for macs (or a pc with an sdcard slot) a shortened sdcard (https://www.adafruit.com/products/1692). who knows what's running (maybe bomgar remote support, virustotal, jamf casper, etc. and other apps scan/access) in your business issued laptop on a regular basis. trust no one, not even your hard drive :) ok have fun!

PEOPLE CAN TELL WHOSE PUBLIC KEY THE ENCRYPTED EMAIL MESSAGE IS FOR.
WHEN SENDING ONE EMAIL MESSAGE TO MULTIPLE PEOPLE TAKE NOTE!
Its important to know that all the keys can be viewed by anyone who has the ciphertext. They will not be able to decypher the message if it was not intended for them but they can see whose keys can. A way to see this is to use PGPDUMP https://github.com/kazu-yamamoto/pgpdump , there is an online demo version (not to be used for sensative messages) here http://www.pgpdump.net/ . A way to remove keys from a message is to use THROW keys https://www.gnupg.org/gph/en/manual/r2110.html You can read more about this here on VICE MOTHERBOARD http://motherboard.vice.com/read/pssst-your-pgp-is-leaking . A good idea is to send the message from yourself to yourself and bcc: each person one by one their own encrypted message.

QUIT QUIT QUIT!
MAC people, if you do use this textedit based workflow be sure to CLOSE TEXTEDIT often. it has a undo feature that will show encrypted text as its original plaintext. encrypt a message, then click undo, to see what i mean.

HOW DO I CANCEL/DELETE MY PUBLIC KEY FROM A KEY SERVER?
well there is no way to CANCEL CANCEL your key. it doesn’t get deleted from the key server pools but it does get marked as KEY REVOKED!!! and software

will alert or refuse to use the key.

to generate a revocation certificate:

ON A MAC:

1) run gpg keychain
2) select your name and email from the list of displayed keys
3) right click on your name and choose “ GENERATE REVOKE CERTIFICATE” or in the toolbar under KEY -> GENERATE REVOKE CERTIFICATE
4) you save this file to your desktop or a usb and use it when you want to cancel this key.
5) you can transfer the certificate to a usb and tape shut in a shoebox buried in your backyard or locked away in a safe or cabinet. you most likely (hopefully) won’t need it.
6) if you had to use it you would follow these steps above but choose REVOKE instead of generate revoke certificate. it will ask you for the path to the certificate before it grants your request.

ON A PC:

1) click on WINDOWS icon
2) choose ALL APPS
3) choose WINDOWS SYSTEM
4) click on COMMAND PROMPT
5) a scary black window with a cursor blinking appears
6) type: gpg --list-keys
7) you will see a list of all the users on this machine. the key you made should appear with a username and email
replace <USERNAME> with your username listed above
8) type: gpg --gen-revoke <USERNAME> > revoke.asc
9) create a revocation certificate for this yet? press lowercase y
  b) select the reason you are relocating the keys: press 1
  c) click enter key twice
  d) is this ok that no reason was given? press lowercase y
  e) enter your passphrase
  f) in this folder c:\Users\<windows user>\ is your revocation key! yay! you did it.

HOW TO REMOVE THE COMMENT LINE FROM GPGTOOLS ENCRYPTED / SIGNED MESSAGES:

ON A MAC:

In terminal (command+space, type:terminal)
cd ~ <press enter>
open .gnupg <press enter>
You will see plain english but always a “#” before it.
Find the comment line.
Add a “#” before it.
Save the file

ON A MAC:

I try to encrypt but it says
“No private key selected to add to recipients”
This error is caused by asking gpgtools to automatically add yourself to the list of people whom this is encrypted for, but you have more than one key - and didn’t tell gpgtools which one ot use. Try again but this time when it ask who you want to encrypt the message for, you should look for a dropdown bar where it says YOUR KEY. It is suppose to have your name and the PUBLIC KEY you want to use.

written by raven &
@geminiimatt
geminiimatt@protonmail.com

Additional editors & contributors:
@harlo
@redshiftzero
@blackswanburst
@sidnext2none

Did this guide help you? please donate comments, suggestions, & share widely to make it better!