Guide to Anonymity

Author: Leo Gurr

Table of context

Key

For diagrams in this paper: blue boxes represent objects that are connected to the internet (such as your computer), black boxes represent objects that are not connected to the internet, red outlines mean objects that are dangerous or disposable, and other colors represent different operating systems.

Prologue

To be explicitly clear, I am not affiliated or sponsored by the group Anonymous.

Before I begin this guide, I want to say that there is a real difference between anonymity and privacy on the internet. Privacy is the idea that people should not be able to relate data to you. Example, you do not mind that people know your email address, or that you have a youtube account, but you do not want people knowing what you do with it. Anonymity is the idea that you do not want people relating an identity with you. Example, you do not care that people know that Anonymous43217890 said ugly things, you just do not want people to know you are Anonymous43217890.

I am writing this guide specifically toward people who need anonymity. I am not saying that privacy and anonymity never overlap. If you are interested in privacy, you will find most of this guide useful. Most people who want anonymity are people who are doing something they are not "supposed" to be doing something. This could mean you are a: journalist, whistleblower, criminal, hacker, or anyone else I can not think of. The goal of this guide is to help people evade the adversaries that mean them harm.

Something to note, I am going to assume anyone who could mean you harm is an adversary for the purposes of this paper.

Something to understand is that this guide is not a "direct guide" or a "guide for dummies". Meaning, I am not going to give you a checklist of different things you should do to stay anonymous. Everyone has different needs. My goal is to present different problems and present a few options with the pros and cons. In certain aspects I find critical for your anonymity, I will give detailed directions on what to do and how to use different tools. If I do not go into detail in this guide about a subject, I will try to post a link to someone who does.

Also, something to note for this guide is the links I provide. It is never a good idea to trust links in a pdf file. So I would recommend copying and pasting the links into a web browser, rather than just directly clicking on the link. If possible, opening the links on a different computer or OS that is not used for anything other than open files. I am not saying that my links are malicious, just helping you take precautions. For the most part, my links only provide additional information to stay anonymous anyways.

There are a lot of different ways that an adversary could try to take away your anonymity. The main ways an adversary might attack your anonymity is: tracking your data (IP address, social engineering, and correlation attacks), your security flaws, snooping on communication, and following money/item trails. My goal is to try and explain each one of these attacks, and the different options to avoid them.

Nothing in this world is perfect. There is no such thing as a "silver bullet" when it comes to anonymity online. Also, this guide is not for everyone. I will go very far in detail about as many things as possible. I will try to teach on a "beginner" level, but that does not mean you can have no knowledge of computers or the internet in general. This guide is best for people who are between novice and expert.

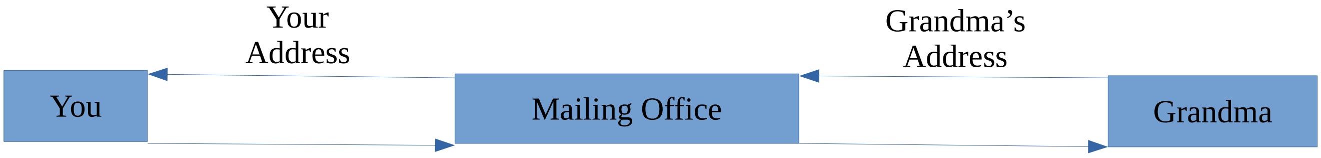
Also, understand that something might be missing in this guide that is critical for your situation, it is important to always have good common sense.

Chapter 1 – Browsing the internet

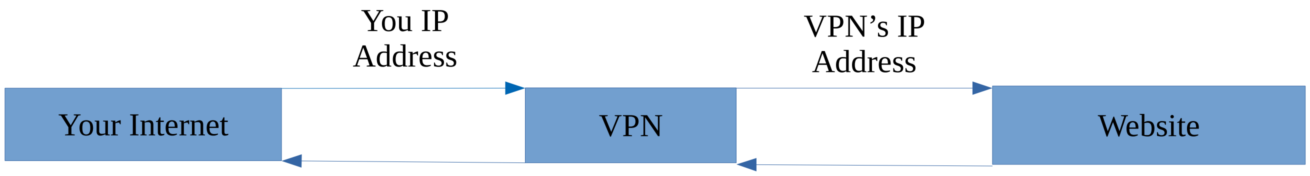
If you want to stay anonymous on the internet, know it was not built to be anonymous. As time has progressed, there has become a need to be anonymous on the internet. But, understand is that not everything you do online should be anonymous. For example, if you use a bank online you want the bank to know you are who you say you are. To fix this, you should have two separate worlds on the internet, your public world, and the private world. That is the first point I am going to make in this guide, you need to have separate identities. You private identity, your pseudo-identity, is one that should never be linked to you. The ways your pseudo-identity can be linked to you based on your internet usage is your IP address, browsing habits, and the accounts you make.

[**IP addresses Intro]** One step to separate identities is to never have your "direct" data traced back to you on the internet for your private business. To understand how to stay anonymous on the internet, you need a basic understanding of how the internet works. You have most likely heard the term "IP address" thrown around a few times. Most people think it is this complicated thing that only hackers need to know. But this is not true. Everyone should have a basic understanding of how the internet works, and how IP addresses relate to you. Your IP address is a key aspect of making sure your internet works.

Let's think of how you would send mail to your grandma's house. First, you write a letter, then you write your grandma's address on the card, then you write your return address, and then you send it to the mailing company. The mailing company does its thing and the letter arrives at your grandma's house. Then your grandma wants to write you back a letter. Your grandma looks at the return address, writes the letter, writes your address down, then sends it to the mailing company. Again, the mailing company does its thing and the letter arrives at your house. If you had not written down your return address for your grandma to send you mail, then she would not know where to send the letter.



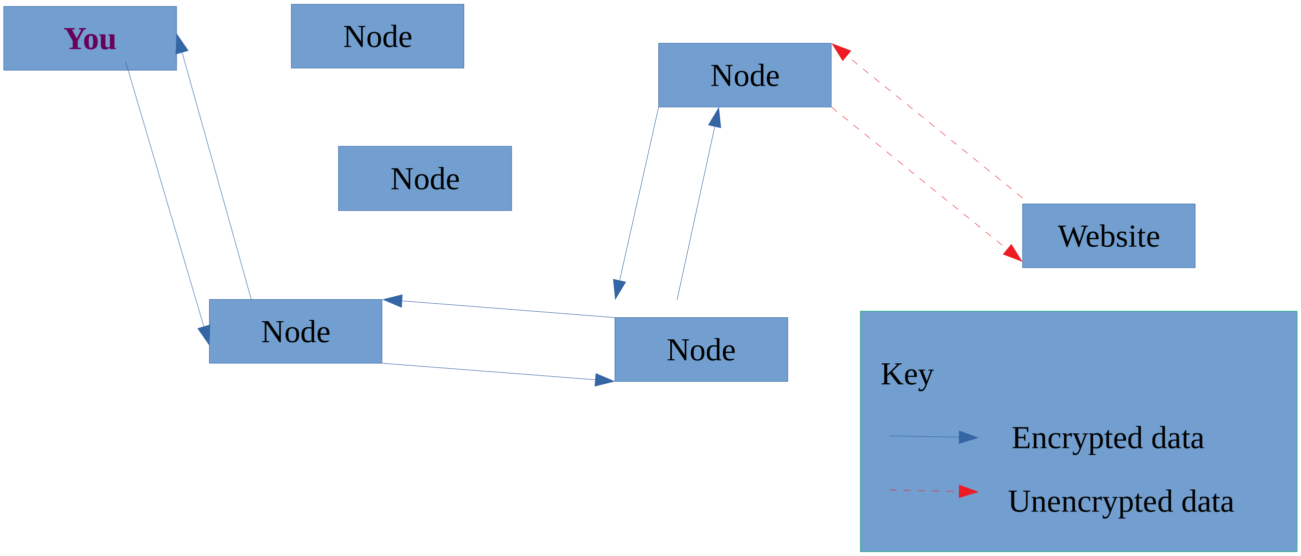
[**VPNs]** This idea is extremely similar to how the internet works. For you to get data from a website, you have to have your IP address connected to the websites IP address. These addresses are how you and the website communicate. Now say you are doing something that an adversary might take interest in. It would be very easy for them to track you using only your IP address. Because you are directly giving up your IP address to the website. Now there are quite a few ways that you can "mask" your IP address from an adversary, but we are only going to look at VPNs and Tor for the purpose of this paper. VPN stands for Virtual Private Network, the goal of a VPN is to replace your public IP address with the public IP address of the VPN. So instead of your data being sent directly to a website, your data is first sent to the VPN and then to the website. Then the website sends the data to the VPN, then the VPN sends the data back to you.



[VPN cons] Again, to most people, a VPN is good enough. But there are a few flaws with a VPN. A VPN has the ability to log everything you are doing. Even though an adversary is only able to see that traffic is flowing to and from the VPN in use, the VPN sees everything you are doing. If the adversary has enough power, they could demand the logs from the VPN and your traffic is no longer hidden. Most privacy-focused VPNs have at least thousands of clients, and would be no need to dig up your files unless you are doing something that an adversary has taken interest in. For example, if you are a criminal or a whistleblower, your government will take interest in your activities. I would not recommend using a VPN for this reason when it comes to being completely anonymous.

If you are casually browsing the internet, then you do not have much to worry about this as much. It is always good to use a strong VPN to keep companies from knowing all of your interest. VPNs are great for keeping a website form knowing who is looking at what. This is why VPNs are great for the average person. If you want more *information on different VPNs, you can visit* *https://www.deepdotweb.com/2014/07/08/is-your-vpn-legit-or-shit/*.

[Tor] Now let's talk about Tor, The Onion Router. To most people, Tor sounds a lot like a VPN. The reality is, they were made for completely different purposes. VPNs were made for security, while Tor was made for anonymity. A basic overview of how Tor works is by routing your traffic through 3 different nodes. If you want, you can think of Tor as three VPNs tied together. Your data goes into an entry guard, then a middle guard, then an exit relay, and onto the website.



[Tor Cons] So you might be wondering why Tor might be better than a VPN, well it some ways it is not. If an adversary were to have control of your entry, middle, and exit node they would be able to decrypt all your data and find out what you are doing. Also, if an adversary were to have access to just your entry and exit node, then they can find out what website you were visiting (But not the data you were sending or receiving). While this might sound scary, Tor has things in place to try and minimize this threat. First off, it is very unlikely that an adversary has control of all your nodes at the same time. The three nodes changes with every website that you visit. So since your path is constantly changing, it is very difficult to track everything you are doing. This idea of using three nodes and a changing path is called onion routing. Also, Tor is very slow. This makes casual internet browsing very difficult on Tor, due to the fact that your internet is jumping all over the world. People volunteer to host Tor nodes, and as more people use that node, the slower it will become.

[**Hiding Tor]** Your ISP, Internet Service Provider, knows that you are using Tor unless you are using a VPN with Tor or are using a bridge to get to Tor. If you would be putting yourself at risk by using Tor, you can learn more about bridges here https://www.torproject.org/docs/bridges . If you are interested in using a VPN with Tor, understand it might not make you IP addresses safer. I would not recommend using a VPN personally unless you have reasons to hide your usage of Tor and can not get a bridge. But, you can visit https://www.deepdotweb.com/jolly-rogers-security-guide-for-beginners/combining-tor-with-a-vpn/ for counterarguments.

[**Hidden services]** Something else that Tor has to offer is hidden services. A hidden service, a website that ends in .onion, is a website that can only be run from within the Tor network. This is useful because your data never has to be decrypted when you visit hidden services. But, hidden services are sometimes used for less the legal things. All the hidden services are considered the "darknet". I find certain hidden services, such as email services, to be very useful. I would make sure you really understand how to be anonymous before you try to use, or infiltrate, a hidden service that host non-legal activities. Here is more information on hidden services https://www.youtube.com/watch?time_continue=1385&v=VmsFxBEN3fc .

[**Youtube in Tor]** If you want to use Youtube while using Tor use, https://www.youtube.com/html5 . If you choose not to use javascript, then you can visit http://m.youtube.com/?persist_app=1&app=m to go to the mobile version of youtube. Then you can watch a video using a youtube converter, such as https://www.yoodownload.com/download.php . You will not be able to return to the desktop version of Youtube until you restart Tor. Do not download the video, just watch it from your browser. *Understand the video will be slow to load, but that is a small cost to make.*

[**General Browsing]** Overall, if you are using Tor correctly, there should never be a link to you and what you do on Tor. Even if no one can trace you based off your IP address, they can still trace you by other means. No matter how hidden you are on the internet, if you log onto your Twitter account you are not anonymous. People will know it is you that is tweeting, regardless if they can trace you over the Tor network. You have to create a completely different identity than what you use outside of Tor. You should have, at the minimum, two identities. One of those is for everyday activities, and the other is for your private business. There should never be a bridge connecting those two identities.

[**Accounts General]** The only way you can create a gap between you and your private life, is to create a pseudo-identity(s). Even if no one can trace you because of your IP address, that does not mean they can not trace you because of your accounts. To better explain what I mean by this, allow me to explain.

> So Johnny just found out about Tor browser and how it can make him anonymous. Excited, Johnny downloads Tor and logs into his Tweeter account. Then he tweets all over social media saying "Hey guys, I am on Tor, no one can know who I am !!!!".

Do you see what the problem is with Johnny's thinking? Even though his IP address was not connected to him when he made the post, the account he was using was. When he registered for that account, he probably used his home network and his real information. Also, has probably revealed personal information on while on this account. In order for an account to be truly anonymous, you need to leave no traces to you from this account.

[**Anonymous Accounts]** In order for you to create an anonymous account, you need to do two things (In terms of what you do while on the internet). You need to never reveal personal information on this account and never have this account tied to your personal IP address.

[**Personal information]** When I say never reveal personal information, I mean never reveal personal information on a new account that you create. Even if you delete something you said that is personal information, assume that information is still stored on a server. Assume anything you say online while using this account is being logged, and someone is waiting to link it to you.

[IP addresses] The anonymous accounts you make can never be correlated to your IP address either. Every time you use the account, always use it from Tor or a trusted VPN. Never use your personal IP address to use the account. Also, when you sign up for an account, you have to create it while masking your IP address. If you have a trusted VPN or a public place where you can sign up for accounts, then you are in luck. But, many people do not have this luxury. Also, even if you do have a trusted VPN, there is a good chance that a lot of people use that VPN. This can make signing up for accounts very difficult. Websites have to avoid robots making spam accounts. The same reason why you want to remain anonymous while making an account, robots want to remain anonymous while making accounts so the websites do not think they are robots. Websites want a way to prove you are human, even privacy-focused websites. I always recommend signing up for all your accounts while on Tor, but this can be very difficult due to spam.

[**Signing up for Anonymous Accounts]** If you want to make an anonymous account, this can make signing up processes very difficult. Many websites try or require, to reveal some personal information when you signup to prove you are human. This could mean they ask for a donation, phone number, or “personal” email address. If a website gives you the chance to pay for their privacy-centered service in an anonymous way (such as bitcoins, more on those later), then this is what I would recommend you do. I believe it is best you pay for your [fill in service] with your wallet, not your privacy. But, some websites require you to use a phone number. This can be very frustrating because you know they plan on tracking you if the service requires you to use a phone number (making anonymity impossible). My suggestion is if the service requires to use a phone number to sign up, then do not use the service. There is no service that requires a phone number that lets you be truly anonymous (looking at you Google). If a service lets you use an email to sign up, there are solutions to this. It is very possible to create anonymous emails.

[**Anonymous Emails (Temporary)]** A temporary email address may be an option, one very popular temporary email service is Guerrilla Mail https://www.guerrillamail.com/ . A temporary email address allows you send and receive emails from an anonymous location. This way, you never you have to have the account tied to a central identity. But, what if you want it tied to your pseudo-identity? Most temporary emails are useless if you want a stable place for people to reach you.

[**Anonymous Emails (Permanent)]** So, what we can do is create a more permanent email. This will allow you to use services that require an email and gives a location for people to reach you anonymously. A personal favorite of mine is Proton Mail https://protonmail.com/ . The issue with permanent emails, however, is there is a trail for an adversary to follow for every service you use the email to sign up for. If you reveal who you are on account 1, then you reveal who you are account 2, and on your email. Because account 1, account 2, and the email address are all the same person. So stable email address provide more usability but come with more risk. If you ever reveal personal information on an account tied to your permanent email address, then all of your accounts are compromised.

[**Social Engineering/Correlation attacks]** Even if you do everything that you are supposed to do on Tor, you can still be traced. Things that you do not even think about can get you caught, or interrogated. What websites you visit at what times, how fast you type, what time do you log onto Tor, your style of typing, your attitudes on certain topics, how much you know about a certain topic, and much more. This type of attack is called social engineering or correlation attack. Where they can try and link what you do on Tor to someone outside of Tor, and confirm it is them by following the real-life person's every move. This is not just a theory, people have been caught because of this.

[**Busts on Tor]** There have been a few busts over the years, but I have not found any articles about people being caught because of Tor itself. People have been caught because they made a mistake that linked their pseudo-identity to them. If you do find yourself in the unfortunate event of being interrogated, never confess is a golden rule.

10-12 hour in the integration room is short compared to 10-20 years behind bars. If possible, do not talk to the interrogator in the first place without an attorney. Here are some of the different bust over the years on Tor https://www.youtube.com/watch?v=7G1LjQSYM5Q . Again, none of the busts were successful because of the design of Tor, but because of the actions of the people who were using Tor.

[**Changing Identities]** Another thing you should be doing while you using Tor is regularly changing identities. How often really depends on what you are doing on Tor and how often. If you are only buying or looking at different websites, then I would change identities every few months. If you are a vendor selling, I would recommend changing identities every year. This may seem excessive, but doing this could save your life.

[**Public Wifi]** If you choose to visit public places to use their wifi, blend in with your environment. If you are using a college Starbucks, dress like a student or teacher. If you are at a library, were apollo or button up with blue jeans and actually read a book. Change your posture, your voices, and the way you look at people. Of course, you should be changing locations very often. The fewer people in your area, the further you should be traveling from your house. Also, make sure to buy everything in cash. Do not pay with hundred dollar bills. Your goal is to stand out as little as possible. I will challenge anyone working in a public to remember someone who visits your store twice a year, especially if they are changing their posture and clothes. If there is nothing to make a person stand out, there is no reason to remember them. You want to buy a computer that you would not mind using in public, and will not turn eyes. In real life, you should be confident knowing no one is watching you because you are paranoid behind your computer screen. Also, please make sure to disable/cover up your webcam. None of this matters if your face gets plastered all over your adversary's networks. Remember what I said, always assume someone is watching you make every keystroke on Tor. As if they are watching you through your window, but as if you are wearing a mask. A truly motivated adversary will always be waiting for you to accidentally remove your mask, to slip up.

[**Central idea]** Here is the central idea when it comes to using the internet. When you are using the internet like normal; you know that people could be watching, you but assume they are not. When you are using the internet over Tor; you know that people could be watching you, *and you assume that they are.* Believe me, when I say this, there is probably someone logging everything that your pseudo-identity is doing on Tor, waiting to link it to you.

Chapter 2 - Security

Even if people can not track you by your IP address, or by your activities online, there are other ways of attacking anonymity, one is through your security. Security plays a huge role if you can stay anonymous or not. Nothing can keep you anonymous if someone can track based off the uniqueness of your computer. If you have a virus or operating system that is telling a company everything you are doing on the internet (Chances are you would not even know), then you are not anonymous. Worst yet, if someone just looks through your hard drive to see what you have been up to, they can know everything you were doing without much hassle. Let's take about the different solutions to each of those problems.

[**Fingerprints]** The very first thing to worry about is your digital fingerprint. Similar to how an adversary can track down a person based on little things about them, websites can track you based on little things about your computer. Some things that can identify your computer are the size of the monitor, your OS, what browser you are using, what plugins you have, your time zone, and even how pixels are generated on your computer (How ABC looks different on my computer than yours). Private browsing does not help with fingerprinting at all. Here is an article if you want to learn more about fingerprinting https://scottiestech.info/2015/04/12/browser-fingerprints-what-they-are-how-they-work-and-what-it-means-to-you/. If you are using Tor, by default then there are plugins installed that minimize fingerprinting. I will not explain all the different techniques here, but here is a link that goes into great depth http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html . I would recommend disabling Javascript the moment you open Tor. Tor be default does not disable Javascript by default, and here are Tor project's reasons why https://www.torproject.org/docs/faq.html.en .

[**OS intro]** Before I go explaining the different operating system that you might want to use, allow me to explain what an OS, operating system, is. Every time you boot up your computer, your computer first goes into the BIOS. Then from the BIOS, it boots up into Windows (assuming you are using windows). Anything that boots off the BIOS is called an OS by definition. There are other OS's out there than just Windows, MacOSX (What macs use), and IOS (iPhones). The main OS that is used besides these is Linux.

[**Nonlinux OS’s**] One area than an adversary might attack to try and strip you of your anonymity, one of them is your computer itself. Something that an adversary might try to do is to plant malicious code onto your computer. Then have that virus tell the adversary everything you are doing. Even with the best of the best firewalls, there is no way an anti-virus program can catch everything a determined adversary can throw at your computer if you are using Windows. Plus, Windows, MacOSX, IOS, and Androids send your data to their companies for "technical" reasons (read the terms of service). The fix this, we need to attack the source of the problem, the operating system you are using.

I am not going to go into much depth about security on smartphones. Most phones were built with the intent of tracking you. If you choose to use your phone, understand the risks associated with that. There are plenty of articles showing that data providers can sell your location to companies, here is one https://www.stuff.co.nz/technology/109522772/heres-how-your-phone-is-tracking-you . If phone companies and data companies are willing to sell your location, they would also be willing to sell and give up your browsing history.

[**Linux History]** When computers were first being made, there was a debate about whether manufacturers should use Windows or Linux. Linux is much more powerful than Windows, in terms of what the user can do with it. But Windows is more simple than Linux and good enough for most people. So now almost all computers ship with Windows installed unless you are buying a mac that is. But some computers do not have Windows installed as their main OS, they have Linux installed. You can actually install Linux onto a computer that already has Windows installed on it. Plus, Linux can be built from the ground up and be built just for your needs, if you learn how to programme. So, you can imagine why we would want to use Linux over Windows. There is so much more that can be done with Linux that Windows can not do. But, there is also a lot that Windows can do that Linux can not. Here is an article going more into depth about the differences between Linux and Windows https://www.linux.com/news/linux-and-windows-security-compared . There are many different types of Linux distros, unlike

Windows. Some Linux distros were built specially for security, management, scientific research, and privacy. We will be looking at the Linux distros that were made to protect our privacy, and use them to give us anonymity. TAILS and Whonix are the primarily OS's I am going to talk about.

[**TAILS]** Completely amnesic. The goal is to leave no traces on your computer and to have everyone using it look the same on the internet. So in theory, there is no way to tell one TAILS user apart from another TAILS user. TAILS is also run as a Live OS from a removable media, such as a USB stick. A live OS can run on a computer without a hard drive at all. Even if you do have a hard drive plugged into your computer, TAILS was designed to leave no traces on your computer. If you want to learn more about live OS's, here is a link to better understand https://en.wikipedia.org/wiki/Live_USB . Be careful when downloading TAILS though, people can find out you downloaded it and have a TAILS drive. Plausible deniability can go out the window if you are trying to hide only the flash drive at that point. But if you wipe your drive and install it from Tor or using a trusted VPN, you can try and create plausible deniability. Also, you can save data on persistent storage within TAILS, so you never lose your progress no matter what computer you use. The persistent storage is not hidden from an adversary, and there are a thousand reasons why you might have to give up your password. So if there is an adversary knocking at your front door, I would recommend destroying the flash drive. Also, all the internet that is used in TAILS is routed through the Tor network. So no matter what program you run from within TAILS, it can be anonymous in theory. There are drawbacks to TAILS, read the documents that TAILS provides about what TAILS can and can not do.

TAILS FAQ https://tails.boum.org/support/faq/index.en.html
TAILS Download https://tails.boum.org/install/

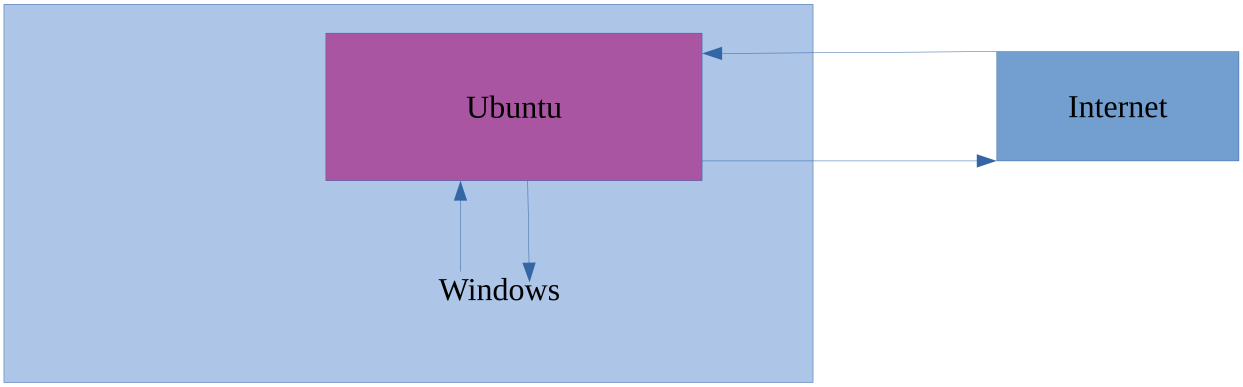
TAILS directly supports the use of Veracrpyt, a way to encrypt information onto flash drives. You might be wondering why you would need another encrypted storage if you already have the TAILS drive with persistent. There are a few reasons actually. The primary reason is that TAILS has to do updates to make sure that you have maximum security. When you update your TAILS drive, there is a good chance that you will lose everything during the update. So keeping your important data on a separate flash drive is a must. Also, you can *really* create plausible deniability. You can keep the TAILS drive in the open and the Veracrypt in a private place. Plus Veracrypt has hidden volumes, so there is no way for an adversary to prove that a file or volume even exists at all in the Veracrypt drive. If you want to learn more about plausible deniability, visit https://www.veracrypt.fr/en/Plausible Deniability.html . At the time of writing this, TAILS does not allow you to encrypt the drive while using TAILS. That means you will have to download Veracrypt onto a separate trusted HDD and OS.

Veracrypt download https://www.veracrypt.fr/en/Downloads.html
Veracrypt FAQ https://www.veracrypt.fr/en/FAQ.html

For some people, I might be beneficial to have a Veracrypt drive, TAILS, and a main computer with Whonix+Qubes. It all depends on your needs. Veracrypt is supported by most Linux OS's, so I would look into even you are only using Whonix+Qubes.

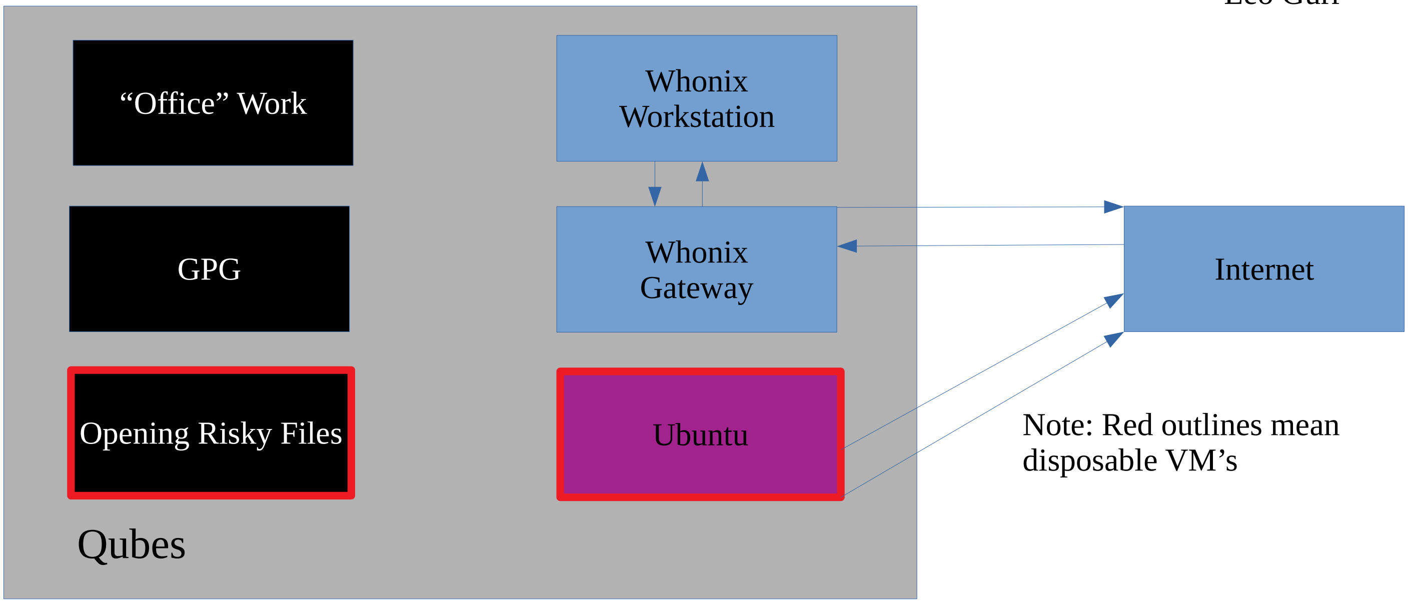
[**Whonix intro]** Stable privacy. Whonix is much more complicated to get set up than TAILS in my opinion. But Whonix is better than TAILS if you planning on using one computer for all of your private internet activity. Whonix saves everything it does on your computer, but it only runs in virtual machines. If you do not understand what a virtual machine is, allow me to explain.

[VMs] A virtual machine, VM, is basically a computer that runs inside of your computer. You can learn how to install virtual machines on almost any OS. So say you download Ubuntu, a popular version of Linux, on a virtual machine inside of Windows. Everything that you do inside of Ubuntu will be separated from Windows. The drawback is that this does not go the other way around. Windows can see everything that the Ubuntu VM is doing. So if your host machine is infected with a virus, the virus can see everything that the VM is doing. So the VM is only as safe as the host machine it is run on. This means we do not want to run Windows+Whonix+Tor for the same reasons we do not want to run Windows+Tor. If you are doing this, all you are doing is adding tinted glass between you and the world. Might be harder to see and get to you, but someone motivated can still find you.



But on the bright side, say your Ubuntu VM gets infected with a virus, it will not be able to escape the VM into the Windows host machine.

[**Qubes]** So, we want a host machine that is safe to run virtual machines on. Almost any Linux would work fine for this, but there is a special OS that was built specially for this, Qubes. Qubes was built with security in mind. Everything you do has the ability to be run in its own VM. So if one of your machines gets infected, you can just destroy it and move on. You can even create disposable VMs that are used only to open dangerous files, then delete once you are done. This is where we are going to be using Whonix. It is important to remember, you do not have to use Whonix with Qubes. Qubes can be used for everyday activities, it just has a steep learning curve to get used to if you have no experience with VMs.



Note: Red outlines mean disposable VM's

[Whonix] If you did not notice, there are two different VM's for Whonix in the diagram above. This was done on purpose. Whonix actually is meant to be run from two separate VM's. One is the Whonix gateway, and the other is the Whonix workstation. The gateway's only job is to connect to the Tor network and act as a router for the workstation. Since the VM's are separate, if someone were to hack the workstation they can not find out your IP address. This is because not even the workstation itself knows what the IP address is. If someone were to gain complete control, root access, to your virtual machine, they can not find out your IP address. Because not even the workstation knows what your real IP address is. You still have to realize the drawbacks with using Tor are still present while using Whonix. One of Whonix's famous quotes is "the more you know, the safer you are".

Whonix FAQ https://www.whonix.org/wiki/FAQ
Qubes FAQ https://www.qubes-os.org/faq/

Whonix Download https://www.whonix.org/wiki/Download
Qubes Download https://www.qubes-os.org/downloads/

[**Whonix gateway for other VMs]** Something else to note with Whonix is that you can run the gateway with any other VM. The gateway acts as a router for the workstation, which means we can make it act like a router to any other VMs. This would be useful for a journalist who likes to work in a certain OS, such as Ubuntu, but have all of their traffic run through Tor. This would also be useful for hackers using Kali Linux who need to be anonymous. There are not many guides on how to do Whonix+Other OS, so I will try to teach you in this guide. Here is a link for video instructions https://www.youtube.com/watch?v=Lopiey2tkYs that I found useful.

First get the virtual machine that you want to run with the gateway set up. Then make sure to shut down then VM without saving. Boot up your gateway and make sure it is running the whole time you use the OS of your choice. Then go to the setting of your VM from the VirtualBox menu. Afterward, go to Network. Set **attached to: internal network** then make sure the **name says Whonix**. Then boot up your VM. Once the VM is running, go to the network settings. Then go to the setting in the wired connection. Go to **IPv4** and select manual. Then type...

Address: 10.152.152.11	**Gatway: 10.152.152.10**
Netmask: 255.255.192.0	**DNS: 10.152.152.10**

If all is well, your network should connect and everything you do should be run through Tor. There is a chance that something went wrong. So we can try and check if our numbers are correct for the manual IPv4 settings. Open the terminal in the gateway and type

```
user@root: ~$ sudo ifconfig
```

Then your password, if you never changed it will be **changeme**

Then look for e**th1/0: inet =** gateway **inet =** DNS **netmask =** netmask

Understand the underlined aspects are for the OS VM that is not your gateway, *while none underline aspects are found from the gateway VM in eth0 or eth1.*

Then the address should be on a different port than the DNS and Gateway, so if

inet = 10.152.152.X then address **= 10.152.152.Y**

Where X does not equal Y

Once you change your setting, you should now be able to run all your data through Tor on any VM. Understand if you want to browse the internet, you should still download the Tor browser. Even though your IP address cannot be traced, your computer fingerprint can be traced (Remember chapter 1?).

[**Seperating OS's]** Regardless if you are using TAILS, Whonix+Qubes, or some other Linux box, it is good security to separate your OS's. I would recommend using a "standard' OS for your everyday activities. This could be MacOSX, Windows, IOS, Ubuntu, Qubes, or anything else depending on your needs. This is further separating our private and public life. You would not want a bug in our public life OS that could spread into our private life OS, and vice-versa. I would recommend having another Hard drive or computer for Whonix+Qubes and removing your hard drive for TAILS. The best case scenario is having a whole separate computer for your private activities, but many people can not do this.

[**Linux commands]** Something else that is required for you to have maximum security while using Linux is learning Linux commands. I would try to teach you the basics about Linux commands, but there are too many basic commands put into this guide. Something I would highly suggest is setting up a VM just to learning how to use commands. I learned most of my commands in Ubuntu. Since Ubuntu, Qubes, Whonix, and TAILS are all Debian based, what you learn in one OS will help you in the others. Here is a link to a separate guide to learn Linux commands http://www.linuxcommand.org/lc3_learning_the_shell.php . I would highly suggest getting somewhat familiar with the Linux command line, you will need it for GnuPG in the next chapter.

[**Data encryption]** Lastly, there is another way that adversaries can attack your anonymity from a security aspect, which is your saved data itself. Hopefully, this is not one that is as much as a problem for most people. But there is a chance you might find yourself in a situation where you do not want people getting into your computer, flash drive, or hard drive. So something that you must do is encrypt all of your drives. Almost all Linux OS's support encryption when installing the OS, to include Qubes. But if you are looking to keep other operating systems encrypted, I would recommend Veracrypt. If you want a better understanding of encryption, here is a great link https://en.wikipedia.org/wiki/Disk_encryption_theory .

Veracrypt Download https://www.veracrypt.fr/en/Downloads.html

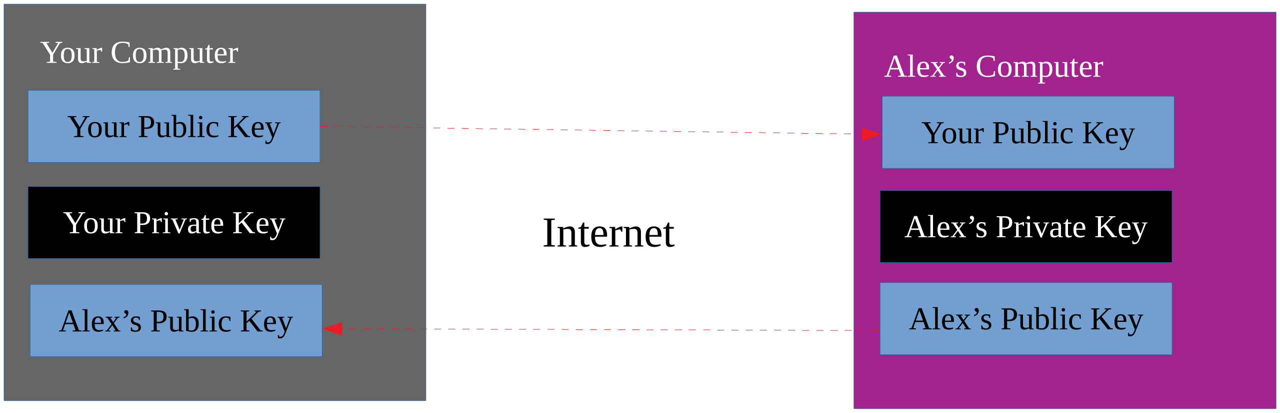
Chapter 3 – Communication

Another way that adversaries might try to attack your anonymity is by your communications. It does not matter that no one can trace from your data, or that people are unable to learn who you are from social engineering tactics, or people are unable to hack your system. If your email provider can send an adversary everything you say, you are giving yourself up. There will come a time where you will have to trust someone, other than yourself, on the internet. When this time comes, you will give some personal information when communicating. Examples are, the groups you are communicating with and people you want to buy from. You want to avoid giving an adversary the ability to read what you say. Allow me to explain how to avoid compromising your comms using encryption.

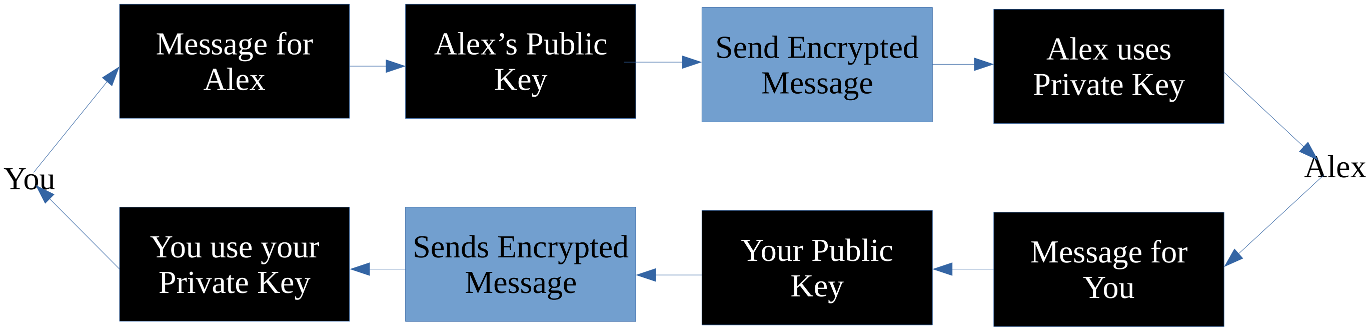
[**PGP intro]** Say you have some sensitive information that you need to send over a dangerous area. This could mean you have a king send a messenger to give a message to another king. Before the messenger sends the message, the kings discuss an encryption strategy. Every letter in the message is to be rotated four letters down the alphabet. So now a=d, b=e, c=f, d=g, e=h, etc. So to the messenger, the message just looks like a jumbled mess. This would also be true to an adversary who would take the message away from the messenger. The adversary would have no idea what the message was saying. In terms of today, this is very weak cryptography. We have much stronger encryption today than the days where kings sent messages across the battlefield. But there is a key flaw in this type of encryption. It is assuming that both the receiver and sender both know how to decrypt the message before the message gets sent. The way to decrypt the message, the key, can not be sent along with the message. Then the adversary could use the key to “unlock” the message. This is where PGP comes into play.

Some very smart person invented PGP, pretty good privacy (Understand when I say PGP in this guide, I am referring to the OpenPGP standard, not necessarily the program PGP). Things are going to get complicated, so buckle up. So imagine that you have two separate keys, public key, and private key. One of the keys is to be public and the other is to be private as the names suggest. You send your public key out to everyone who you want to communicate with, and you always keep your private key to yourself. You use your private key to decrypt the messages sent to you. To message people back, you use their public key to encrypt the message, then they use their private key to decrypt the message. So both people have two keys and only share one. If this sounds confusing, that is okay. I will try to paint a better picture for you. If you are not understanding, keep reading and try reading other guides. Once the idea clicks, it will all make sense.

So you and Alex want to share sensitive information. You and Alex both have a public and private key. You exchange public keys in the open air. So now you have Alex’s public key, and Alex has your public key.



So now Alex can encrypt messages using your public key on his computer. Then sends you the encrypted message over the internet. Then you receive this encrypted text. If you were to try and read the text without decrypting it, the message would like random letters and numbers that no human or computer could understand. Since you have your private key, you can use that to decrypt the message. Since you are the only one with the private key, you are the only one that can decrypt the message. Then you want to send Alex a message back, you can encrypt your message using Alex’s public key. No matter who gets a hold of this message, only Alex will be able to read it since he is the one with the private that can decrypt the message. This is a cycle that gets repeated for every message that gets sent. While it may seem tedious to send messages back and forth this way, it is necessary to take such precautions. Here is the flow of how messages are sent using PGP.



[HTTPS] This is the same idea that HTTPS uses. The S in HTTPS stands for secure. That is why people suggest you always use HTTPS rather than HTTP. Even if someone is intercepting your data while you have HTTPS is active, they will not be able to understand it. Tor browser has HTTPS everywhere enabled by default, so you should not have to worry about this if you using Tor. The idea is even though people know you are sending information, they will have no way to read it unless they have to right to.

[GnuPG] The program that is commonly used for sending and receiving PGP encrypted messages is GnuPG, most of the time shortened to GPG. GPG is installed in almost all Debian-based Linux distros, including TAILS and Whonix. It is important that you understand the fundamental ideas behind PGP before you jump into using the commands for GPG. If you do not understand how PGP works, then read other guides. If you want to try using GPG before fully understanding how PGP works, understand that you might get very frustrated. Here is a link to help better understand PGP http://curtiswallen.com/pgp/ . I am going to give instructions on how to use GPG, even though there are lots of other guides for GPG. I have found that other guides are very broad and do not fully explain how to use GPG in a practical way. But, if you want to use someone else's guide, here is a link to a decent one https://www.dummies.com/computers/operating-systems/linux/how-to-use-gpg-in-linux-to-encrypt-files/ .

[**GnuPG instructions]** For you to use GPG from the command line in Linux, you need to have some basic experience with the command line. I am going to mimic what the Whonix command line looks like, but the commands are the same for most Linux distros. To generate a new key pair, both public and private. Type in

```
user@root: ~$ gpg --full-gen-key
```

This creates a window for you to follow. You will have to option to create different types of keys, select RSA and RSA (Default) until you learn more. Then type the max amount of bits for security length. 3072 is good enough for most people, but you know. Then set the key to expire at some point in the future. Make is so everytime the key expires, you create a new identity (Remember chapter 1?). I would recommend three to four months for most people unless you are a vendor. By the way; 1y = one year, 3m = three months, etc. Once you create the key, you should create a revocation certificate. You can learn how to do that here.

https://debian-administration.org/article/450/Generating_a_revocation_certificate_with_ gpg . You do not have to use any real information for a GPG key to be generated. You do not even need a valid email address. But, it is recommended you use information that matches your pseudo-identity. A big part of PGP is trust, someone can easily fake being someone else. So, put information that matches your pseudo-identity, but obviously not your real identity. Then make a really strong password that you can remember. You will need it to sign and decrypt messages. Then your key pair should be generated after some time.

Your fingerprint gets printed out after your key pair is generated, but this is not your public key. People can use this fingerprint to look up your public key if you submit your public key to a database. You can learn how to export your public key to a database here https://debian-administration.org/article/451/Submitting_your_GPG_key_to_a_keyserver . Understand that commands may differ for different OS's for exporting keys. To actually print out your public key that will send to people from the created key pair, type...

```
user@host: ~$ gpg --export --armor [user]
```

Where user means: Name, email, or fingerprint correlated with key

Armor means: Human language

It is important to use armor, because if not GPG will print out a string of code that can not be used for anything practical.

This is the key that you can send out in the open air. I mostly communicate with people over email, you can send this as the first message to someone. Say someone gives you their public key, you can import it by using...

```
user@root: ~$ gpg --import
```

Then paste the public key into the terminal. Once pasted, leave a blank line, then press ctrl+d to exit back into the terminal.

By this point, you have your public key, your private key, and the other person's public key (Let's call them Alex). Alex has his private key, his public key, and your public key. To send Alex a message, you need a message to send. To create a message, you can open LibreOffice and type your message there. Or you can do type it from the terminal. If you want to save the message, use...

```
user@host: ~$ nano [filename]
```

Then type your text, afterward use crtl+x to exit, y to save, enter to exit back to the terminal. To encrypt the message that you just wrote, type...

```
user@host: ~$ gpg --encrypt --armor [filename]
```

You will be asked to choose the recipient(s). Type the name, email, or fingerprint that belongs to Alex's public key. Afterward, a new file is created with the same name of the old file but has .asc subfix. To read the message, type...

```
user@host: ~$ ls
```

This will show all the files in your current directory

```
user@host: ~$ cat [filename with .asc]
```

Copy the cat output, this is what you will send to Alex. You can send this encrypted message to Alex by whatever means, but I always recommend using email.

If you do not want to save the file, you can do that easily. Just type...

```
user@host: ~$ gpg --encrypt --armor
```

Then choose your recipient(s), and press ctrl+d when done. Copy and paste the output to send to Alex.

Something that to understand is you will not be able to check if the message was created correctly. Since you encrypted the messages using Alex’s public key, you would need Alex’s private key to decrypt it. Since only Alex has the private key, hopefully, then no one else can decrypt the message.

Once Alex reads your message, he can encrypt his own message using your public key. Once you get the encrypted text, type...

```
user@host: ~$ gpg --decrypt
```

Paste the encrypted message, then your password that you made earlier. Then the clear text will print, and you ready to create a new message for Alex.

Those are the basics of GPG. Once you understand how to use these commands, you can do research to learn what else GPG has to offer. You can use GPG anywhere you can send messages, but I always recommend an anonymous email. Also, GPG can be used for verifying signatures and creating your own signatures. By the way, once you learn how to verify signatures, I would recommend reinstalling everything you have downloaded. You would not want any backdoors installed on your software before you go and do important private business. You can learn more about signatures here https://www.gnupg.org/gph/en/manual/x135.html .

[**Trust]** As far as knowing who to trust on the internet, mainly talking about the darknet, I can not tell you who to trust. Everyone has different needs for their levels of trust. This is where having good common sense is key. Even if no one outsiders can read your messages, what if you are directly messaging the adversary? Here is a link to the mentality you need when trusting criminals https://motherboard.vice.com/en_us/article/ezvk7p/darknet-drug-dealers-have-a-trust-problem-and-they-want-to-fix-it , and here is a link to explain and help avoid honeypots https://darkwebnews.com/dark-web/how-to-avoid-honeypot .

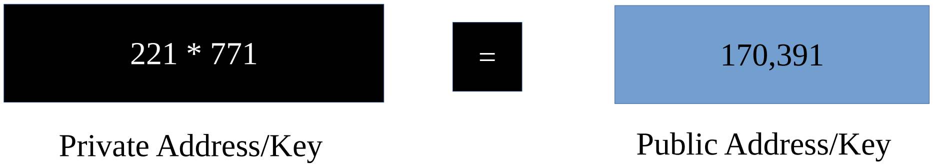
Chapter 4 – Buying Anonymously

So there are a lot of steps you can now take to become anonymous on the internet, but there is something else you have to worry about. Adversaries can follow money and item trails that you leave behind when you buy something. Most of the time, this could be your bank account when you use credit/debit cards. Trying to handle national currencies in a way that is anonymous can very difficult. In order to try and keep purchases anonymous, cryptocurrency is what we will be looking at. While most cryptocurrencies were not made with the direct intention of being anonymous, we can use them in a way that is.

[**Crytography intro]** Before I begin talking about Cryptocurrency, I first want to talk about Cryptography. In the previous chapter, you learned how to use public and private keys to communicate. In this chapter, I am going to teach you how to use public and private addresses for Bitcoins wallets. It is very difficult to learn a private address/key, given only the public address/key. But, you may be asking why you can not get a private address/key from a public address/key. Well, allow me to ask you a question.

What two numbers multiplied together give the number 170,391?

The reader may have a very hard time factoring 170,391. But, if you were given the original two numbers, you can easily multiply those numbers together to get 170,391.



This is grossly simplifying how cryptography works, but you can really understand why you would have a very hard time getting a public address from the private address. Yet at the same time, you can easily get the public address given only the private address.

[**Crytocurrency intro]** When it comes to using cryptocurrency, there are many different types of cryptocurrencies that you can use. Exactly what different forms of cryptocurrencies are digitally, and how they are mined is out of the scope of this paper, but you can learn https://en.wikipedia.org/wiki/Cryptocurrency . My goal in this paper is to explain how to use Bitcoins anonymously. I have chosen to use Bitcoins because they are the most universally accepted as of the writing of this. There are cryptocurrencies that were made with privacy in mind, a such as Monero. If you want to learn more about Monero, you can do so here https://ww.getmonero.org/get-started/what-is-monero/ and here https://www.youtube.com/channel/UCnjUpT9gGxyQ_lud7uKoTCg/videos . As I said before, this guide will be focused on Bitcoins. But, you can always use the knowledge you gain from this guide for other cryptocurrencies. Once you learn how to use Bitcoins, you will better understand how to use other forms of cryptocurrencies.

[**Bitcoins]** So bitcoins, similar to traditional money, is a fiat currency. It only has value because we as a society say it has value. And bitcoins are stored in a "bank" similar to how your money is also stored in a bank. But there are differences. A normal online bank is basically only good for managing your money. It moves money from point A to point B, where the money in your account relates to real life money, a physical object. Bitcoins are stored in wallets, where you do all the movement yourself. Bitcoins have no real life physical object that relates them to the real world, but they relate to a mathematical equation. So math represents bitcoins. That is why there is not an unlimited number of bitcoins because the equations to generate them are getting more complicated as more are made.

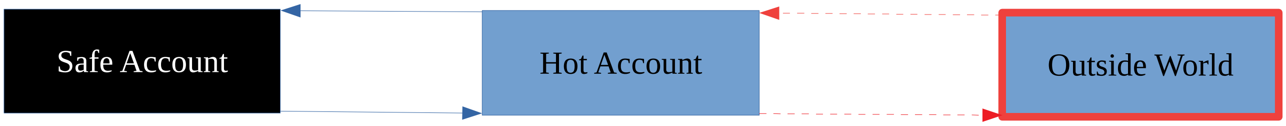
[**Bitcoin wallets]** The way that bitcoins can be sent and received are through bitcoin wallets. A bitcoin wallet, like a bitcoin itself, it based off of math. So math tells the blockchain, the central hub of bitcoins, how much money there is in a wallet. Unlike a regular bank, blockchain has no power over what happens to bitcoins. The blockchain is only able to view where bitcoins go. This is why you have so much control and at the same time vitality. People know that their wallets have received bitcoins from your wallet because of the blockchain. In order to be able to use Bitcoins, you need to understand how to use Bitcoin wallets.

A Bitcoin wallet has two different parts, the public and private address.

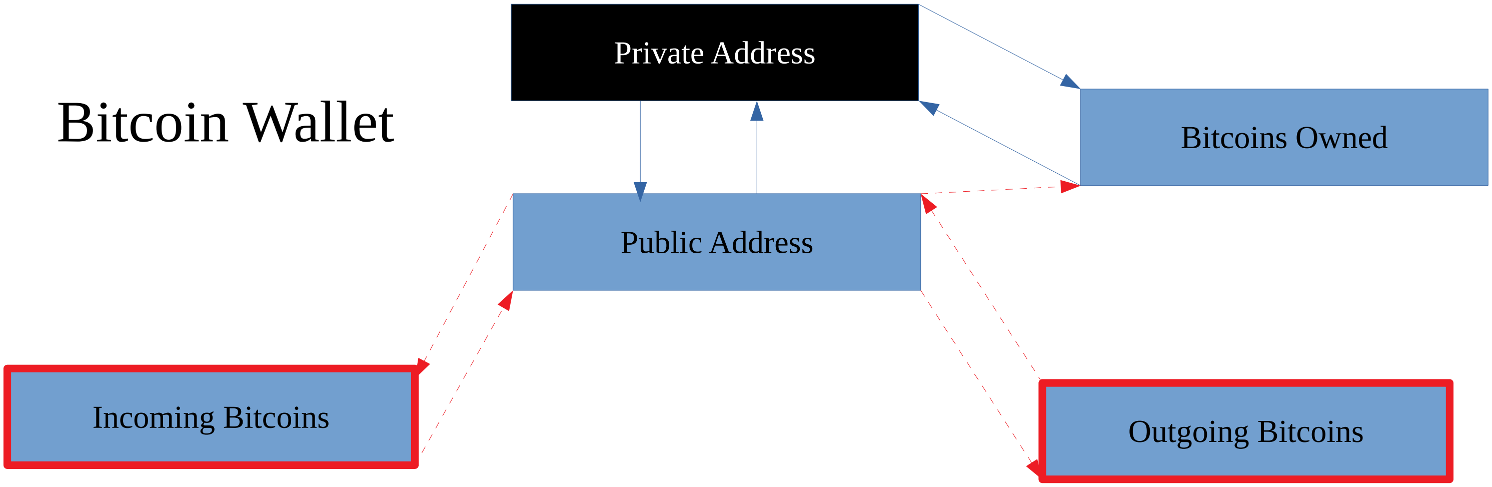
A Public address with look like: *1M9ZBp9L5iYkZVehEmNoDUkes8P67B4kR1*

Private address: *KypQgxiqpJHRAo2Fdqaccaiqd5nmkvAvd1BRfMkrNEkWtCBFsdRG*

The public address is able to receive and send bitcoins, and nothing else. While the private address has full control over all your bitcoins in the wallet. Trying to use traditional banking systems does not truly paint how bitcoin wallets work, but they can be used to try and get a vague understanding. So imagine you have two banks, just for yourself. One bank is strictly for moving money. Whenever this bank account gets money, it will physically and secretly send it to your second bank. The second bank stores all the money and can not be reached. Then when you need to send money back out, your second (and secret bank) will send the money back and your first (public bank) will send the money out.



This idea is not a complete presentation of how bitcoins wallets work, but it helps to paint the idea of how the public address and private address are used in a bitcoin wallet.



Something to note, you can tell how many bitcoins are in a wallet given only the public address. So this can make certain wallets a target for adversaries.

Using bitcoin wallets has a lot of security, but can easily be compromised. If you ever lose the private address, you will lose all the money in the wallet. Because an adversary can use that address to send all your bitcoins to their own wallet.

[**Hot vs Cold wallet comparison]** If you are wondering how you get a bitcoin wallet set up, there are two different "types" of bitcoin wallets. You have hot and cold storages. There are many different definitions out there for what is defined as "hot" and "cold", with some even creating the term "warm wallet". In my mind, there are better words to use, "liquid" and "frozen" wallets.

[**Liquid Wallet]** For the purposes of this paper, a liquid wallet is one that is connected to the internet. This could be an app or program that helps manage your bitcoins. Liquid wallets have their benefits, you can easily remove and add funds to them. Also, they tend to be simple. You do not have to worry about a private address at all with liquid wallets, only your public address. You tell the program where to send the bitcoins, and it does all the hard work for you. Then when someone sends you money to your public address, and it gets added to your total. A personal favorite liquid wallet of mine is Electrum https://electrum.org/#home . Electrum is pre-installed in TAILS and can be easily installed in a VM inside of Qubes.

[**Frozen wallet]** For the porpuses of this paper, frozen wallets are wallets that are kept offline. Frozen wallets are much more secure than liquid wallets. Cold wallets are always made offline and kept offline. You are able to add funds to cold wallets, and there is no trail that adversaries can follow to reach your funds. Then once you are ready to "withdraw" your funds, you can move the Bitcoins to a liquid wallet.

Think of a frozen wallet as the spot under your mattress, and a liquid wallet as a bank.

[**Hot wallets cons]** The drawback form a hot wallet is that since it is connected to the internet, there is a trail for an adversary to follow and find a way to steal your bitcoins or trace them to you. There is no such thing as "hacker proof", believe me on this one. But there are different risk levels with hot wallets. Some factors are: how much money you are keeping on it, what service(s) is(are) running the wallet, what do you buy with the bitcoins, and where do you get bitcoins from are some. Your risk level could be really low or really high depending on the answer.

[**Frozen wallets cons]** The downside with frozen wallets is their lack of mobility and that you can easily lose them. Since frozen wallets are to be made and kept offline, then that means you have to keep them in a place that is not connected to the internet. A good place for this a sheet of paper. If you print out the wallet addresses, however, then there is a chance that your printer can save your data. This gives a trail for adversaries to follow. Thus make the wallet not a frozen wallet by the definition as stated earlier. This means you have to *write* down the public and private addresses to your wallet. And, you make sure that there never a connection to your private address and the internet. You do not even want an adversary to know you even made this Bitcoin wallet, in theory. Plus, frozen wallets can take a long time to generate. That is a lot to ask and make cold wallets not a popular choice for many people.

[**Gernerating Frozen wallet]** If you want to make a frozen wallet, however, you can create a frozen wallet on a website such as http://www.bitcoinaddress.org/ . If you want to create a frozen wallet on bitcoin address, select the brain wallet option, then go offline. You will have to use Javascript for you get a Bitcoin wallet set up, so I would recommend using a live OS. Any live OS will work, but I would recommend TAILS. Then make sure you generate the wallet while offline, and do not reconnect to the internet after you generate it. Only reconnect to the internet on the live OS after you restart your computer. This way the wallet is not stored on your computer nor found anywhere on the internet. A brain wallet is a bitcoin wallet that is generated using keystrokes that are human-made and converting that into a wallet using a hash algorithm. So, in theory, an adversary could try and brute force wallets with weak "passcodes". You do not have to remember or write down the passcode, it is only used to generate the wallet. So you should make the passphrase really, really long. This means no adversary can know that you ever created the wallet. Then write down your public and private address. You want there to be no link to the internet and this wallet. Well, you do not want a link for the private address. When you write down your wallet, make sure you can tell the difference between your characters. For example, be able to tell difference between 0/O, b/6. g/q, I/l, etc. The last thing you want is to try and withdraw your funds, and not be able to re-type the private address. Bitaddress has an option to test your private address, so use this to make sure you wrote down your address correctly while you are offline. Then you can use liquid wallets to transfer funds to your frozen wallet, and no one should be able to track down the frozen wallet. Then once you are ready to pull the funds out, you can sweep the frozen wallet into a safe liquid wallet.

[**Imporance of Bitcoins]** Bitcoins will play a large part in staying anonymous, it is important you understand how to use them. If what I used to represent bitcoins wallets does not make sense to you, find an article that does a better job than me for you. I am going to say again, make sure you really understand how bitcoins work. Even if you do not understand how anything else works in this guide, but you are following instructions, make a valid effort to understand bitcoins. You can learn more general knowledge about Bitcoins here https://bitcoin.org/en/getting-started .

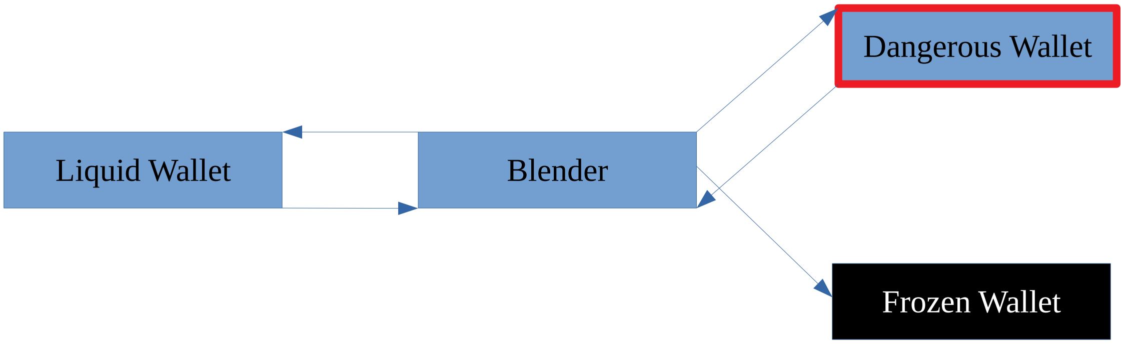
[**Bitcoin Blockchain]** If you remember, there was something that I mentioned that was cause for concern about bitcoins, the blockchain. If you want to learn how adversaries can follow Bitcoins using the blockchain, then you can learn here https://bitcoin.stackexchange.com/questions/12427/can-someone-explain-how-the-bitcoin-blockchain-works . How can bitcoins be anonymous if an adversary is able to view exactly where all bitcoins go? There are a few different ways to fix this issue. Option 1, get bitcoins in a way that does not leave any traces to you. Option 2, use bitcoin blenders to mix your coins with other people's coins to make tracking very hard. Option 3, use option 1 and option 2 at the same time. Guess what we are going to talk about, option 3.

[**Anonymous Bitcoins]** You need to ways of getting Bitcoins in order to use Bitcoins. Most ways of getting Bitcoins are by trading other forms of fiat-currencies (such as USD) for Bitcoins. While this sounds good, very few websites offer services that allow the user to get Bitcoins in a way that does not identify them in some way. One popular Bitcoin trading website is https://localbitcoins.net/ . But the issue with websites like Localbitcoins is that they are centralized. They require you to sign up for an account to keep track of how many Bitcoins you have in your liquid wallet on the site. This does not mean that they are trying to strip you of anonymity per se, but it does leave a trail for adversaries to follow. If you leave any personal information behind when signing up or using the service, you would be compromising yourself.

[**Bisq]** There is a solution to this problem, decentralized networks. A service that was designed to keep your anonymity is Bisq. The goal of Bisq is to never leave any trails of your activity on a server somewhere. You do not even need to sign up when you use Bisq. Also, everything you do in Bisq is peer to peer, many of the times face to face with cash. I would recommend the funds you store on your frozen wallet to be swept into the Bisq since you can anonymously trade them. Here is the link to Bisq's website https://bisq.network/ .

[**Bisq cons]** But, Bisq is not perfect either. The same reasons why Bisq is good for some people is the reason why it is bad for others. Everything that you do with Bisq is stored on your computer. You can create an encrypted VM with Qubes that is only used for Bisq, but this is not an option for everyone. Some people who have to only use TAILS might find Localbitcoins to be better since nothing has to be stored on your computer. Also, Bisq requires you to have a certain amount of Bitcoins upfront before you can use their service. The reason for this is because you are so anonymous when using Bisq, there has to be a security deposit for trust to be built between sellers and buyers. If the seller or buyer breaks their end of the trade, then all security deposit funds go to the victim. But, since Bitcoins are required upfront, it can be difficult to get the starting Bitcoins in a way that is anonymous. Bisq explains alternatives on how to get the startup Bitcoins and many other things on their FAQ page https://bisq.network/faq/ .

[**Tumblers/Blenders Pros]** So once you have your bitcoins, there is a reality that you will have to face. There might be some trace between you and the bitcoins you bought. Even if you got bitcoins in a way that there no way to trace you, you do not want to take chances. Say you have found a marketplace that you do not want people knowing that you are buying from. Marketplaces have their own built-in liquid wallets that you send your bitcoins to and from to buy and sell things. So to keep your bitcoins clean, we can “laundry” them similar to how the Mafia laundry’s their money. There are services, even some hidden services, that are blenders to mix your bitcoins. So first you send you bitcoins to the blender, the blender “mixes” your coins with other people’s bitcoins, then sends the desired amount to the target wallet.



This way there should be no link between you and the marketplace wallet. Also, this is how we are going to send funds to our frozen wallet that you made earlier. If you have funds that you do not want to be compromised, use a blender to keep your identity away from the frozen wallet. Once you are ready to move funds out of you frozen wallet, most liquid wallets provide a way to sweep fund from a wallet given the private address. This is why we want to keep our private address safe.

[**Tumblers/Blenders Cons]** Even though blenders are a beautiful thing, there is still a level of trust that needed with blenders, also known as tumblers and mixers. There is a chance that the blender does not mix your coins at all, but just moves them around. Plus, there is a real chance that a blender might be a scam, and just take all your Bitcoins without giving you anything. Also, almost all blenders charge a fee for their services.

The fees can range from 1% all the way up to 5%. The very large fees can turn people away from using Bitcoins blenders. If you are interested in using blenders, however, here is a list of mixers https://bestbitcoinmixers.com/ .

[**Receiving goods intro]** When you buy something while trying to be anonymous, understand that there will always be risk associated with your purchase. One is where you are sending your items to. Say you were messaging an adversary about trying to buy guns. The adversary can just show up at your house and begin to question you. But, Let's imagine a scene.

> You are a politician and you want to get rid of the competition. You do not want to get your hands dirty, so you send guns and drugs to their house hoping to get them arrested. Even after the packages make it to their house, you still see your competitor on the news making speeches. So you leave an anonymous message to an adversary ratting out your competitor with detailed information. The next day, however, you see that they are still making speeches. How?

There are laws in place from you being incriminated from someone else sending you illegal items. If you never bought the items that came to you, why should you go to jail? This is the very point I am going to make. If there is no way to prove that you bought what came to your house, then you can not go to jail for it. So even if an adversary comes knocking on your front door and begins to question you about a package. Do not confess no matter what they might tell you. It is not your job to prove your innocence, it is their job to prove you guilty. If you decide to buy something of a questionable nature, it is very important that you buy it in a way that can not be traced to you. Even if you try to deny you bought a package, if an adversary can prove that you did then you have no plausible deniability.

[**Location for goods]** If you do buy something of questionable legality, make sure you can have plausible deniability. Do not ship to an abandoned house where you have no explanation for being there. Also do not look too eager to get a package. Where you ship your goods, I would recommend your house or a postal box, ship other items there too. Buy things off of Amazon or eBay. Make this package look like any other package. So if an adversary were to question you, you have the ability to say you thought it was another package that was supposed to come. Have good reasons for why you are doing what you are doing. Even if the adversaries do not believe you, do not confess. Assuming you followed <u>all</u> the steps above, there is no way to prove you bought the package. You may be in an interrogation room for 10-12 hours, but that is a short time compared to 10-20 years behind bars.

If you are worried about the police as your adversary, I would recommend never talking to the police unless you have an attorney. There are some parts of the world where this is not possible. So really understand the risk when buying things of questionable nature in your area. Understand I am not condoning the purchasing of illegal items for self-gratification or to harm others, but only to help others. If you do *not understand how illegal items can be used to help others, then do not buy illegal items. Illegal items that are used for selfish reasons are addictive, and will eventually catch up to you.*

Epilogue

Assuming you follow everything that this guide has to offer, you anonymity should be mostly safe. But understand that nothing is perfect in this world, and anonymity is no exception. As time progress, everything I have said up to this point might be void. So do not rely on this guide for perfect anonymity. My job is not to tell you what to do with the information I give you, only to provide you with tools you will need to stay anonymous.

If you have any questions, comments, or concerns, you can email me at the addresses below. Also, use my public key (found below and on Reddit) if you message me. I will not respond to any unencrypted messages. I have given the right to everyone to modify and distribute this document since I am not looking for profit or credit. But, if you want to make sure the document was not modified, you can use the detached signature to verify that was provided at Reddit (Waiting until final release before adding a signature).

Stay safe, stay anonymous.

Hidden Service Email: Anonymous43217890@torbox3uiot6wchz.onion

Clearnet Email: Anonymous43217890@protonmail.com

If you wish to donate to me using Bitcoins, you can do so here

12VDS9nAMR8y4PBamzAdCbxaKLFCQmWupH

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFwlXOcBEACwy7Kq2igs3kJ8w9ALTAWCFCSJpYF4MLGlPGPyVYIxAJ/IY+Qf
cPL6g5vPxUccBnTK/peAbhowf3xmu34fk6ix0OcwKDf0q9AKjg37fpjNDsHnI0uZ
44KuY5J2UviESsR71DF69uilfeiFhQdSEwRpkGKDlXyPKjUp/7AyVSzqzE2Ot+0B
nvc5dYNf9UkT8nmz7KYzacoeJCQElYqMvK0bak8kVvblVwwOrN897AuyyzxSh5eq
iuxkupYN7DAwmNWeJpUHZJGi7Qbfkv8wCyGlqwlFVshRWWtwUUxVVwxVJtxK/ZPc
Yyl090B8ejNagxN61USRnrAt9uhkHLTvsFIFU1MQ9X6CkG9D28FlMgZBo695lEjg
eXPWGzn9f+AP8WRMDWmKauHI1mnPZd+AaS7N3+o3zLyyZJyCzBm2I8FN3Dv8SWze
fdP1nKhm/UZjLB3/xWlpF7TbO6oTDDTk2J/pUqIm29cgrLqzht21QCFFxRvNZRym
CkvslNefZ06DvT7fMiAlKKljjUcyeoBW/mpIRp3J46oulT60fO4turkl78cDfWhh
AGuLGoItniD+fPaBxfqs3oMaT0y/aVlbQib1HXAOKlYGBv9N5nIrZTekTKjDXCGH
HfpHysK8WYJMPZjxVPHzy8Xr6V/Tmn/g3I7RPG+vKA3/vENq4PTO5Ivs+wARAQAB
tH5Bbm9ueW1vdXM0MzIxNzg5MCAoRm9yIHBlb3BsZSB3aG8gd2FudCBtb3JlIGlu
Zm9ybWF0aW9uIGFib3V0ICJHdWlkZSB0byBBbm9ueW1pdHkiKSA8QW5vbnltb3Vz
NDMyMTc4OTBAdG9yYm94M3Vpb3Q2d2Noei5vbmlvbj6JAk4EEwEKADgWIQTjIaKD
NCESn/i5YDQS2FJUWXWSAAUCXCVc5wIbAwULCQgHAgYVCgkICwIEFgIDAQIeAQIX
gAAKCRAS2FJUWXWSALcsEACr/YNVQJ2DG9ZhCOWMHpA7TAj5y850kMtVH94aNrOm
9oJ8/Y0hLPs8SidKjYhM5QH45OneW9KI4RjmV/kRt27Qz38V3E+icapysht0Vh7S
7lSicznqFpolFC65nbr0wYBF5f9wUFljWlsqZfu0o2yI3lojfro66ypgG0ovU5ww
xoQJqE/s+WVjghTVwjG4co2M3t/+xSD1yldHB7/bD7VqHsSwwm51iU8YOGHYuvAV
tJPl1eZbKR44X/wAyas//kMu44iVbWjgEDLsnW31QVIKL6UmGn+o1qRVzKZlQNVe
Gb3vwTYTmKkwxOW04l7r+wKTpb2mX9KH5xrL5+kNq/FXoeTo5oXtMZZyvj9CD2Zm
5s+aX6YYF65uV+DpCAzcT094DZPjLdG3YtNnvXuN7Rd35DROCnAZMx7luQtt4g+n
0CL/9p1sn8XmOaQVUDp7zK1Fc7BMZKFNv4/geGlDXwUhRHCwjjk+7JsKewe9FR8/
B7RMA/nbcuvfyocasvj5rs9tgPIgVKGy0qqVnwdiiU8u4iWHnKtsIdpgvMqNnBAM
NM17d6H+uNEWQHTjLt+RxCykCACg2Ej57DDuXHvH0XPM2SQdnsxqJvf7H31jLYQ9
FszBwp52j2Zt4zXTlSNS2LOYM6GE/ToFqyDiPlgJJp5GR+XZLcpyyD05xHn2Sane
97kCDQRcJVznARAAoO8DK7rZLw84b/5gYxgFZIXuBPOsMlMnH7Eb1BKTx/rXS1qz
Kc6E1DHQSonMdEu0tdJpwup+w1acLc9/ncLdMsCqc/ubVc/k64l/02mEKkAQ3jAG
cL8AG768GHSKZg6n0FohARv5nfNuQ/uFhFVT4hfJKFXFNhkjH6CXzT0omkDKlrzZ
8cRxNWyefsndSGDTQfmKZSl3Zhkjm+hpvB0rIW1Ht4GVNjERwuLtKD0PWNh9ak6a
4Np2Ux5rHyyHjNGmYBlmtJy+v4AQVF+PKP4eJzm2fAWMM2Wj1adQbYfOsmNY7Yp8
/I7nVt5/6N8VNMSjDEQTRdlrX6abcyVTFgCAJAnlJfpbfNyYeELyZuNeMFb76Msp
rpGp2BxHLVaX0MJ8zZx8ovllYG1d8H2aduyoL+U9gJzO9P6j8hp3FSN79uLWEa0o
g/2YVyq0HAjWv1WOi3nx5Y2mYh/JwT89OF/O2CyzFd712eIb8+9u8LIgTlut+BTr
O3QHr33fwTDUAzZduUGLXUoHgXo1NPttdcg9V7EN/OgI/GhcgXEzccNLZgHHrcuq
PtOrn3uOfzUVzySyXllrtB50HG/zQkeS0uFYJmzXeIw0jkBYZ+0leT/OZFAhN8H9
EsVzxJUlzQeectz20ANQ+YGCLktxEamz5BBtwCayYejXKtMUxrKqgwa6czcAEQEA
AYkCNgQYAQoAIBYhBOMhooM0IRKf+LlgNBLYUlRZdZIABQJcJVznAhsMAAoJEBLY
UlRZdZIAZYEQAJfHG0W1qxnPldInCOgDK/qMp/mox6MrxhA0yHZir1UjmfQwr/hB
xOpWf/ZcMMqEB0KV0udBrPdiF6Xxe+ApLUnRF8CQQoZIZZPFgWalRs35qPJYY6MG
9jUU3xEgv8QKkQ7akFx3eZ+x+/IEgQ1z8ttKuD8BDqr17cEF71nKv3eysKBx/IMx
ZOYfwCzzsyy4ikJAQLtY/Yj8t7HA+dI4oxVtuwh3r9F849U835/xc+Bos7MS9Jmm
zI1qThd5LwA/E7o266ZaFYe6OJu8mqz866MZW3STNIBvofAJSamt8Ot4b+dUSME8
R51F1nc2ftcDIHhq1OD1rNE0/+7j78mk2duVEs2hE+EHc2qwZSivTU/H/KQWFlZa
Ph6L9cvgiQb/UIQajanZ+4a7gqcDh6Z3EK1NpvIBh8tohosEtqqTODYmJ6ANqLYG
OWfA4R6fY2s6Q2bPqLIgT8KAmTBtX6NO/cZ8nF2p5ZytYY7qs4bHASJDUUCFwqp2
h/PA5pAKoYaq1f7kVOQfMtqAufUNn155S/TeHNTRCh7mDVicmc3ouWJZRTZekqfU
gvi+0Yyl49oPkOJbvFSd0twFYsIzYjfhCFPhvWcj1jw9p/O9mv/70gRCipEhwD6W
zX9vlhfp/1cb47DOl5XwLIGeErn9S5gn5Asrh7pQqKrItrO7/5fvdwPU
=WxJV

-----END PGP PUBLIC KEY BLOCK-----
```