




An abstract graphic on the left side of the book cover, consisting of white lines and circles on a dark blue background. The lines resemble a circuit board or a network diagram, with several vertical lines and many horizontal and diagonal branches. Small white circles are placed at various points along these lines, some at the ends and some in the middle, creating a sense of connectivity and flow.

# ANONYMITY

ARLETA JUSZCZAK



# AGENDA

- Anonymity vs. Privacy
  - Pros and Cons of Online Anonymity
  - Proxy
  - VPN (Virtual Private Network)
  - Tor
  - Using VPN and Tor together
  - I2P (Invisible Internet Project)
- 
- 
- 

# ANONYMITY VS. PRIVACY

- **Privacy** - ability to control who (if anyone) sees what activities you engage in online (no one is able to see what you do, but they can know who you are).
- **Anonymity** - ability to perform actions without them being traced to the person (nobody knows who you are, but can potentially see what you do).



-PRIVACY-



-ANONYMITY-

# PROS AND CONS OF ONLINE ANONYMITY

## PROS

- Offers Privacy
- Promotes Freedom of Speech (e.g. criticizing laws and government without fear of repercussions)
- Creates a Sense of Security
- Offers Data Security (prevents hackers from getting access to sensitive information)

## CONS

- Promotes Cybercrime
- Establishes Misrepresentations (creating an elaborating online persona)
- Individuals can bully, stalk and libel
- Criminals can seek contacts for performing illegal acts

# PROXY



- The destination server receives requests from the anonymizing proxy server, and thus does not receive information about the end user's address.

# PROXY

- Most proxy servers forward data packets with additional HTTP header fields:
  - **X-Forwarded-For:** *YOUR IP address*
  - **Via:** *Proxy IP*
- High-anonymity proxies:
  - **don't** add such fields
  - are usually paid
- Proxy servers keep log files!

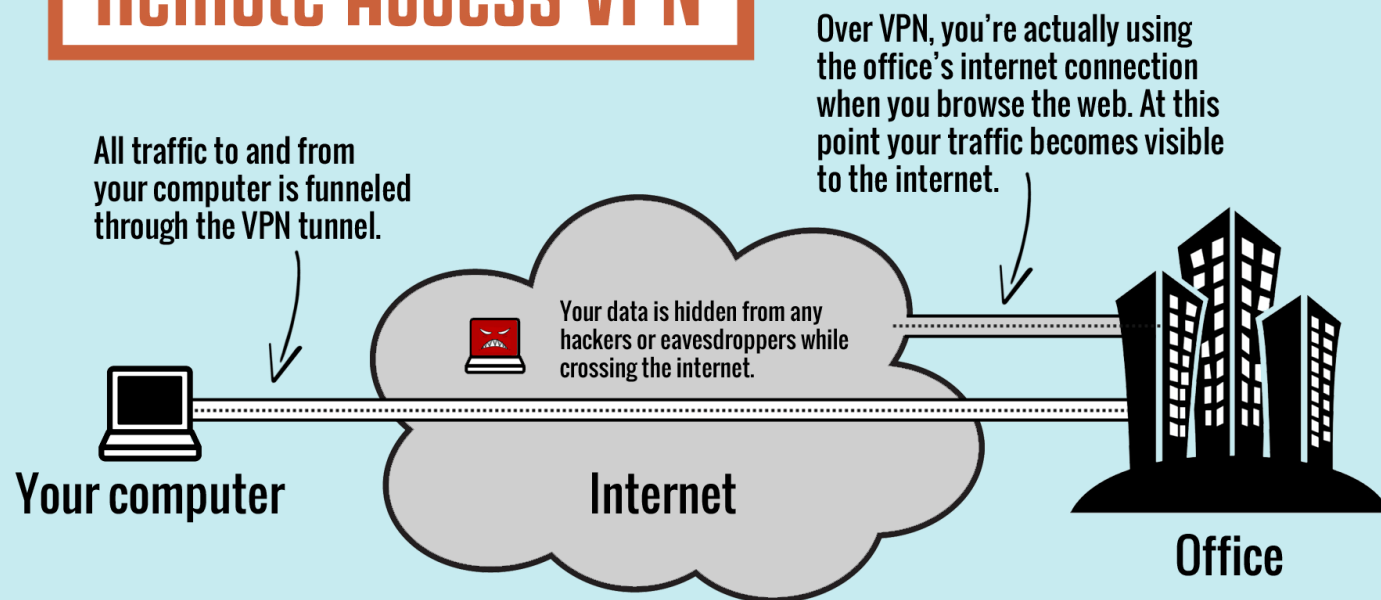
# VPN

- Virtual Private Network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet.
- VPN technology was originally developed to allow remote workers to securely connect to corporate networks in order to access corporate resources when away from the office.
- Although VPN is still used in this way, the term now usually refers to commercial VPN services that allow customers to access the internet privately through their servers.



# VPN

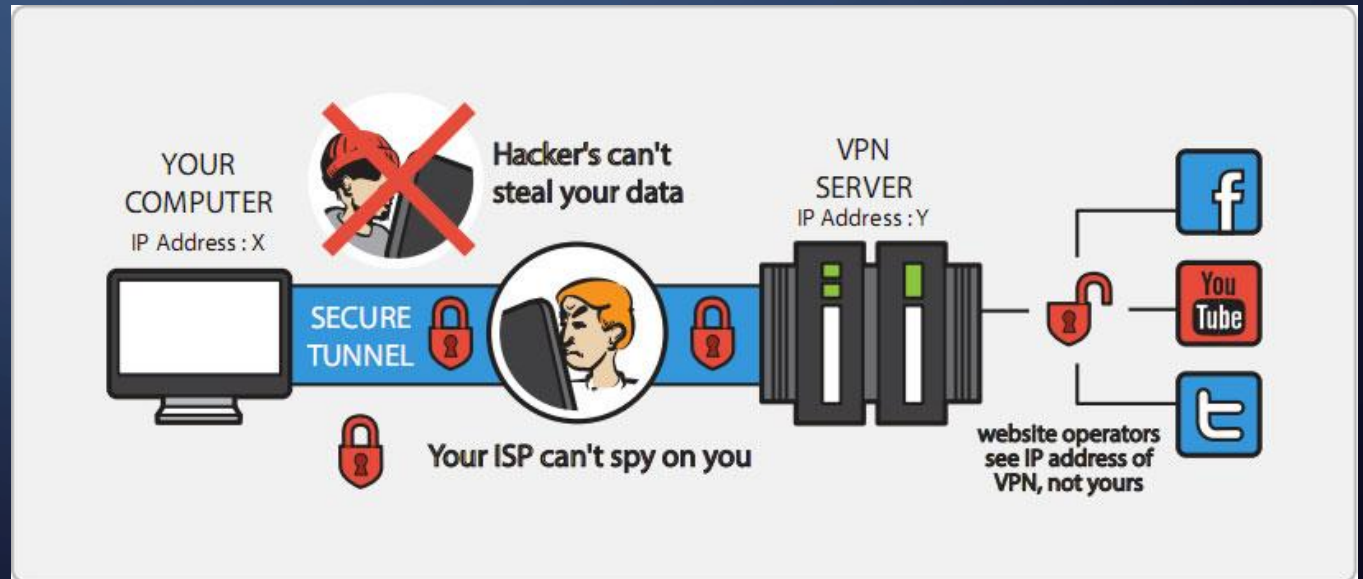
## Remote Access VPN





# VPN

- When using VPN you connect to a server run by your VPN provider (a “VPN server”) via an encrypted connection (sometimes referred to as a “VPN tunnel”). This means that all data traveling between your computer and the VPN server is encrypted so that only you and the VPN server can “see” it.



# VPN PROTOCOLS

- A VPN protocol is the set of instructions (mechanism) used to negotiate a secure encrypted connection between two computers.
- Most common VPN protocols:
  - PPTP
  - L2TP/IPSec
  - OpenVPN.

# VPN PROTOCOLS: PPTP

- Point-to-Point Tunneling Protocol (PPTP) is a common protocol because it's been implemented in Windows in various forms since Windows 95.
- PPTP uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.
- PPTP requires both TCP port 1723 and the GRE (Generic Routing Encapsulation) protocol.

# VPN PROTOCOLS: PPTP

- PPTP Protocol has many known security issues and it's likely the NSA (and probably other intelligence agencies) are decrypting these supposedly “secure” connections.
- *„It's the nature of the MSCHAP V2 authentication, how it can be broken trivially by capture of the data stream, and how MPPE depends on the MSCHAP tokens for cryptographic keys. MPPE is also only 128-bit, reasonably straightforward to attack, and the keys used at each end are the same, which lowers the effort required to succeed.”*

# VPN PROTOCOLS: PPTP

## PROS

- It's fast (the users who opt for this protocol usually prefer speed over security)
- Very easy to set up
- Can be utilized with almost all platforms

## CONS

- Very insecure
- Definitely compromised by the NSA
- Easily blocked (because it runs exclusively on port 1723 and uses non-standard GRE packets which are easily identifiable)

# VPN PROTOCOLS: L2TP/IPSEC

- Layer 2 Tunneling Protocol (L2TP) does not provide any encryption or confidentiality on its own, usually IPsec is used along with that to secure the connection.
- It uses 3DES or AES-256 bit to encrypt traffic.
- L2TP/IPsec encapsulates data twice, which slows things down.
- L2TP/IPSEC uses UDP 500 for the the initial key exchange, protocol 50 for the IPSEC encrypted data (ESP), UDP 1701 for the initial L2TP configuration and UDP 4500 for NAT traversal.

# VPN PROTOCOLS: L2TP/IPSEC

## PROS

- Easy to set up
- Available on all modern platforms
- Usually considered secure

## CONS

- It is easier to block than OpenVPN due to its reliance on fixed protocols and ports.
- Slower than PPTP



# VPN PROTOCOLS: OPENVPN

- OpenVPN is an open source technology that uses the OpenSSL library and TLS protocols.
- It can be run on any port and both UDP and TCP protocols — which makes it extremely difficult to block.
- Due to the fact that OpenVPN is based on the OpenSSL library, it can use all the ciphers available in it, such as AES, 3DES, RC5 or Blowfish, which gives great configuration possibilities.

# VPN PROTOCOLS: OPENVPN

## PROS

- Very secure
- Supports a wide range of cryptographic algorithms
- Highly configurable
- Open source
- Can bypass firewalls

## CONS

- Needs third party software
- Can be hard to configure

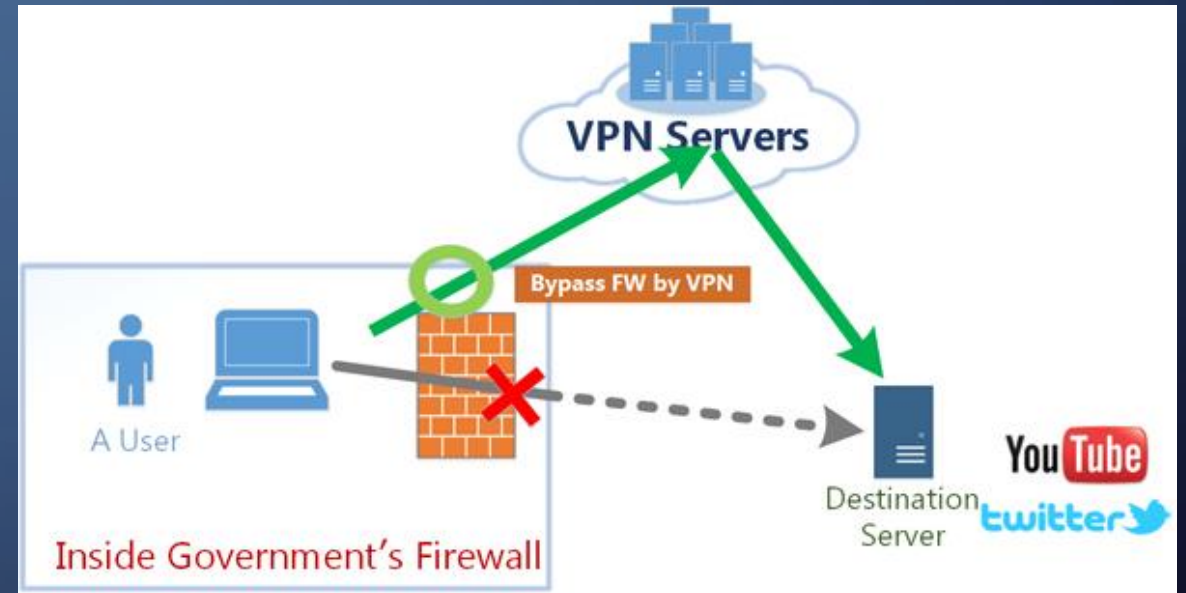
# VPN: BENEFITS

- **Enhanced security.** When you connect to the network through a VPN, the data is kept secured and encrypted.
  - Your ISP can only see that you are connected to the VPN server.
  - It is safe to use public WiFi hotspots



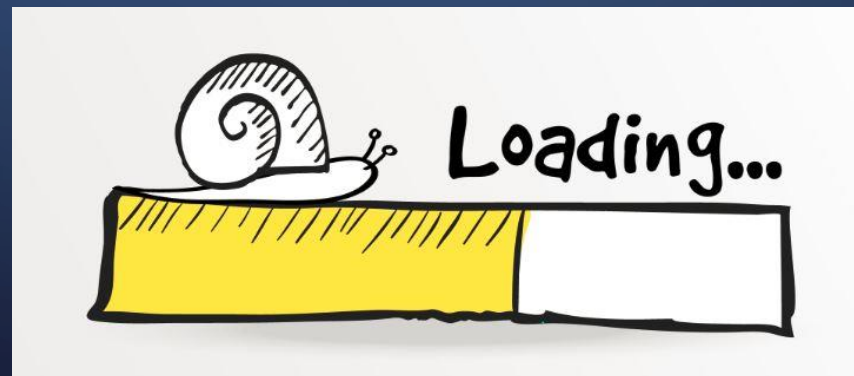
# VPN: BENEFITS

- **You appear to access the internet from the IP address of the VPN server**
  - Anyone monitoring your internet activity from the internet will only be able to trace it back to the VPN server
  - Ability to bypass Geo-restrictions on Websites and Content (circumventing geographical censorship)



# VPN: DRAWBACKS

- **Your internet will slow down because:**
  - Encrypting and decrypting data requires processing power. This also means that, technically, the stronger the encryption used, the slower your internet access.
  - The extra distance traveled by your data (to and from VPN server).



# VPN: DRAWBACKS

- **Your VPN provider *can* know what you get up to on the internet**
  - You are shifting trust away from your ISP (which has no interest in, or commitment to, protecting your privacy) to your VPN provider who usually promises to protect your privacy.
  - In the majority of European Union countries, VPN providers are required by their respective governments to retain users' browsing history over a year.

While your VPN provider may well be promising that their service is anonymous, with no logging, **there is no way that you can verify this!**



# FREE VPN?

- **HIDDEN MALWARE**

Many free services have hidden malware that can steal your data. This can be done by sending you spam emails, stealing your credit card details, making your device inaccessible, or hacking into your online accounts.

**Around 38 per cent of Android VPN apps found to contain malware.**

- **TRAFFIC LEAKS**

Traffic leaks happen when your IP address is leaked out of the VPN tunnel, exposing your identity and information. A VPN is supposed to do the opposite, i.e. encrypt your data. Free VPNs are almost always responsible for traffic leaks.



# FREE VPN?

- **HIDDEN TRACKING**

Generally, a VPN is not supposed to log user data.

But free VPNs not only log user data, but also track your activities online.

Your private information can be sold to third parties by the VPN service.



# FREE VPN?

- **BROWSER HIJACKING**

The VPN redirects you to some other website instead of taking you where you wanted to go. Many of these can also be malicious, and you could end up downloading a virus and infecting your device.



# FREE VPN: HOLA



- When a user installs Hola, he becomes a VPN endpoint, and other users of the Hola network may exit through his internet connection and take on his IP. This is what makes it free: Hola does not pay for the bandwidth that its VPN uses.
- Hola *cannot* control what its users do, so if someone using Hola in another country acquires your IP address/connection and does something illegal, the consequences may fall on you (at least initially).

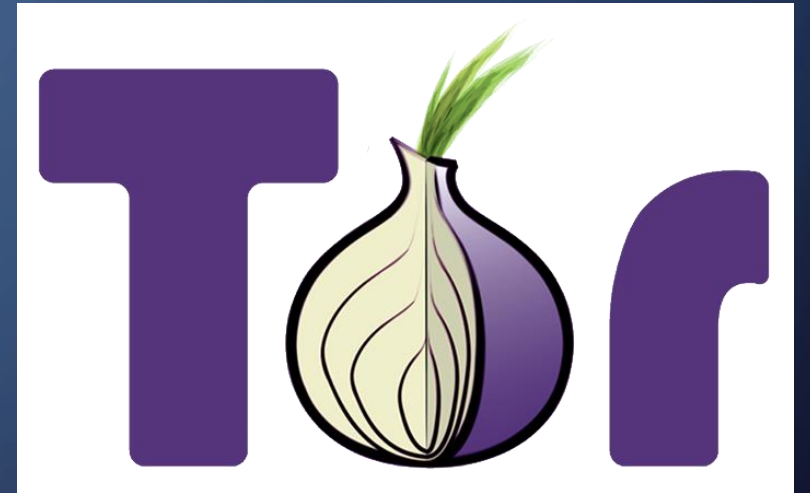
# FREE VPN: HOLA

- Hola sells user's bandwidth through a company named Luminati (which they own): <https://luminati.io/>.
- Luminati makes use of Hola's massive network, which includes over 80 million members. That is a truly huge pool of IP addresses and thus a lot of broadband bandwidth available for rent.



# TOR

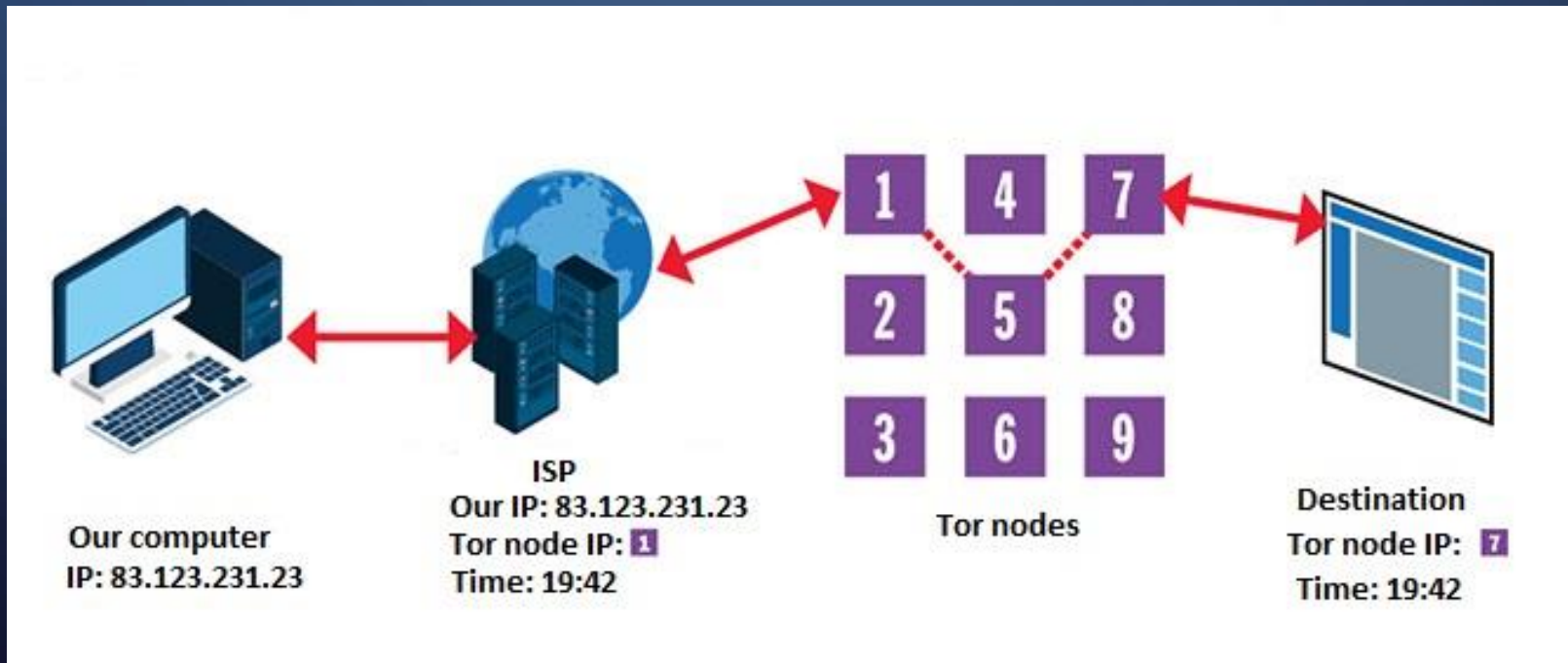
- The Onion Router (Tor) is free software and an open network that allows users to protect their privacy and security against traffic analysis.
- Tor does not prevent an online service from determining when it is being accessed through Tor. Tor protects a user's privacy, but does not hide the fact that someone is using Tor.





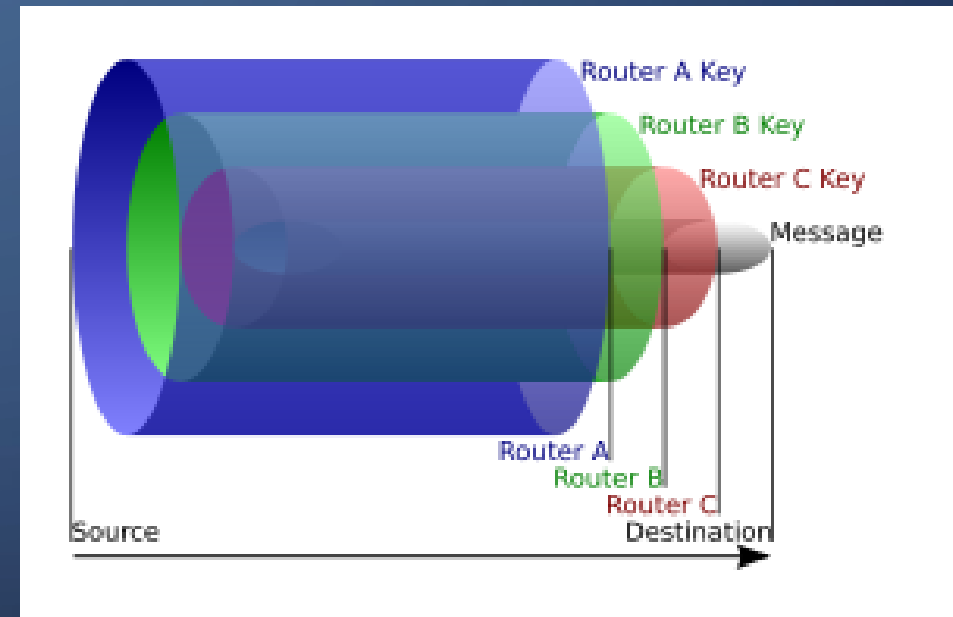
# TOR

- When a Tor user visits a website, Tor creates a **path** through 3 randomly assigned **nodes** on that the packet will follow before reaching the server.



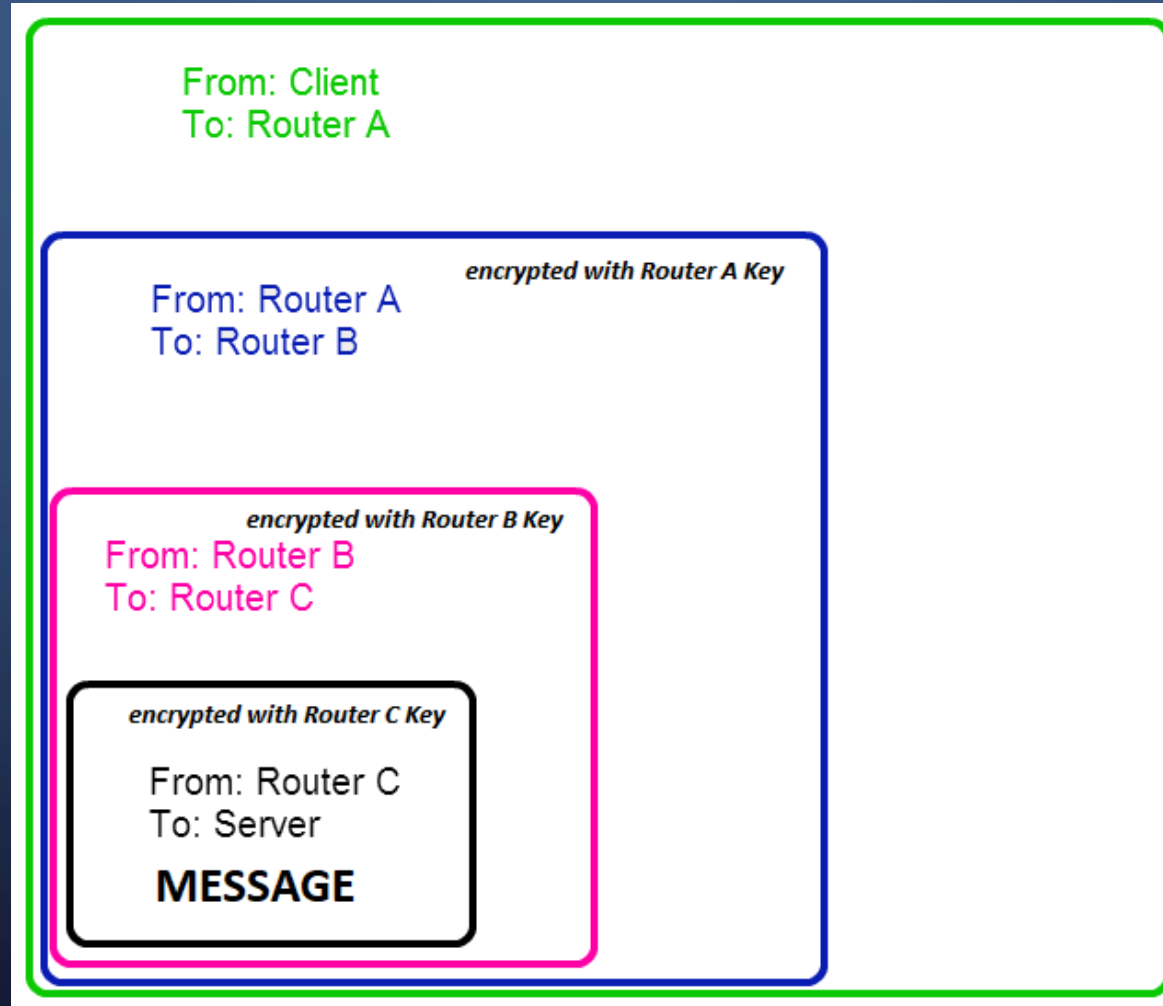
# TOR: ONION ROUTING

- Client selects nodes from a public Tor Node List and gets their public keys, using which it encrypts data multiple times and sends data to first node on the path.



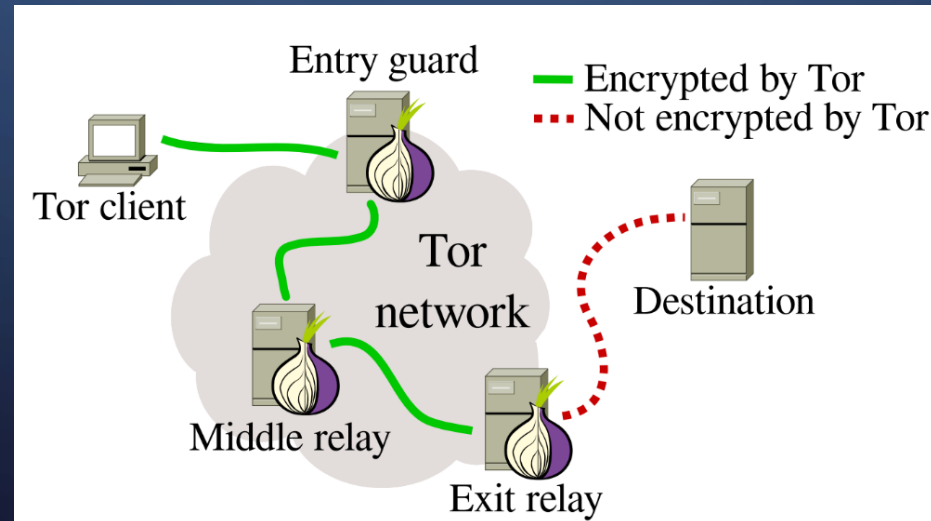


# TOR: ONION ROUTING



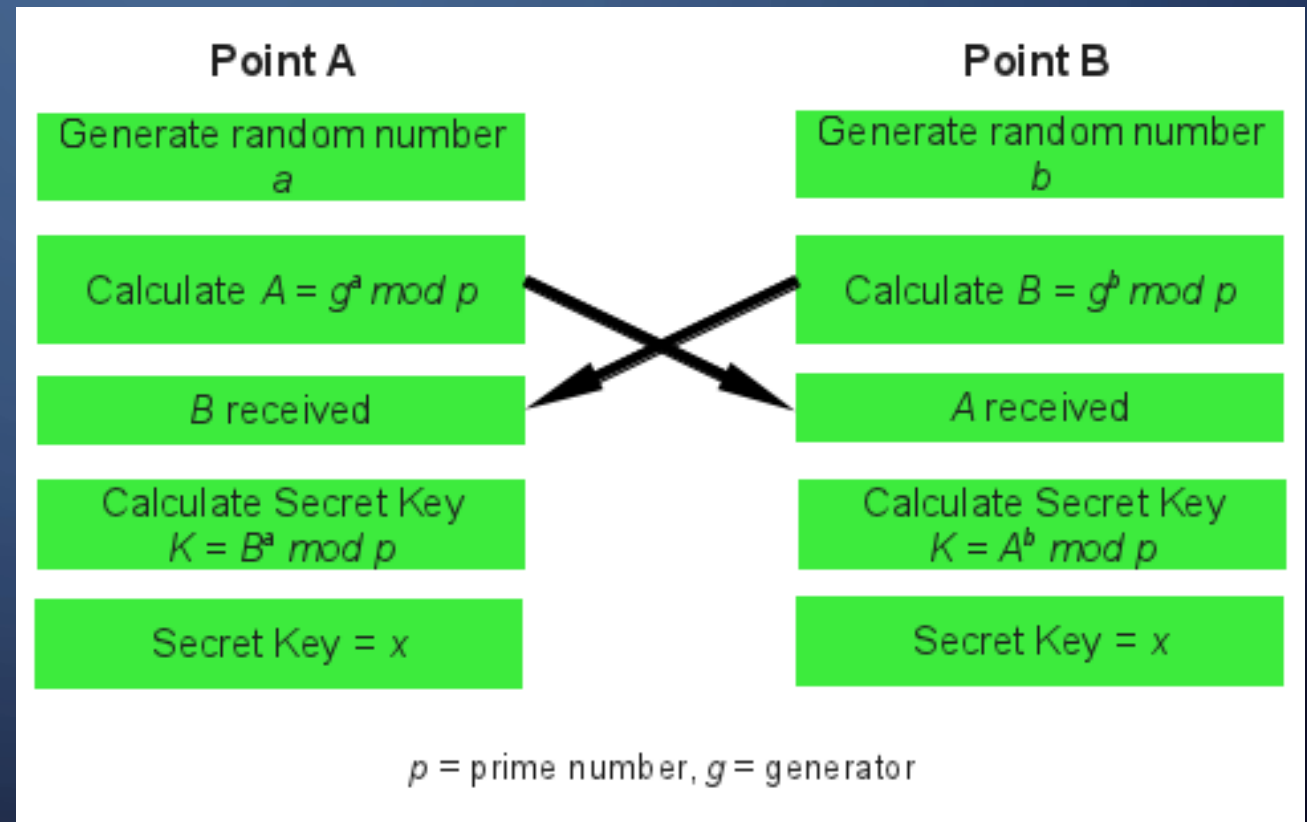
# TOR

- If you use Tor to visit a website that does not use encryption to secure users' connections, then your data packet will not be encrypted when it makes the final hop from the last Tor relay to the website's server.
- So it's best to be sure that a website offers some kind of SSL or TLS encryption.



# TOR: RESPONSE FROM SERVER

- When Tor creates path (randomly selects 3 nodes), it also generates 3 separate shared secret keys (symmetric keys) with each node using Diffie-Hellman Key Exchange.



# TOR

- Tor is a gateway into the Deep Web, the massive portion of the Web that is not indexed by search engines.
- The primary use case for Tor is enabling anonymous access of the public internet (hidden services are an ancillary benefit).



# TOR

- **.onion** is a special-use top level domain suffix designating an anonymous **hidden service** reachable via the Tor network.
- Such addresses are **not** actual **DNS names**, and the .onion TLD is **not** in the Internet **DNS root**.
- Everybody can generate .onion address (for Tor hidden services).

Read more: <https://www.torproject.org/docs/onion-services>



# TOR TIPS

- **Don't use Windows**

- Windows is simply not the best choice of platform to use Tor in an attempt to improve one's Internet privacy because of the **security bugs and vulnerabilities present in the system** may **compromise your privacy**, even when using Tor.



# TOR TIPS

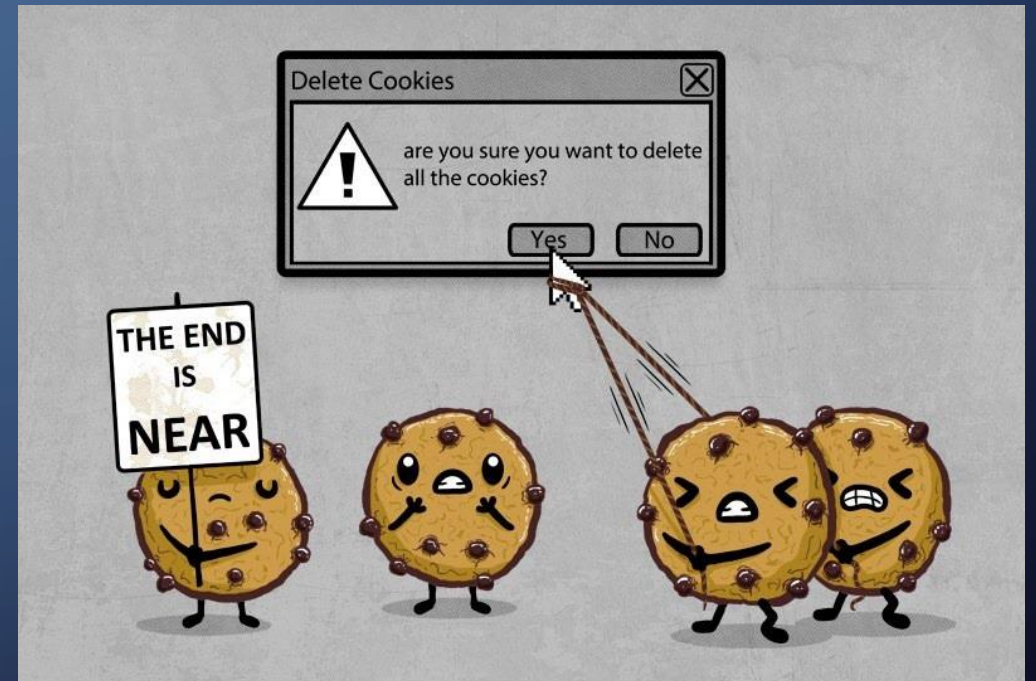
- **Don't use P2P**

- P2P is unwanted in Tor network because it is simply **not built for peer-to-peer file sharing**.
- Exit nodes of the network are set up to block file sharing traffic.
- You **abuse Tor network if you download torrents** and it slows down other users' browsing.
- Using Tor with BitTorrent clients doesn't make you anonymous because **those clients send your IP address directly to the tracker and other peers**, thus compromising your anonymity.



# TOR TIPS

- **Delete Cookies and site's Local Data!**
  - Websites may use cookies and local data storage to track your online activities, analyze your Internet usage, and detect your real identity.



# TOR TIPS

- **Disable JavaScript, Flash and Java**
  - Tor cannot protect your data with **active content** such as JavaScript, Adobe Flash, Java, QuickTime, ActiveX controls, VBScripts, etc. because these binary applications **run with your user account's privileges, and may access and share your data.**
  - They may also store cookies and site's data separately from the browser and operating system, which may be hard to detect and delete.

# TOR TIPS

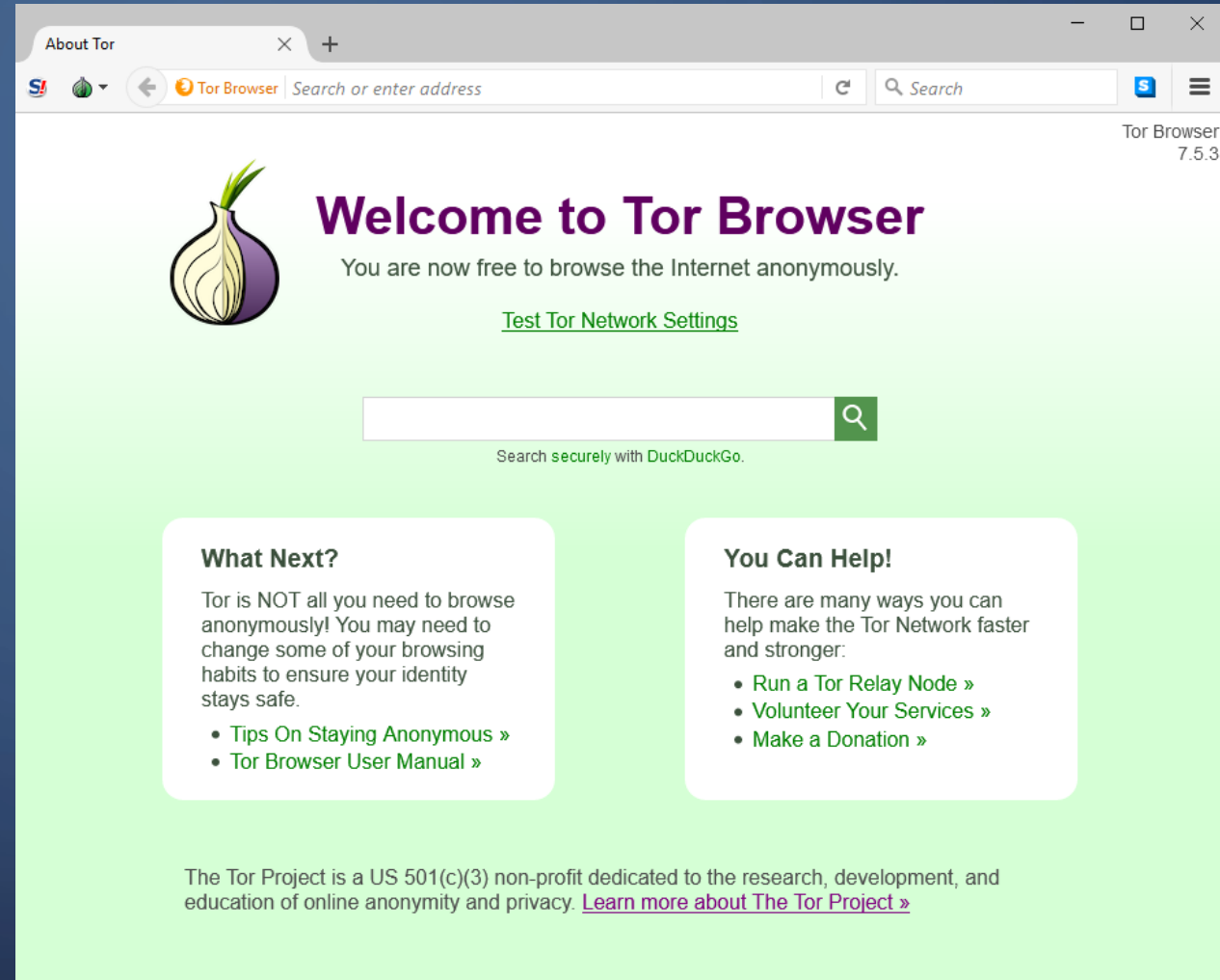
- **Don't use your Real Email**

- How can you **hide your real identity** if you're giving out your real email on the websites?

- **Don't use Google**

- Google is known for **collecting information on users' browsing and search data** to facilitate the growth of its ads revenue.

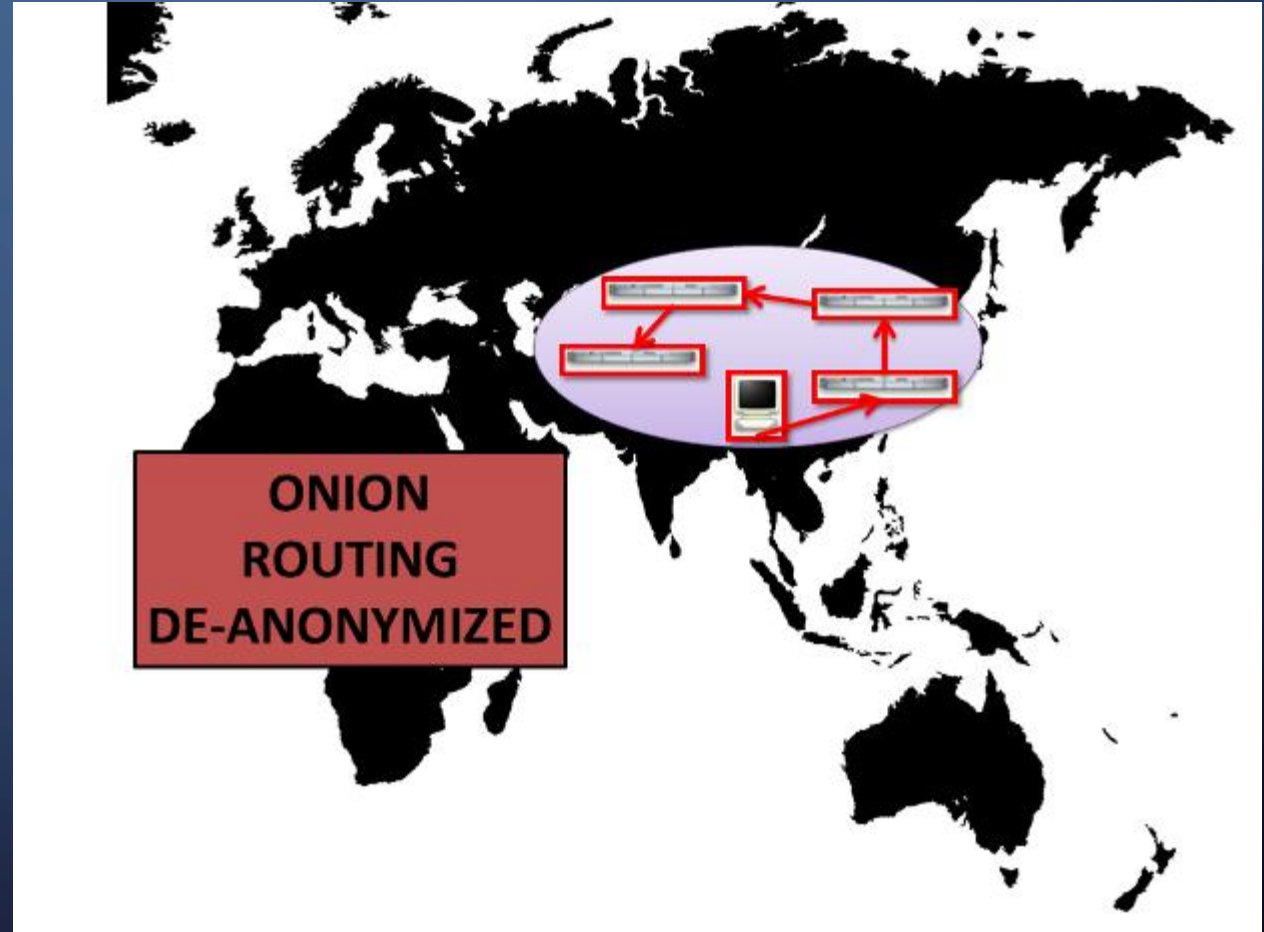
# TOR BROWSER



- You can download it from <https://www.torproject.org/projects/torbrowser.html>

# TOR WEAKNESSES

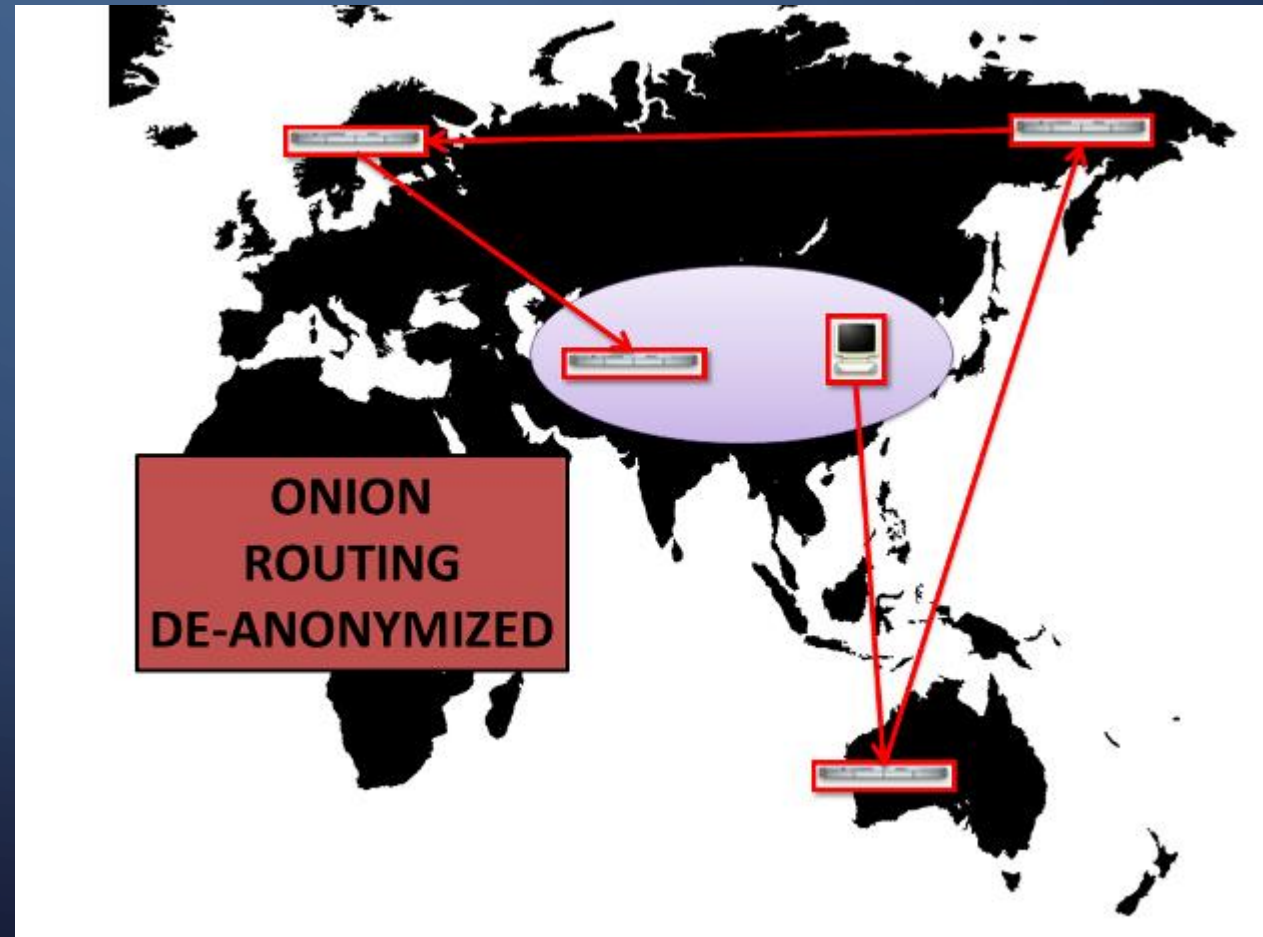
- If an adversary is able to see the entire path, Onion Routing loses its security.





# TOR WEAKNESSES

- If the adversary can see one node (A), and later another node (C) - even if there is an unseen or unknown number of nodes between A and C, an attacker can correlate the traffic.





# VPN VS. TOR

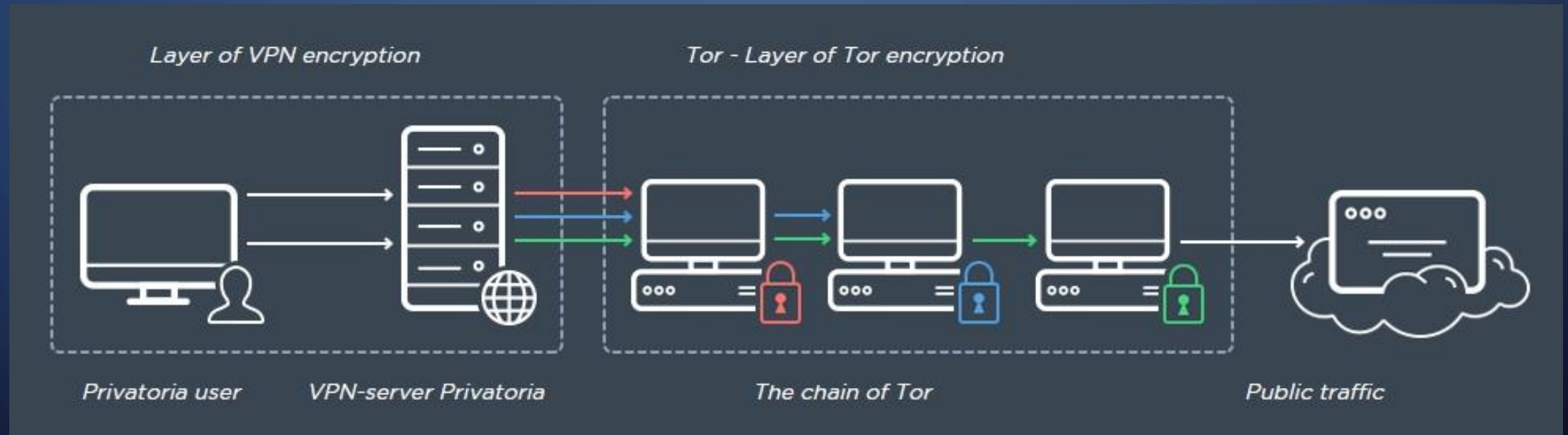
- VPN is faster than Tor
- VPN is suitable for P2P downloading
- But... VPN requires you trust your VPN provider  
(VPN provider can “see” what you get up to on the internet)
- Tor is much slower
- Tor is not suitable for P2P
- Tor does not require that you trust anybody, and is therefore much more truly anonymous
- Tor is often blocked by websites

# USING VPN AND TOR TOGETHER



- VPN and Tor can be used together in order provide an extra layer of security, and to mitigate some of the drawbacks of using either technology exclusively.
- Connecting in this way is secure... but slow.

# TOR THROUGH VPN



# TOR THROUGH VPN: BENEFITS

- Your ISP will not know that you are using Tor (although it can know that you are using a VPN)
- The Tor entry node will not see your true IP address
- Allows access to Tor hidden services (.onion websites)
- The **VPN** you use **is not able to see** what encrypted **data** you are sending over TOR, they will only be able to see that you are connecting to TOR nodes.

# TOR THROUGH VPN: DRAWBACKS

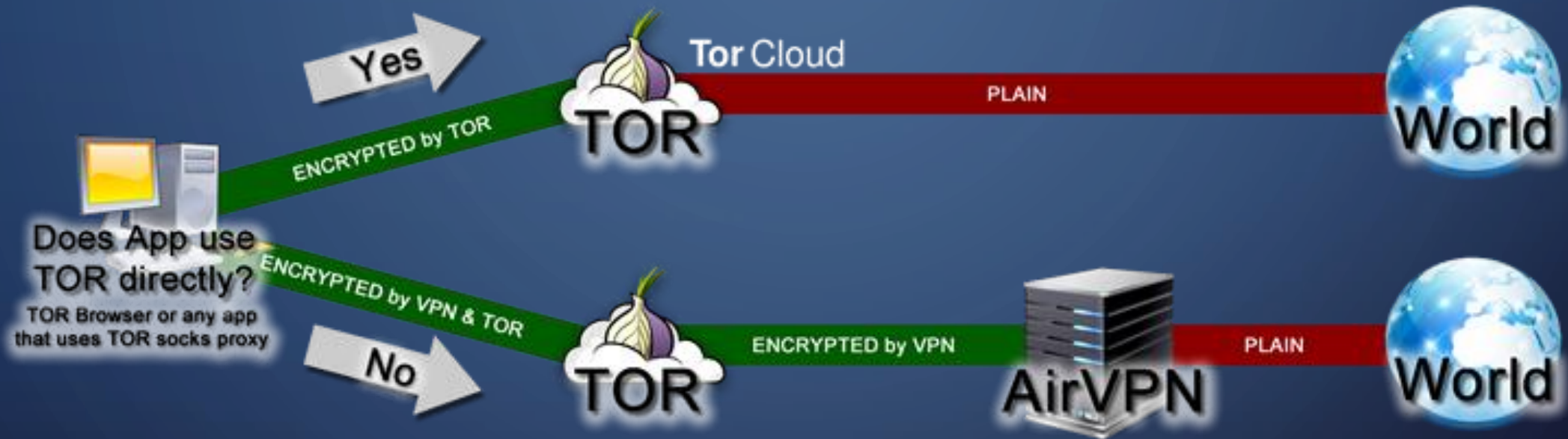
- Your VPN provider knows your real IP address
- No protection from malicious Tor exit nodes. Non-HTTPS traffic entering and leaving Tor exit nodes is unencrypted and could be monitored.
- Tor exit nodes are often blocked
- If your VPN provider is keeping logs, it would not make much difference as if you were just connecting to TOR through your ISP as your traffic can be simply linked back to your true IP.

# TOR THROUGH VPN

- Some VPN services (such as NordVPN, Privatoria and TorVPN) offer Tor through VPN.
- But this is **nowhere near as secure as using the Tor browser**, where Tor encryption is performed end-to-end from your desktop to the Tor servers!
- It is possible that your VPN provider could intercept traffic before it is encrypted by the Tor servers.
- The Tor Browser has also been hardened against various threats in a way that your usual browser almost certainly has not been.



# VPN THROUGH TOR



- This setup requires you to configure your VPN client to work with Tor, and the only VPN providers we know of to support this are *AirVPN* and *BolehVPN*.

# VPN THROUGH TOR: BENEFITS

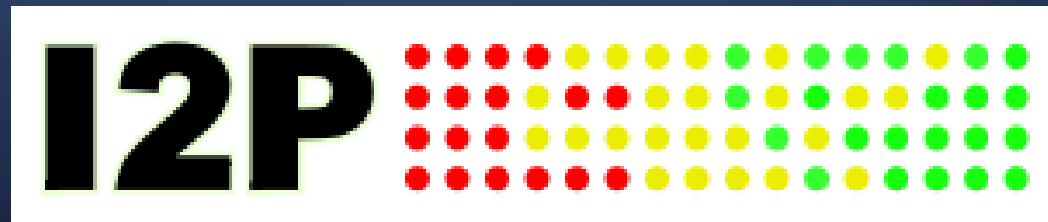
- Your VPN provider cannot see your real IP address, only the one of the TOR exit node. When combined with an anonymous payment method (such as properly mixed Bitcoins) made anonymously over Tor, this means the VPN provider has no way of identifying you.
- Bypasses any blocks on Tor exit nodes.
- Protection from malicious Tor exit nodes, as data is encrypted by the VPN client before entering (and exiting) the Tor network
- Enables you to choose server location which is great for geo-spoofing.

# VPN THROUGH TOR: DRAWBACKS

- Cannot access TOR's hidden services.
- Fixed Tor circuit for each OpenVPN session.


# I2P

- The **Invisible Internet Project (I2P)** is an anonymous network layer that allows for censorship-resistant, peer to peer communication.
- Every machine using I2P acts as a router, which makes I2P a fully decentralized service.





# I2P

- Its primary function is to be a “network within the internet”, with traffic staying contained in its borders.
  - I2P is a Darkweb tool that can also be used to access the surface web anonymously through ‘Outproxy’s’ (which are equivalent to Tor exit nodes).
  - I2P Outproxies suffer similar weaknesses to Tor exit nodes however, and the fact that there are **far fewer of them** (as I2P has a much smaller user base) means that they are **potentially more open to attack**.
- 

# I2P

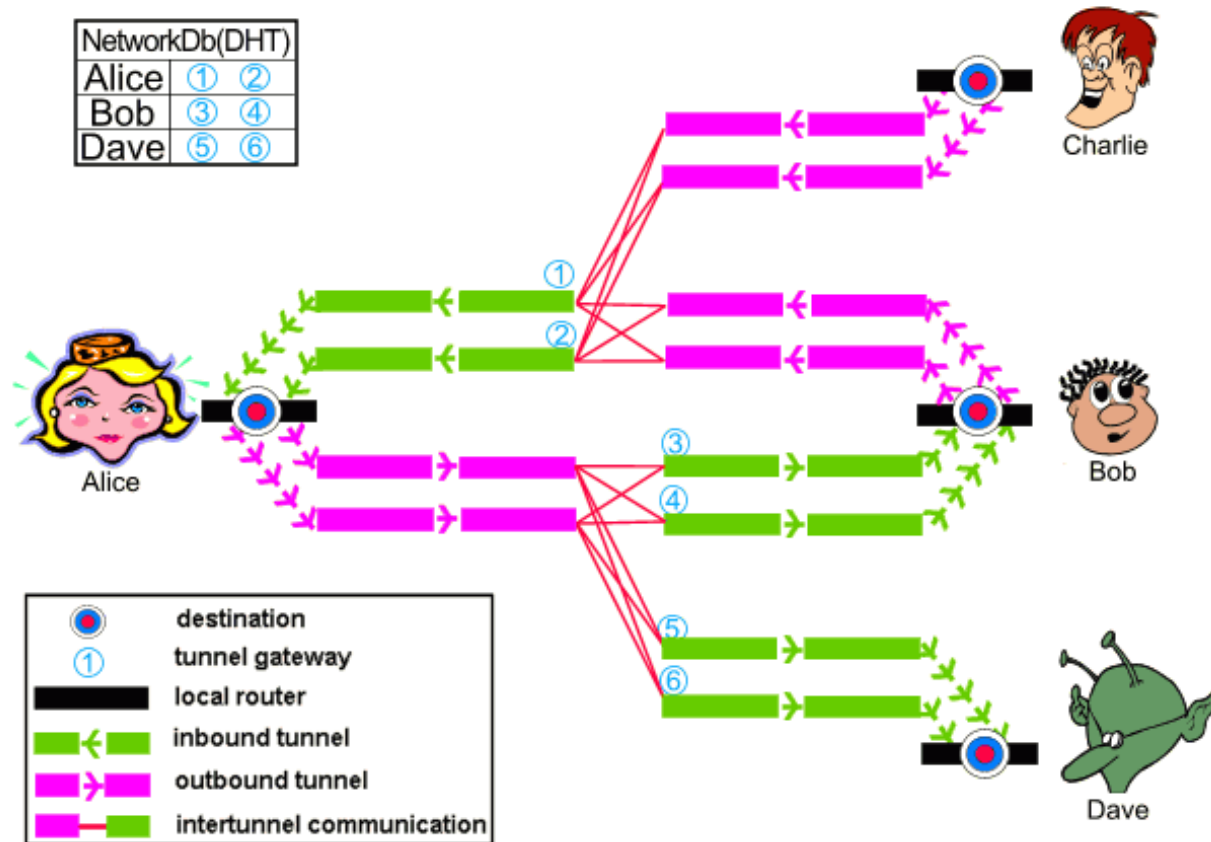
- I2P performs **packet based routing** as opposed to Tor's circuit based routing.
- Unlike Tor, I2P tunnels are **uni-directional**, so incoming traffic and outgoing traffic are completely separate, which improves anonymity.
- Unlike Tor Onion routing, I2P uses **Garlic routing**, which **encrypts multiple messages together** to make it more difficult for attackers to perform traffic analysis.



# I2P

- I2P does not rely on a trusted directory service to get route information.
- I2P's **netDB** is a **distributed hash table** based on the Kademlia protocol, used to **store and share network metadata**.
- Not every peer in the I2P network form part of the netDb, but only those fast I2P users, the so called floodfill peers.
- Any user with high bandwidth can appoint itself as floodfill peer.
- There are two types of network metadata: *LeaseSets* and *RouterInfos*.

# I2P



# I2P: NETWORK METADATA

- **LeaseSet** - provides information about a group of **tunnel entry points (leases)** for a particular client destination.

Each of leases specify the following information:

- The tunnel gateway router (by specifying its identity)
- The tunnel ID (a 4 byte number)
- When that tunnel will expire.

# I2P: NETWORK METADATA

- **RouterInfos** - provides **information about a specific router** and how to contact it, including:
  - the router identity (a 2048bit ElGamal encryption key, a signing key, and a certificate)
  - the address where to contact it (ip and port)
  - when this was published
  - several text options
  - the signature of the above, generated by the identity's signing key

# FEATURES OF I2P: TORRENTS

- **Torrents** - I2P (unlike Tor) has absolutely **no issue with users torrenting**
  - Postman Tracker (it is essentially the Pirate Bay)
  - I2PSnark (it is essentially uTorrent)

The drawback of I2P is speed, with an average of about 30KBps, which is painfully slow compared to the 1-2MB/s that most torrenting sites offer.

# FEATURES OF I2P: EMAIL/MESSAGING

- **Email/Messaging**

There are a few messaging services on I2P:

- **I2P's built in email application**
  - it lets you email the regular internet to, and from I2P
- **I2P Bote**
  - it operates only on the I2P network



# FEATURES OF I2P: EEPSITES

- **Eepsites** are the I2P equivalent of a Tor Hidden Service: they are websites hosted on the I2P network, whose operators can be anonymous.
- Unlike Tor hidden services, Eepsites web addresses are actually readable, with the domain of .i2p at the end.

**THE END**