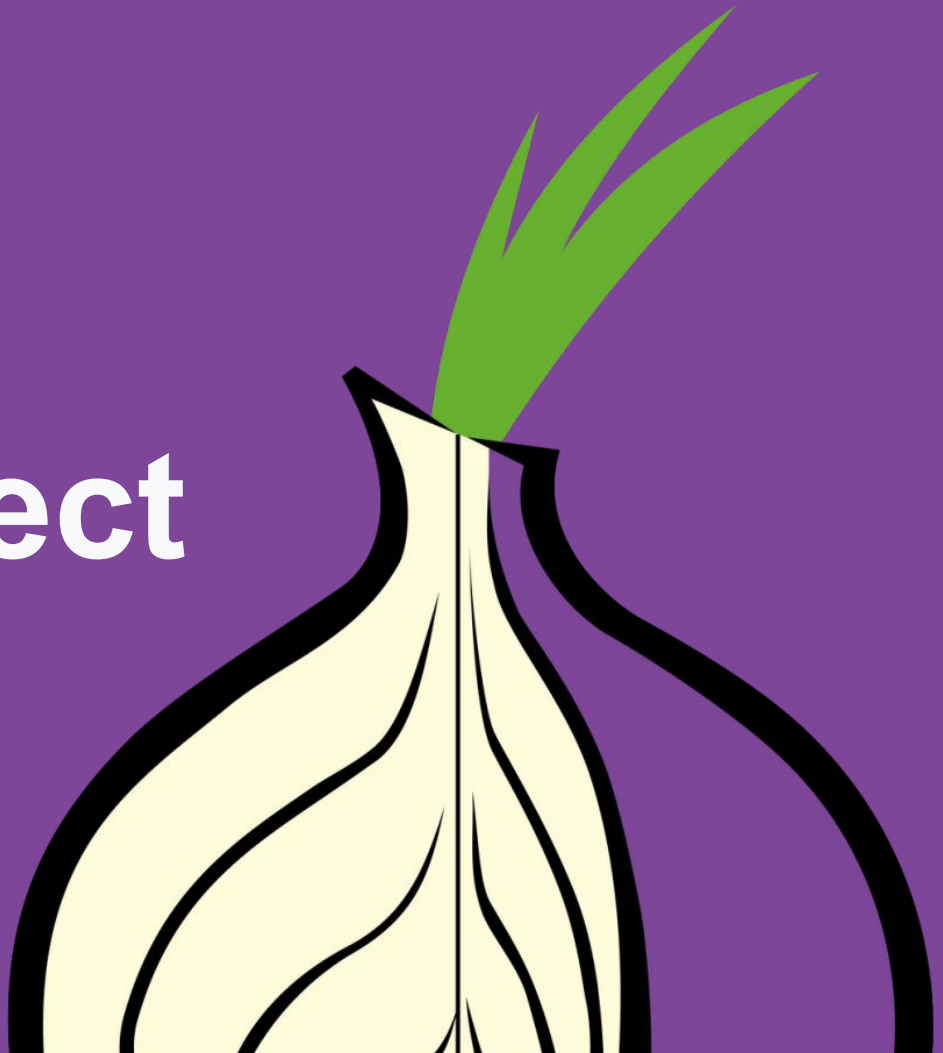
The tor project



torproject.org

Agenda

- Understand in full detail what is tor
- Understand in full detail how tor works
  - This includes the protocol
  - This includes major components in its backend
- Understand what are onion services(a.k.a the dark web)

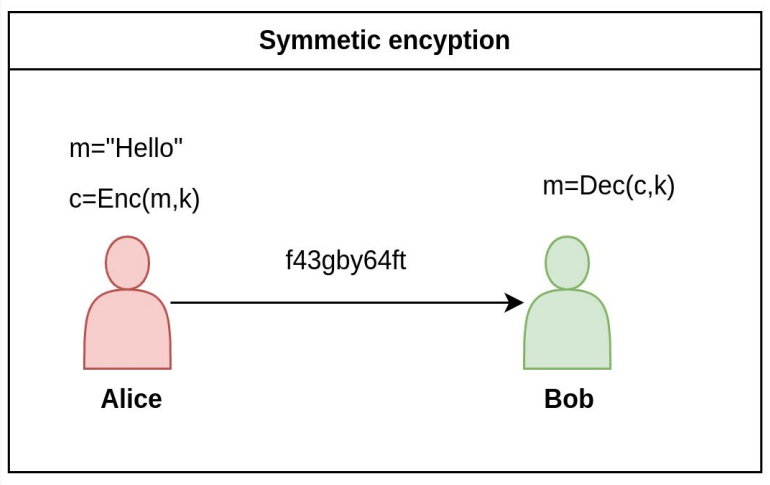
Prerequisites

- Basic networking knowledge(ip,ARP,NAT)
- Basic understanding of encryption
- Basic understanding of ssl/tls

Lets recap basic security concepts

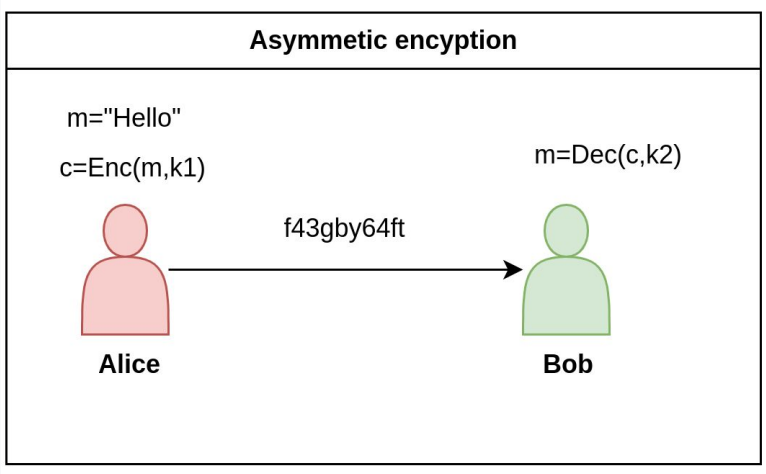
Symmetric encryption

- There are 2 types of encryptions
- Symmetric encryption:
  - Alice wants to send Bob a message **m**
  - Alice uses a special function Enc and a secret key **k** to create a ciphertext **c**
  - Bob uses the same secret key **k** and a special decrypt function DEC to retrieve the original message from the ciphertext



Asymmetric encryption

- Asymmetric encryption:
  - Alice wants to send Bob a message **m**
  - Alice uses a special function Enc and a secret key **k1** to create a ciphertext **c**
  - Bob uses the a different secret key **k2** and a special decrypt function DEC to retrieve the original message from the ciphertext

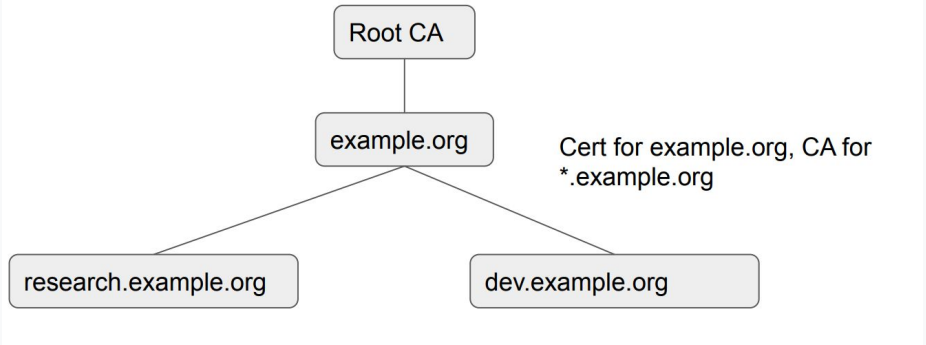


Certificate authority

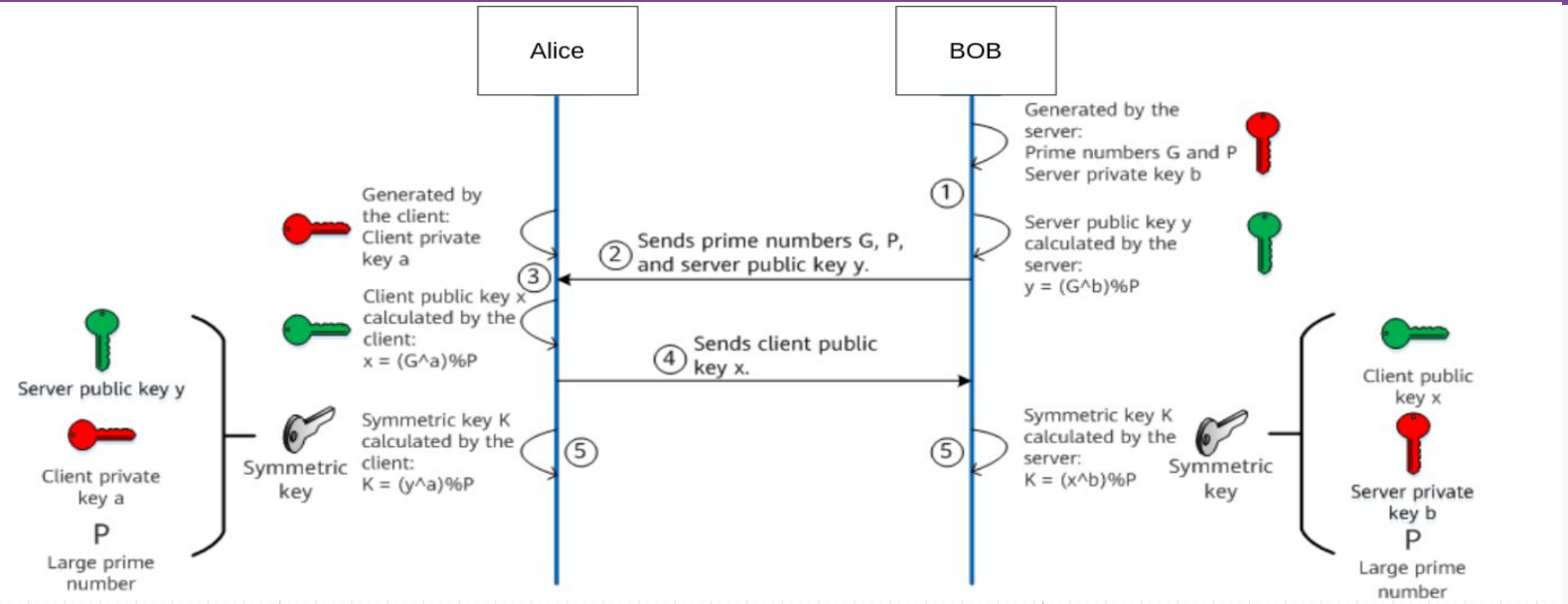
- Establishing keys cannot be done in the open
- A man in the middle can sniff all traffic,decrypt messages and fake keys
- So some method to publish keys is required

Certificate authority

- We can establish a web of trust
  - I trust who my friends trust
  - My friends trust a CA
- Every person must decide who is trust from different authorities



Diffie-Hellman key exchange



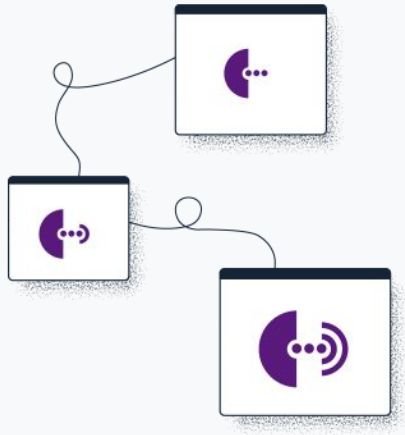
K=(y^a) % P=((G^b % P)^a) % P=(G^(a*b) % P)

K=(X^b) % P=((G^a % P)^b) % P=(G^(a*b) % P)

What is TOR?

Different ways of defining Tor

- Tor ⇒ free software created at NRL starting 2001/2.
- Tor ⇒ an open network of ~9,500 nodes – anyone can join!
- Tor ⇒ a browser that connects you to the Tor network.
- Tor ⇒ a US non-profit formed in 2006.
- Tor ⇒ a community of volunteers, researchers, developers, trainers, advocates from all over the world.



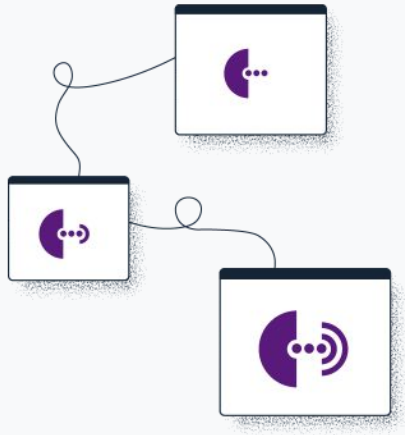
What is Tor?

- Stands for The Onion Router
- A way to use the internet with as much privacy as possible:
  a. by routing traffic through multiple servers; and
  b. by encrypting it each step of the way.
- Hence the term “onion routing”.
- Tor provides anonymity, mitigating against surveillance and censorship.

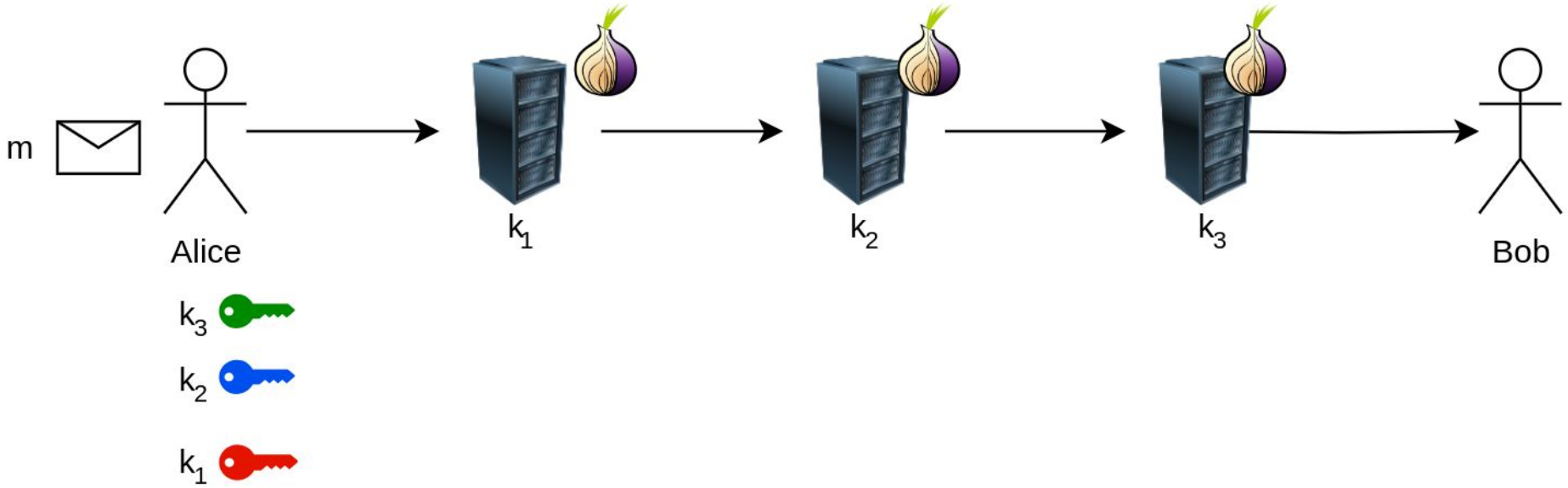
What is onion routing

Onion routing

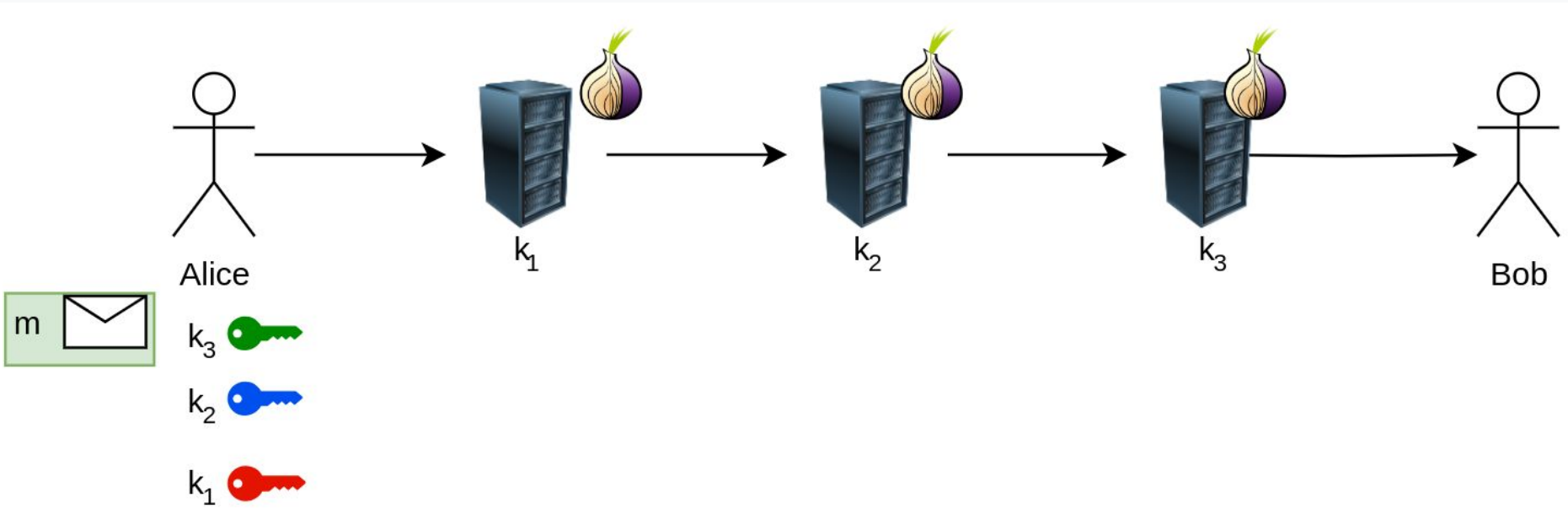
- A method for passing messages between client and server
- A message is sent from client to server through intermediate stations
- each intermediate node knows only its predecessor and successor
- This makes tracing the message source very hard



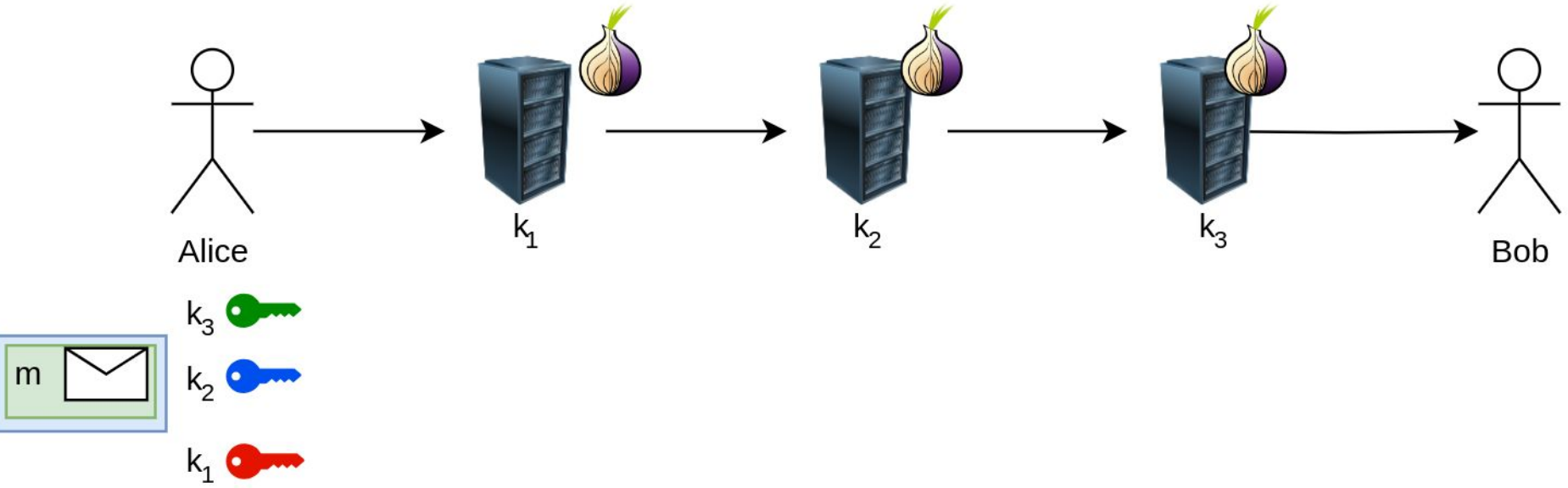
Onion routing



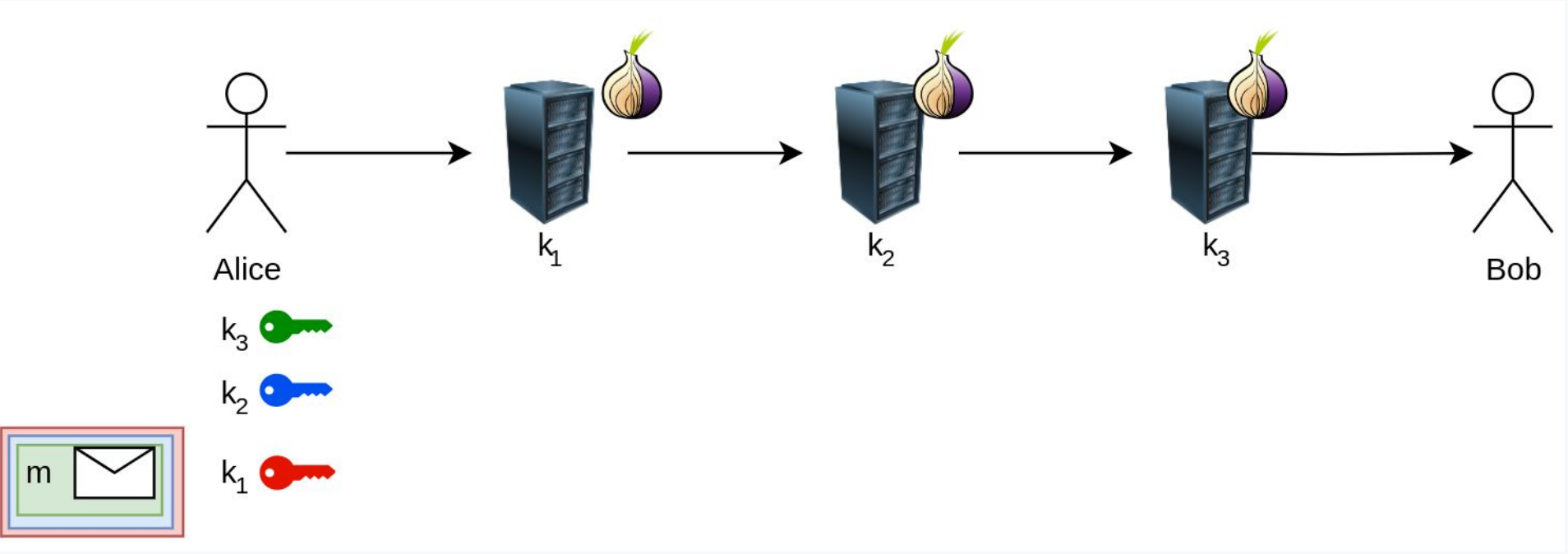
Onion routing



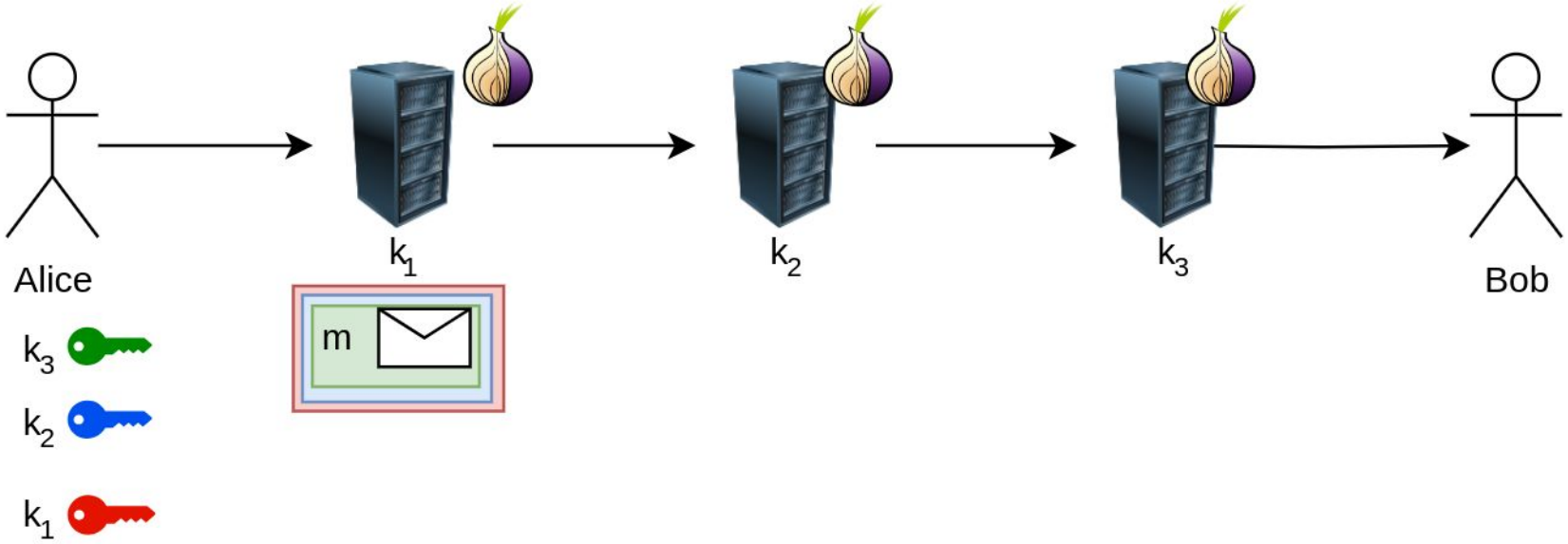
Onion routing



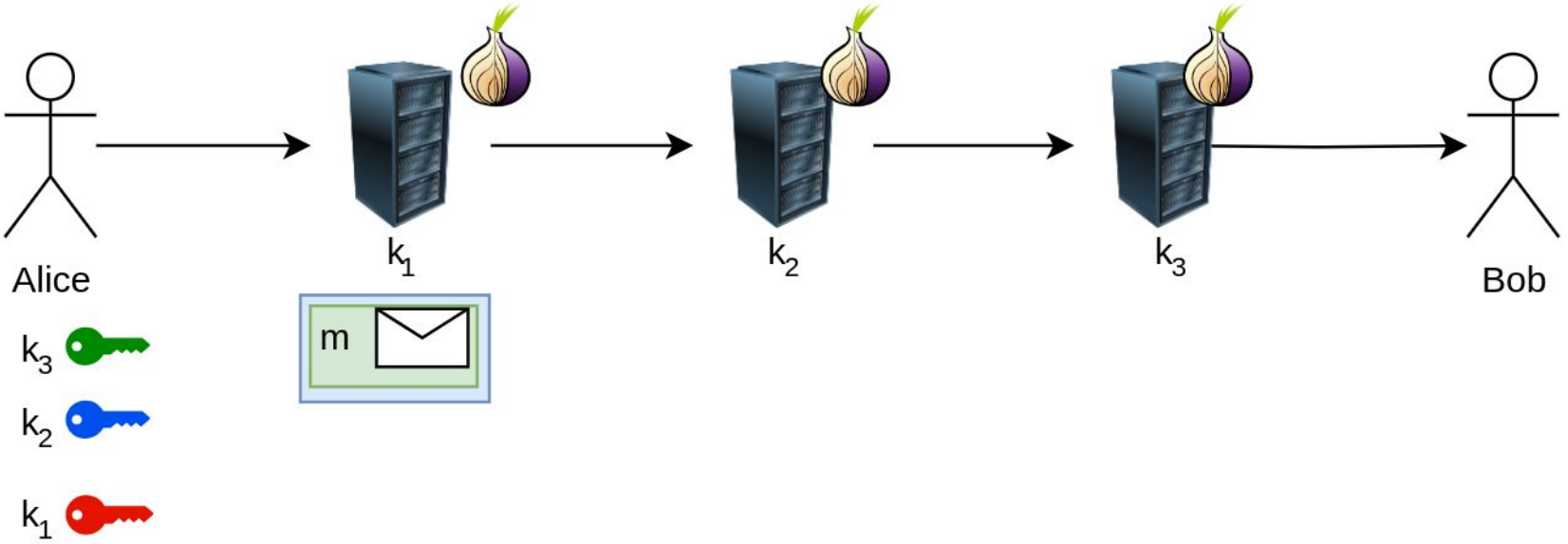
Onion routing



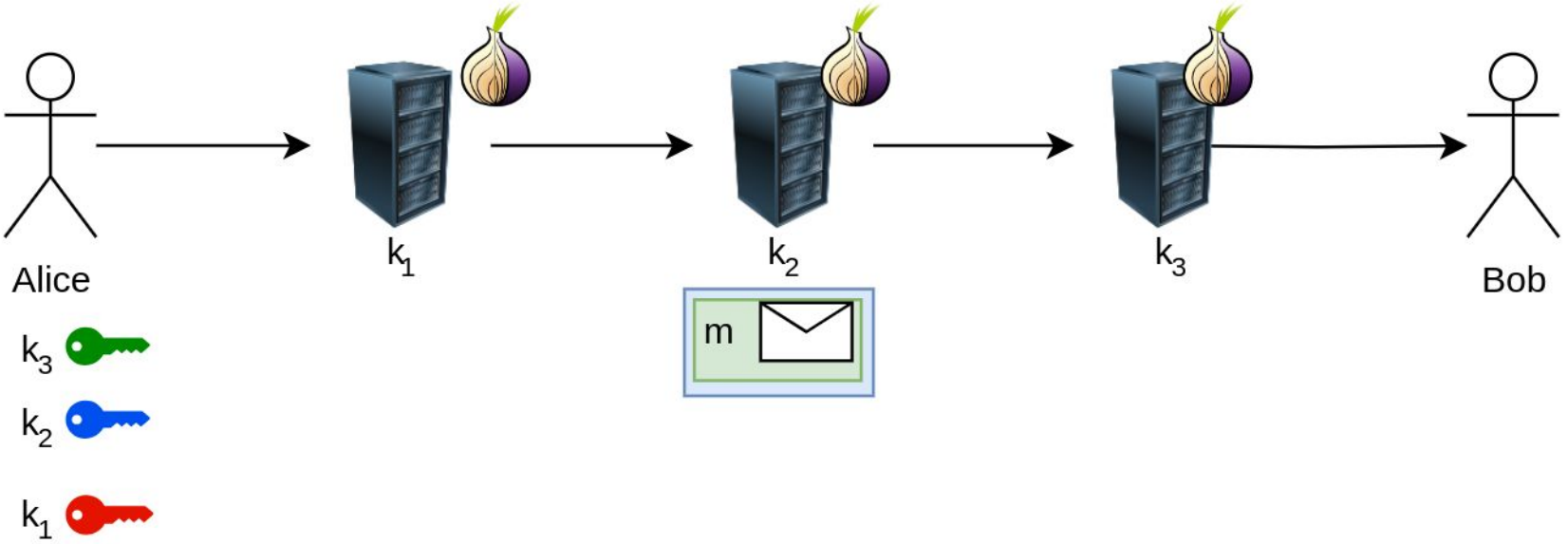
Onion routing



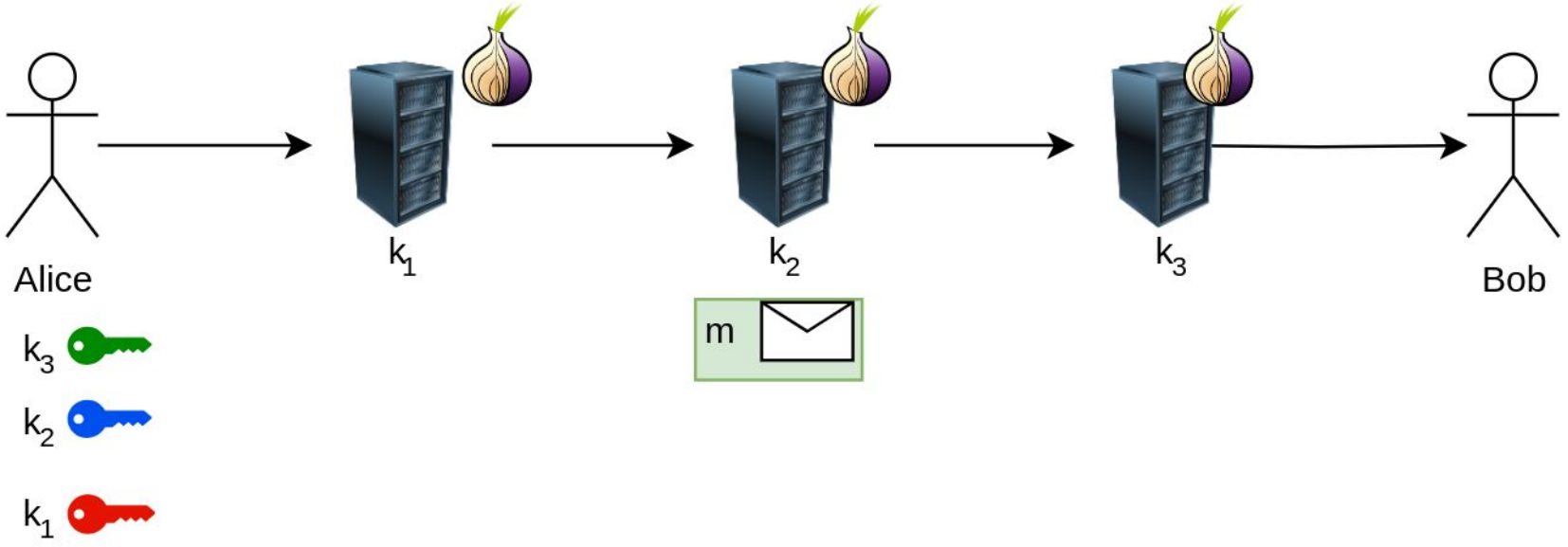
Onion routing



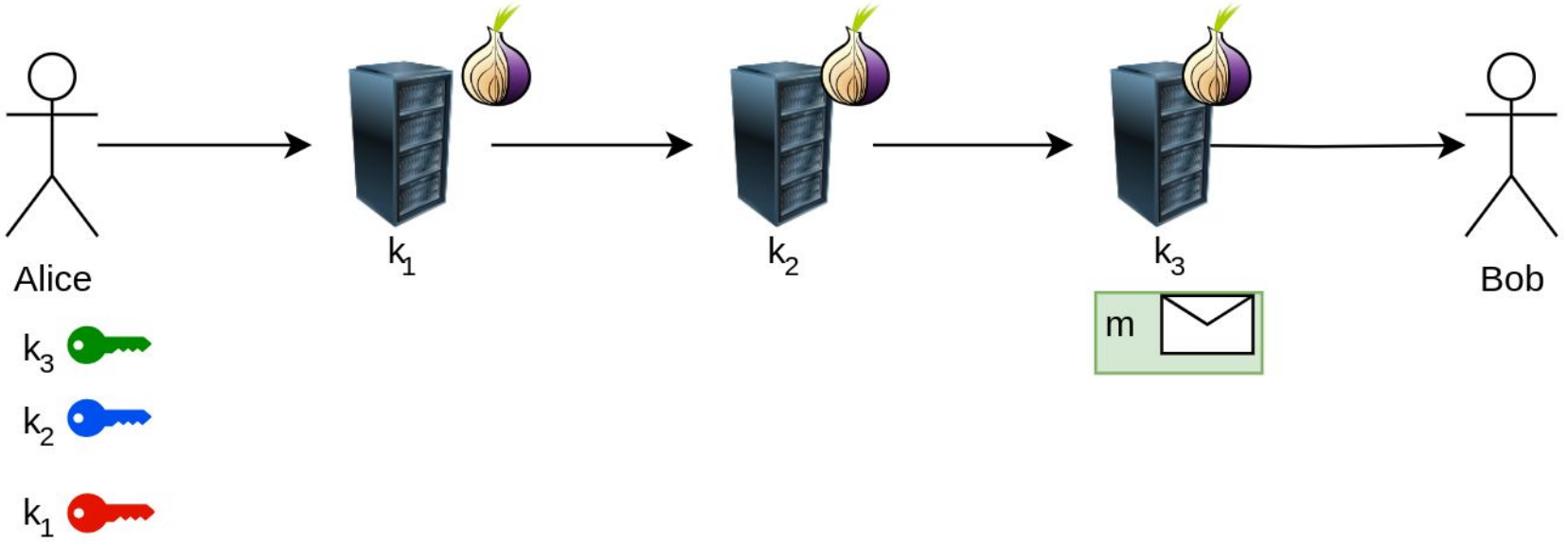
Onion routing



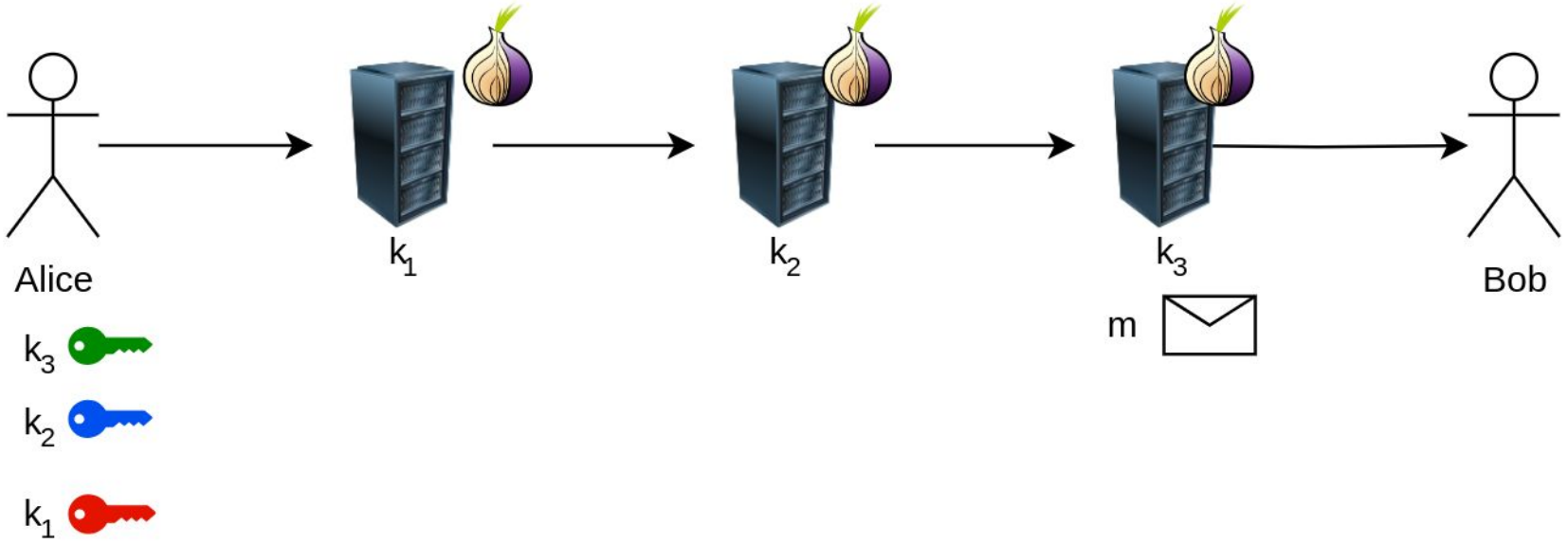
Onion routing



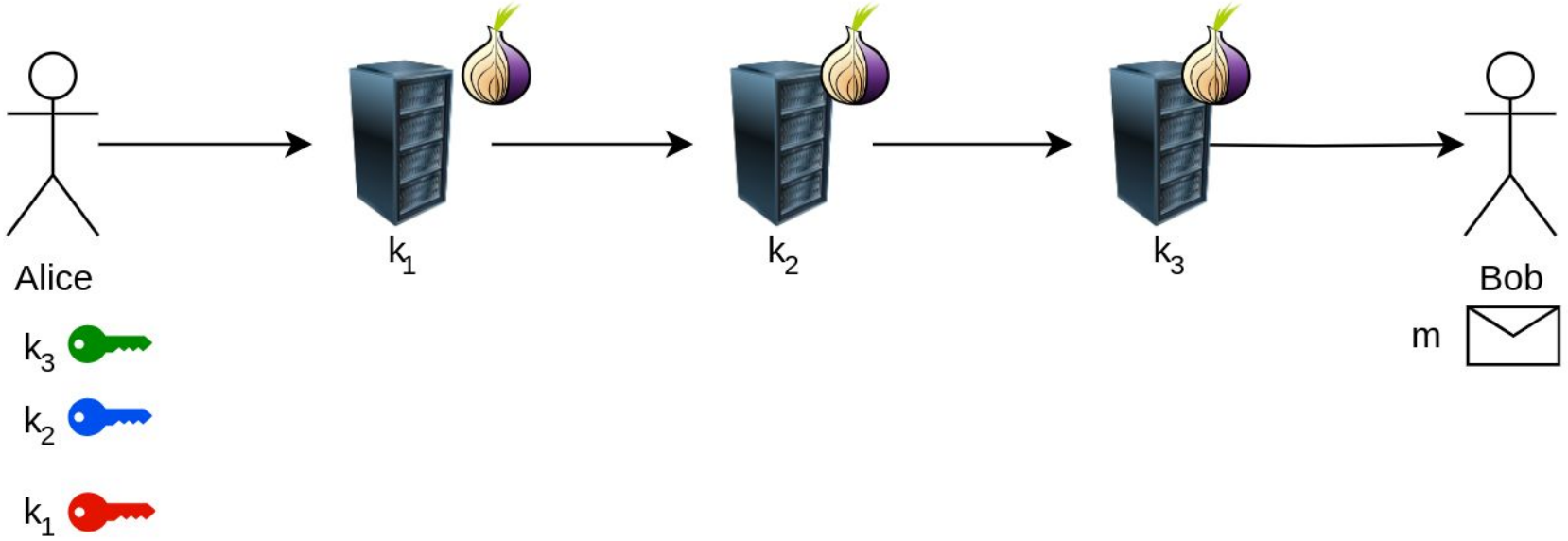
Onion routing



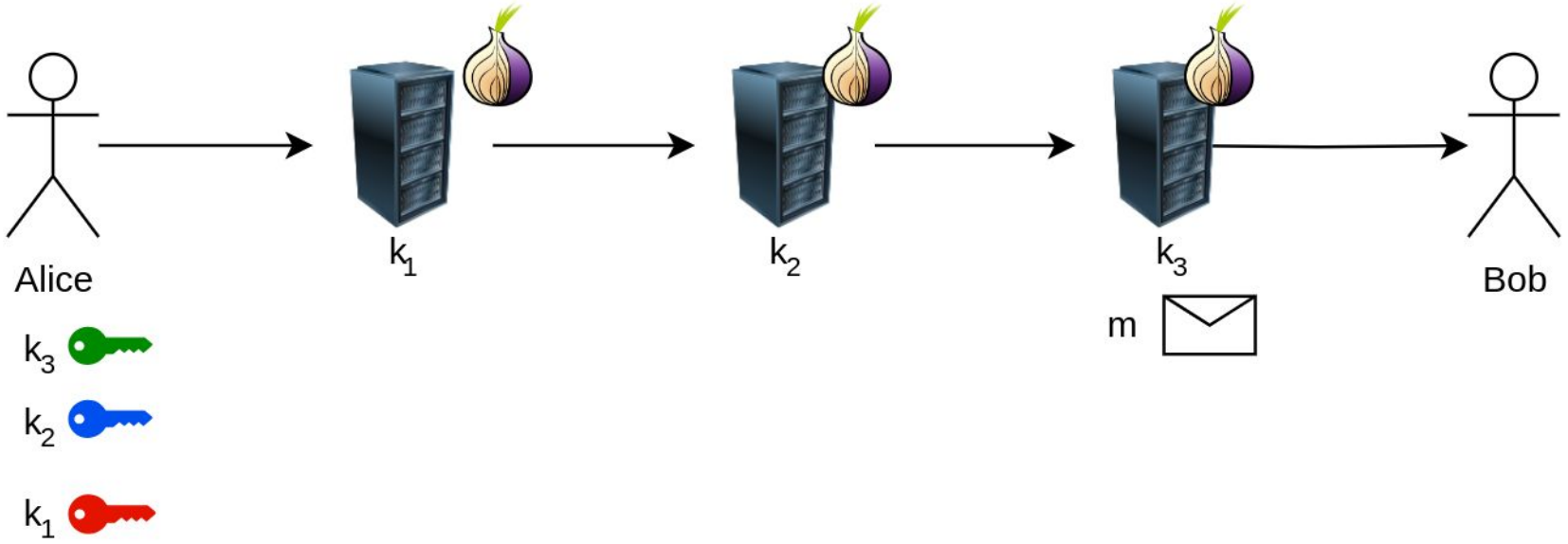
Onion routing



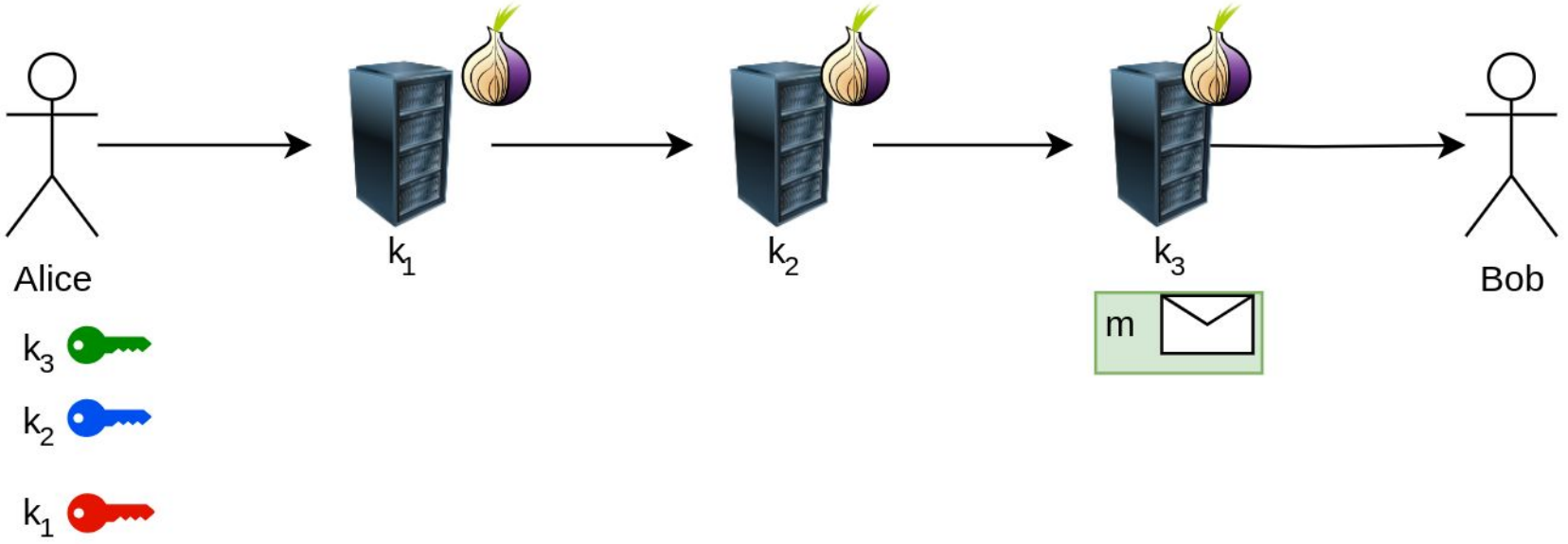
Onion routing



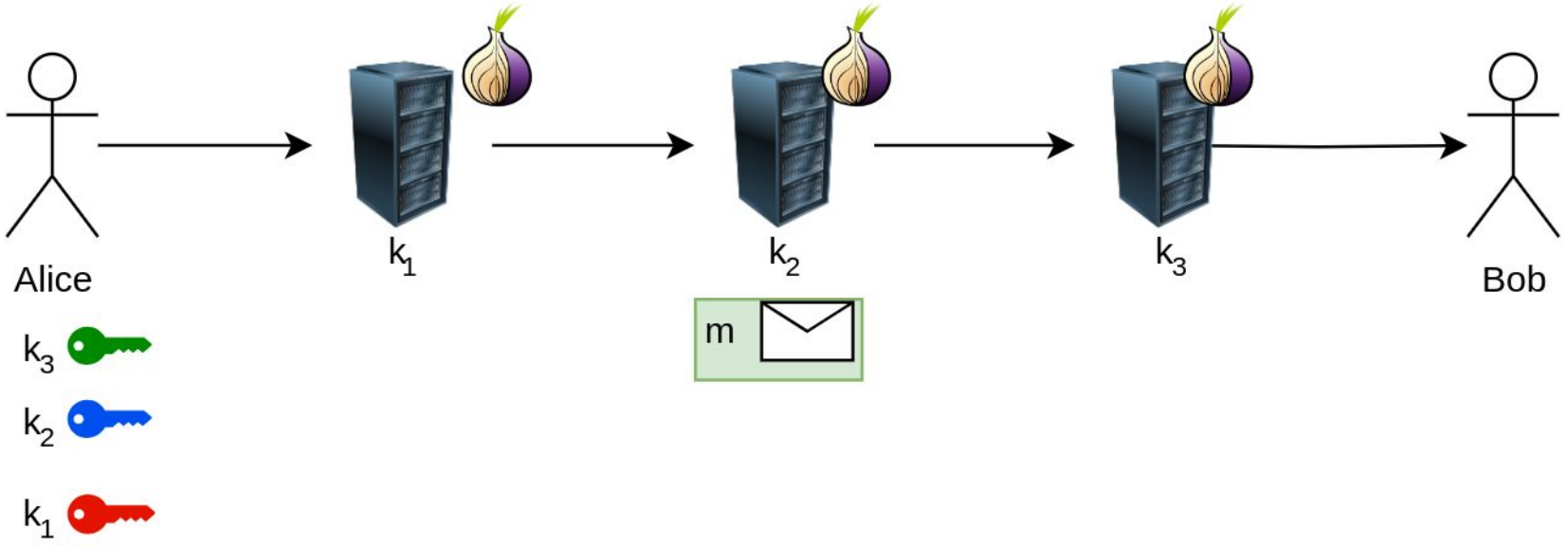
Onion routing



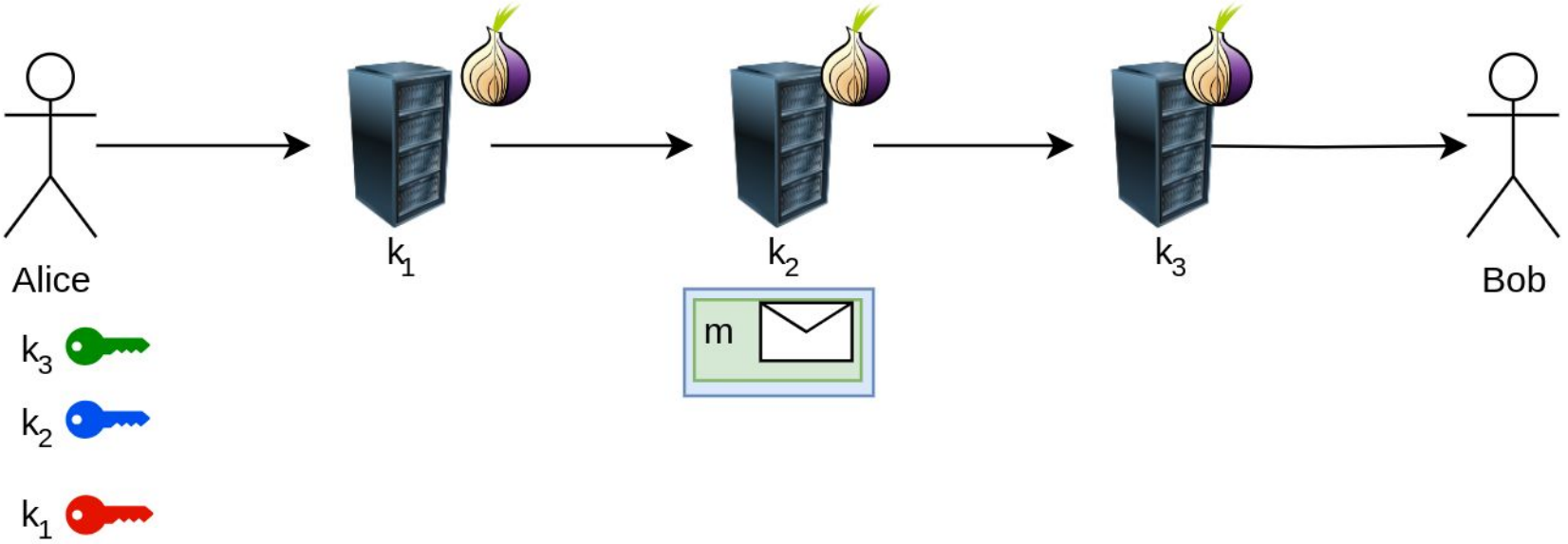
Onion routing



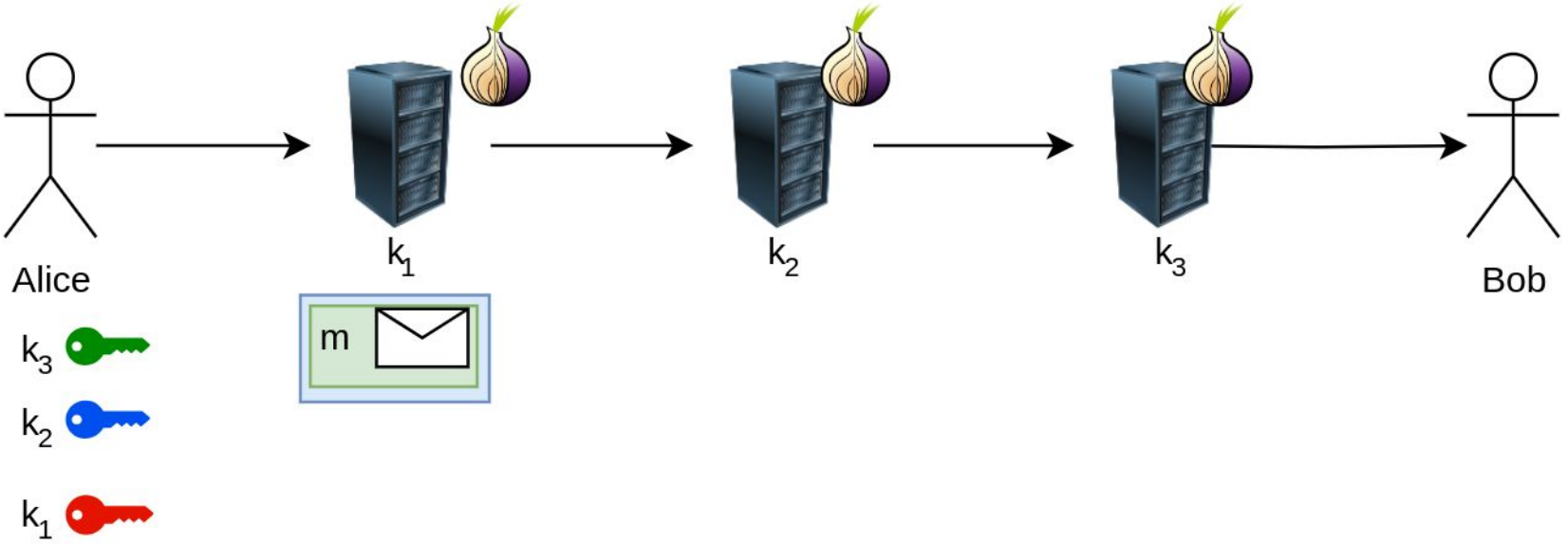
Onion routing



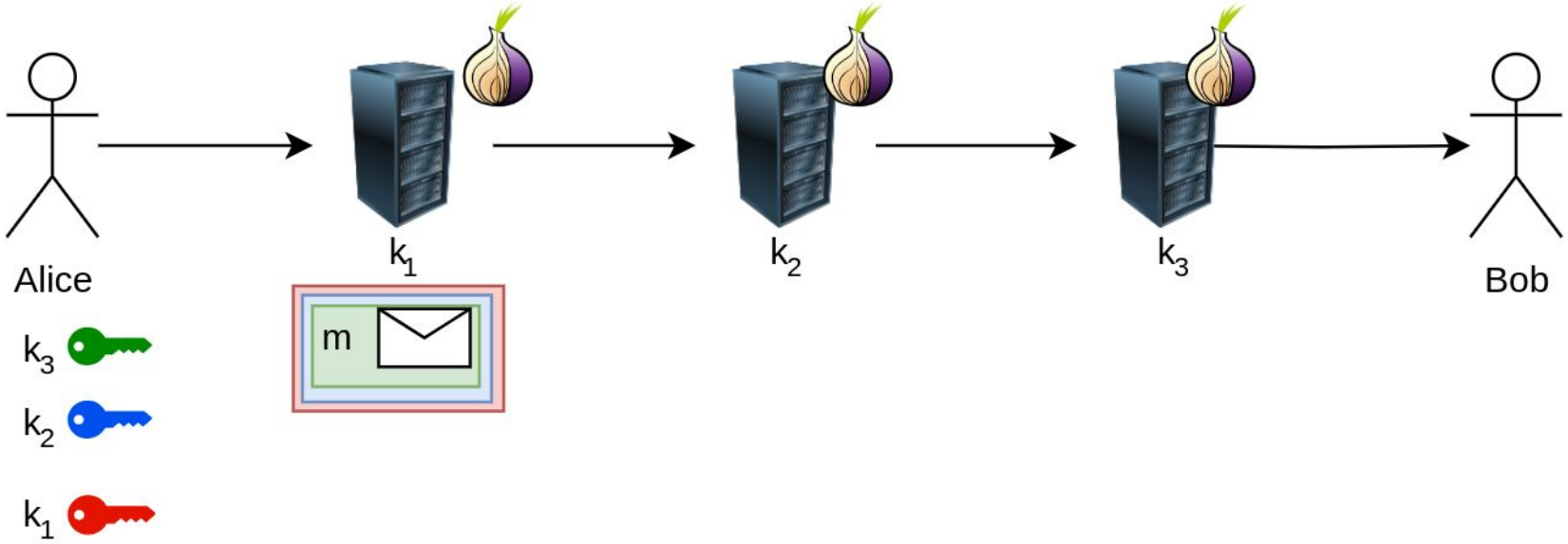
Onion routing



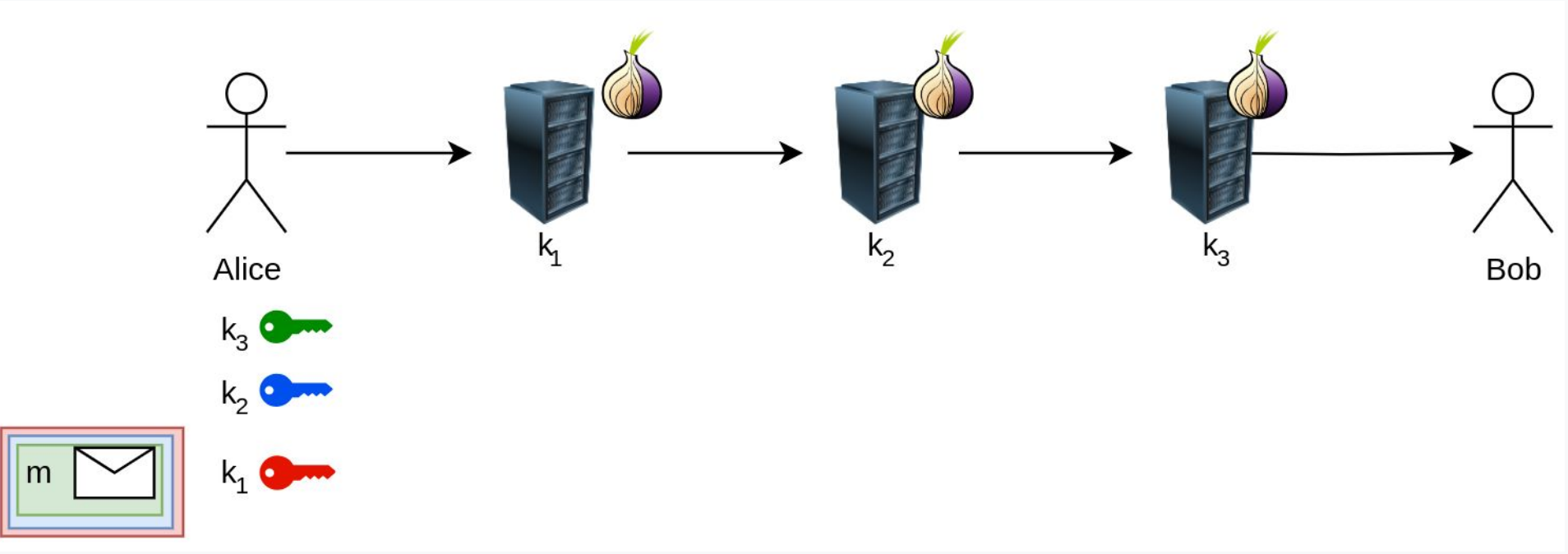
Onion routing



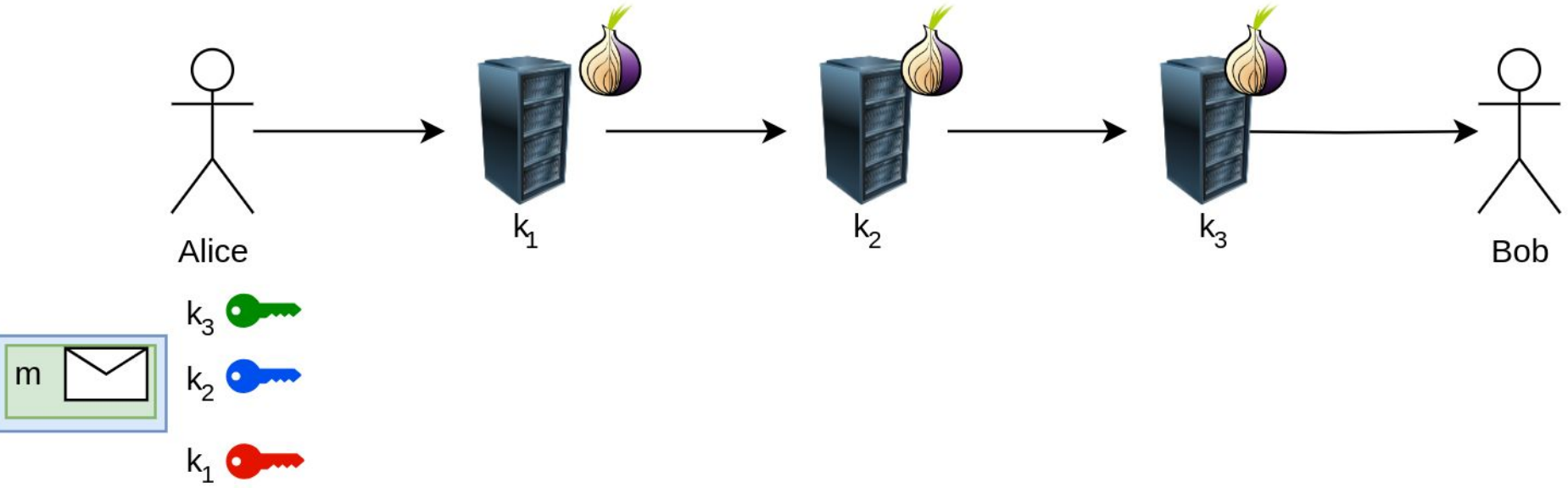
Onion routing



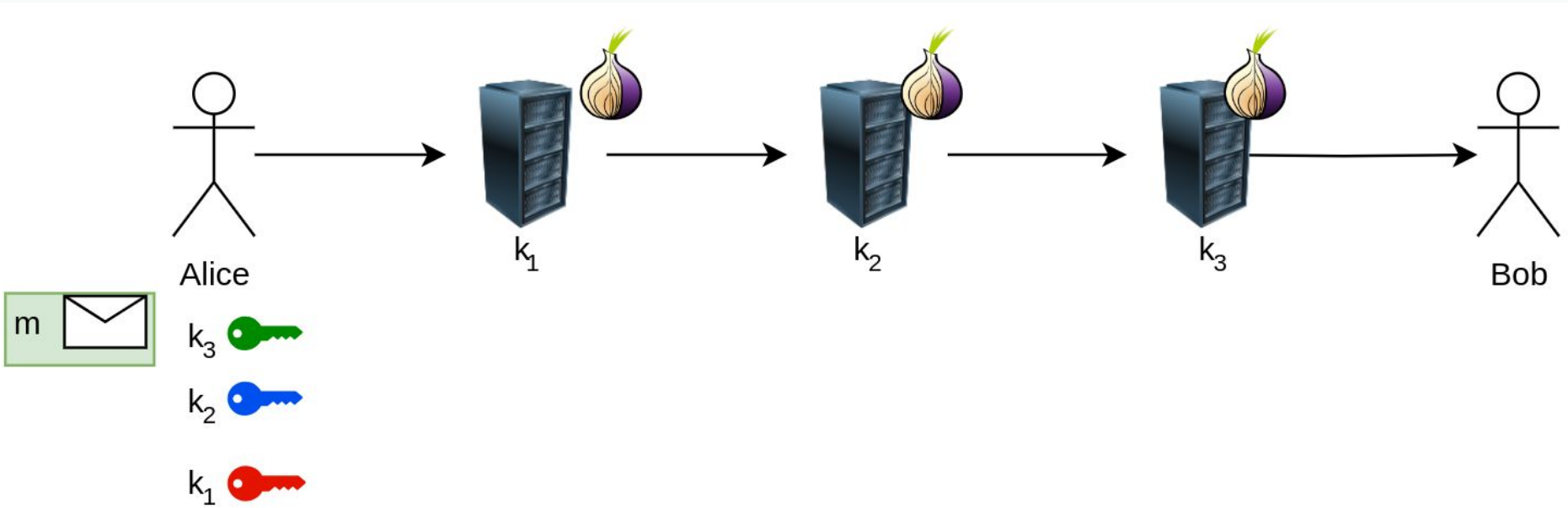
Onion routing



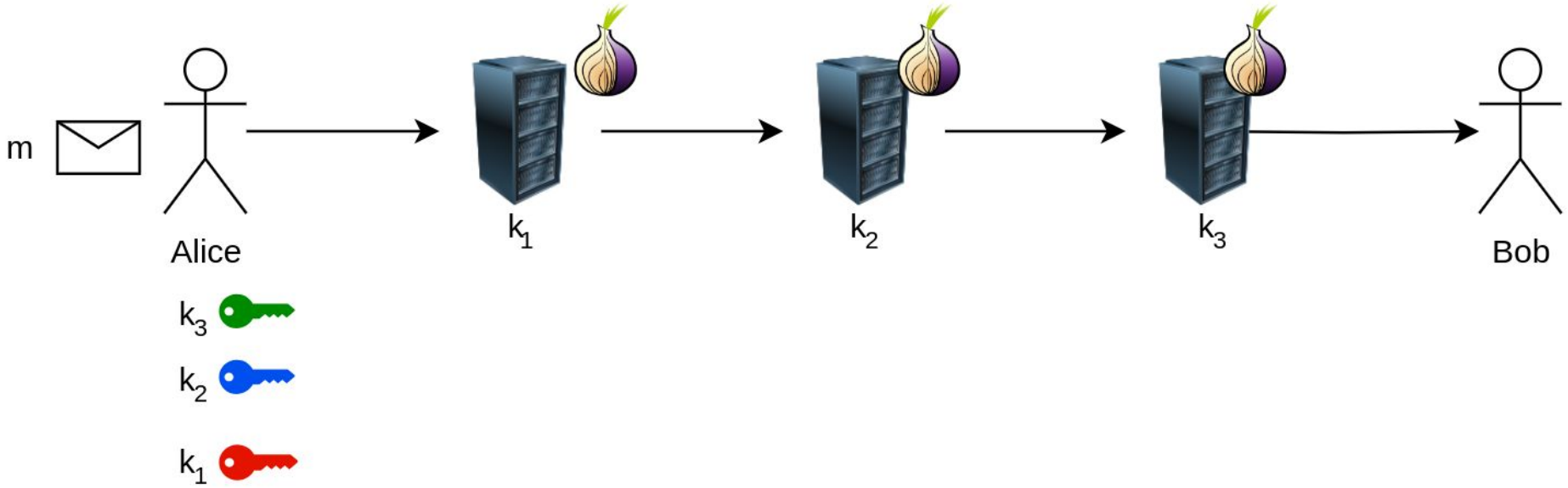
Onion routing



Onion routing



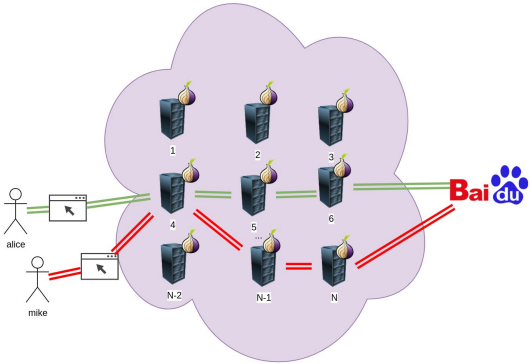
Onion routing



The TOR design

The TOR design

- The TOR network is an overlay network comprised of nodes
- Each node is called onion route
- Nodes create a variation of onion routing paths called circuit
- Traffic from a client is sent through a random circuit,comprised of random nodes to its destination
- TOR assumes large numbers
    - Large number of nodes
    - Large number of client
    - As so very large amount of possible combinations

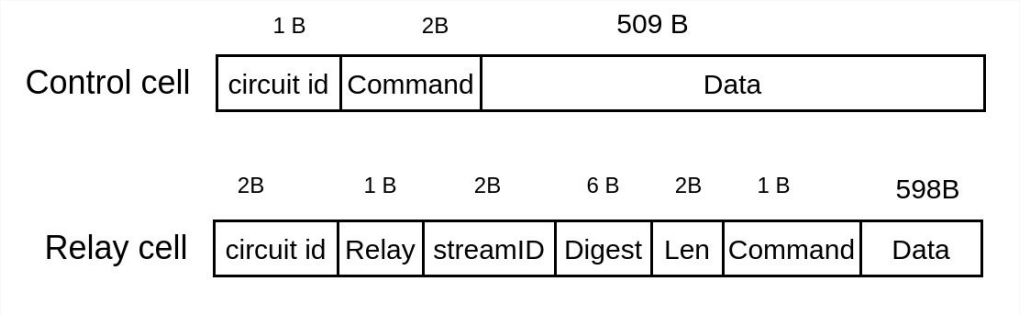


CELLS and communication

- Tor presents the SOCKS 5 proxy for communication
- Tor provides communication only using tls\ssl
  - Currently runs only over TCP!!
- Tor message are sent using a custom protocol
  - Messages are separated into 512 bytes and are called cells

Cell types

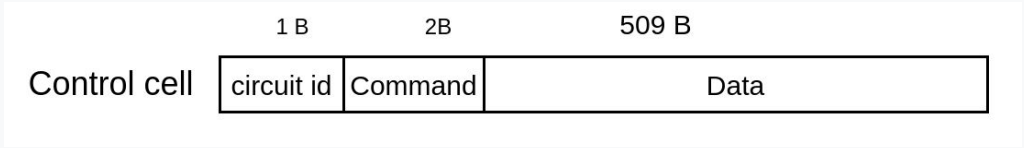
- There are 2 types of cells in TOR
- The first type is called control cell and is used for sending control commands
- The second type is called relay cell and it is used for sending data



Control cell

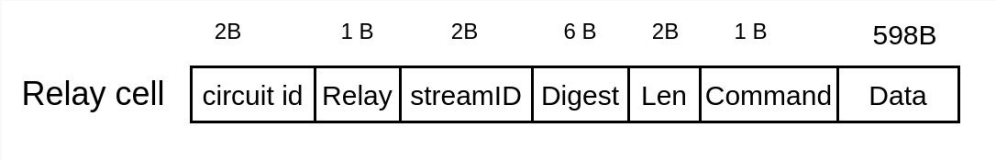
It is comprised of the following structure:

- circuit id : 1 byte, uuid of the current circuit
- Command : 2 Byte representing some control option.The options are:
  - padding : used for keep alive
  - create/created : used for creation of circuits
  - destroy : used for destroying a circuit
- Data : 509 byte command content



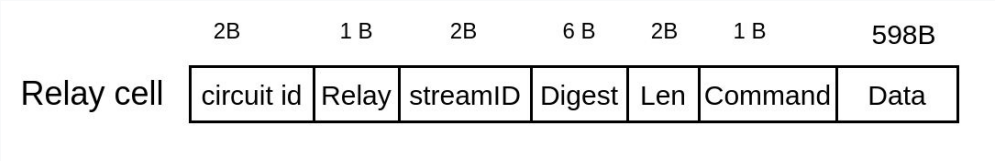
Relay cell

- It is comprised of the following structure:
  - circuit id : 1 byte, uuid of the current circuit
  - Relay : 1 Byte representing some control option.
  - StreamID : 2 Byte representing the stream byte. Multiple streams can be on a single circuit!
  - Digest : 6 Byte, checksum for integrity checking
  - Len : 2 Byte, the length of the relay payload



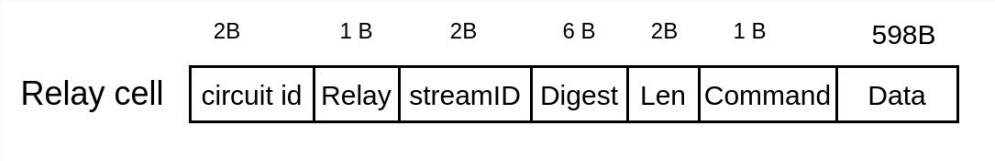
Relay cell

- Command : 1 byte,a relay command.The options are:
  - relay data : for transferring data
  - relay begin : to open a stream
  - relay end : to close a stram
  - relay teardown : to destroy a stream
  - relay extend/relay extended :to ex- tend the circuit by a hop, and to acknowledge
  - relay truncate/relay truncated : to tear down only part of the circuit, and to acknowledge
  - relay sendme : congestion control
  - relay drop : implement long-range dummies

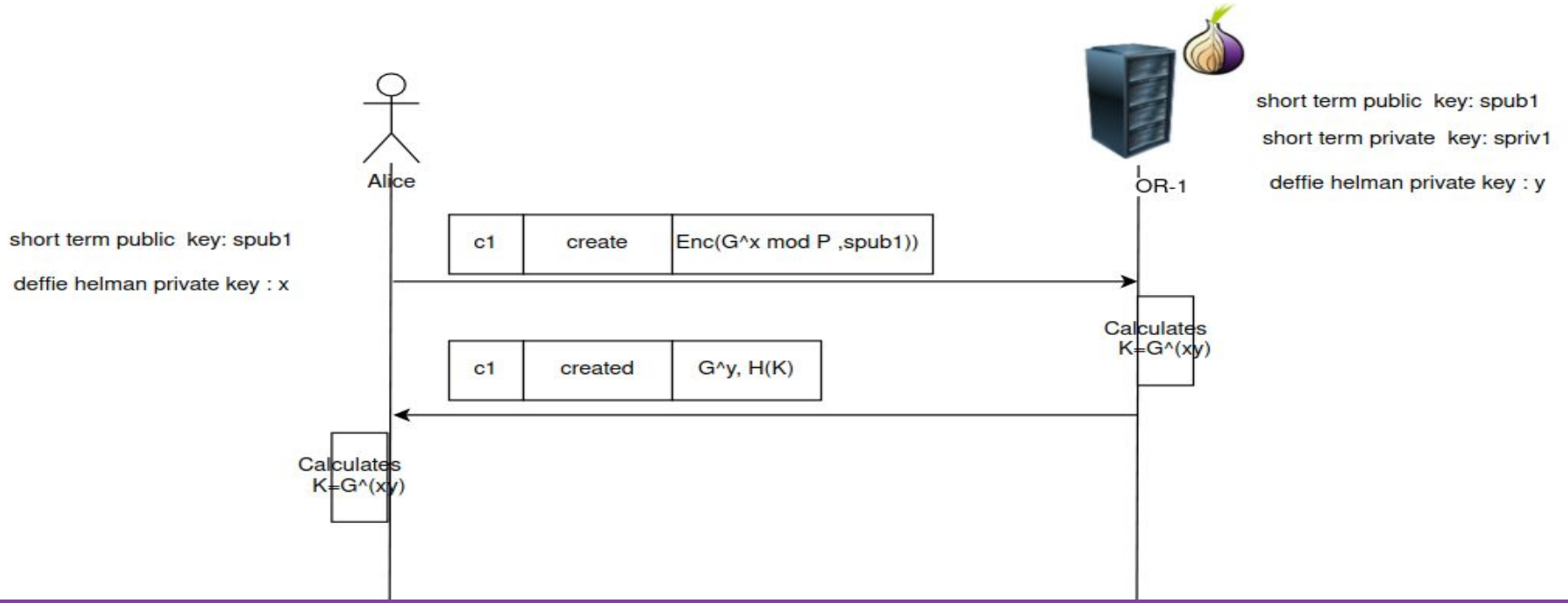


Relay cell

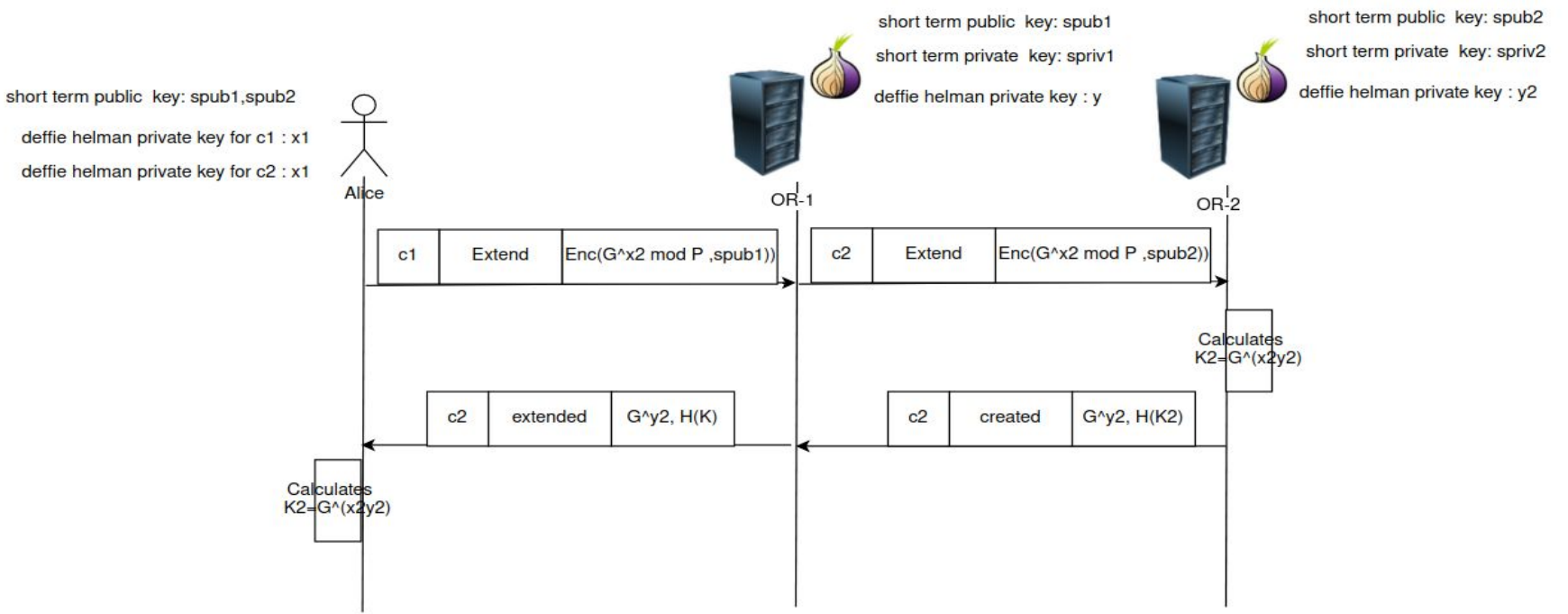
- data : 598B for command data



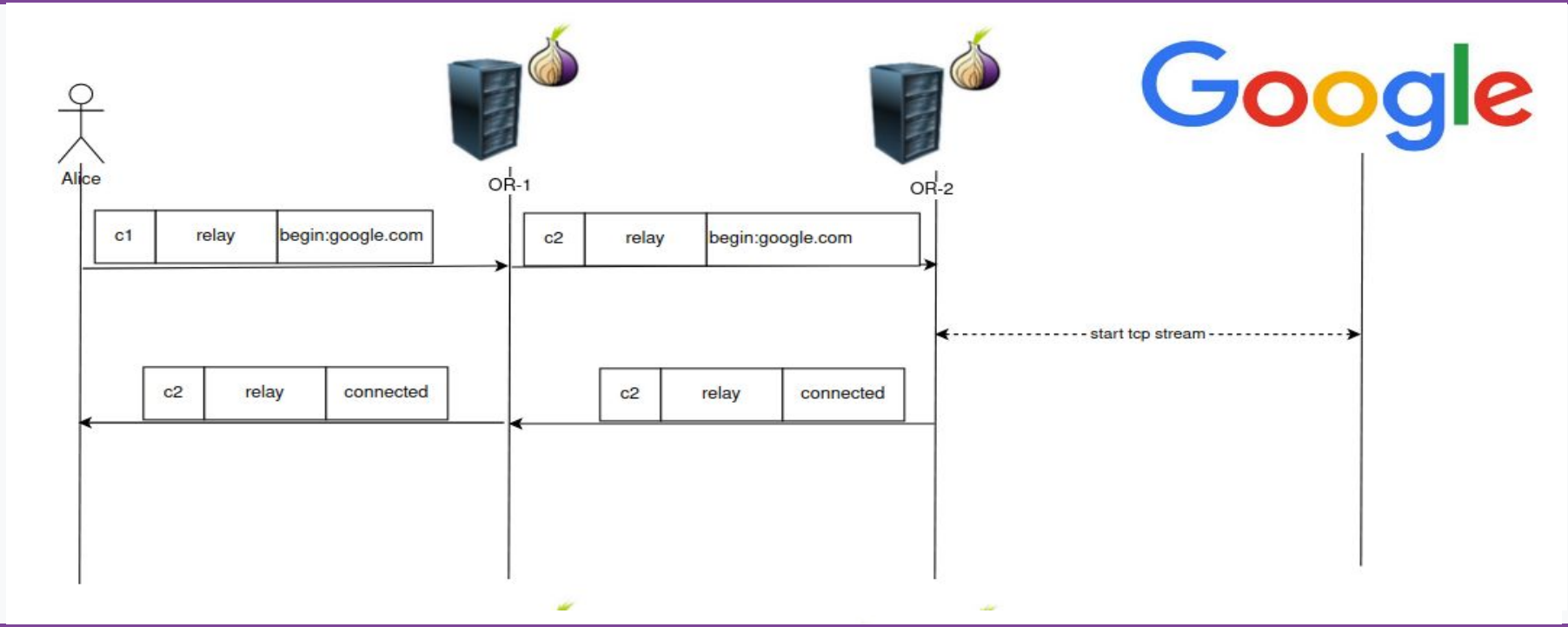
Circuit creation



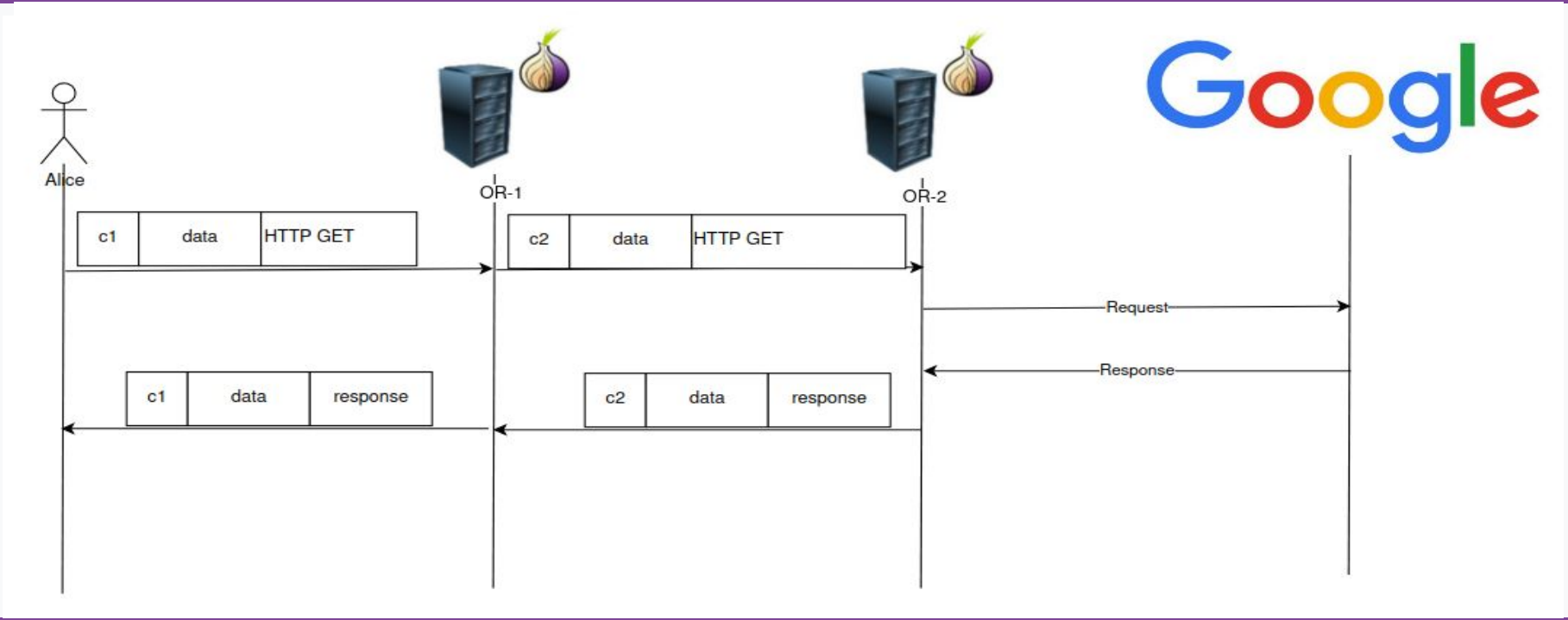
Circuit creation



Circuit creation



Circuit creation

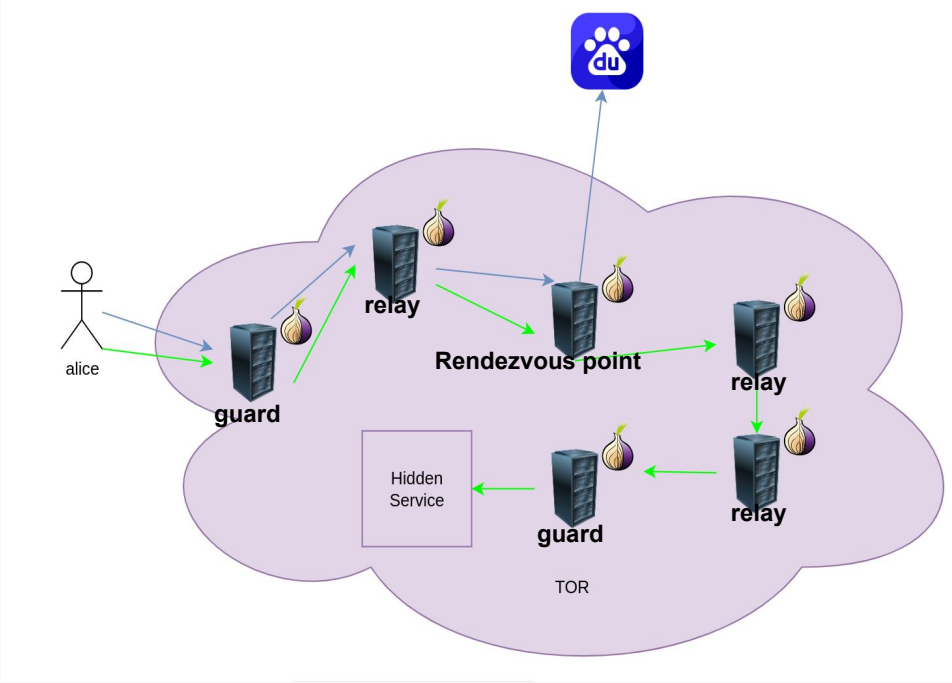


Types of nodes

There are couple types of nodes in a TOR:

- Guard node:the entry node
- Relay node : general term for node in a circuit
- Exit node : the exit
- Introduction nodes: Connects to the dark web
- Redenzous nodes: Connection point to the hidden service
- Authority node : a list of hard coded nodes which contain the data on all nodes in the network in a consensus file.They are trusted
- Hidden directory node : holds information about nodes in the network
- Bridge nodes : not publicly registered nodes in the tor network.

TOR Hidden services aka “The dark web”

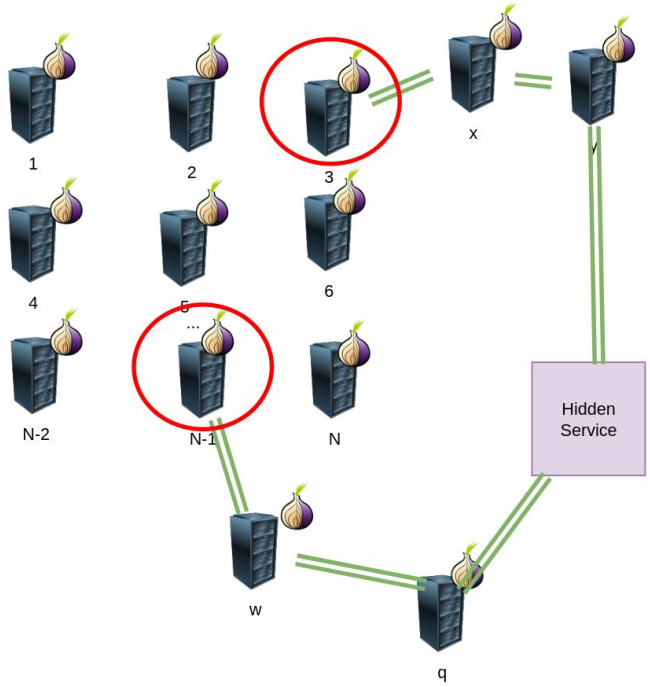


TOR Hidden services aka “The dark web”

- A famous component of TOR is the dark web where illegal stuff are done
- Unlike regular TOR where traffic goes in to TOR and exists to the regular internet,the traffic does not leave thee TOR network
- Traffic remaining in the dark web cannot be easily discovered.
- Unlike regular circuit there are 6 nodes in a connection to a “hidden service”
    - Alice<->Guard<->Relay<->Rendezvous point<->Relay<->Relay<->Guard<->Hidden service

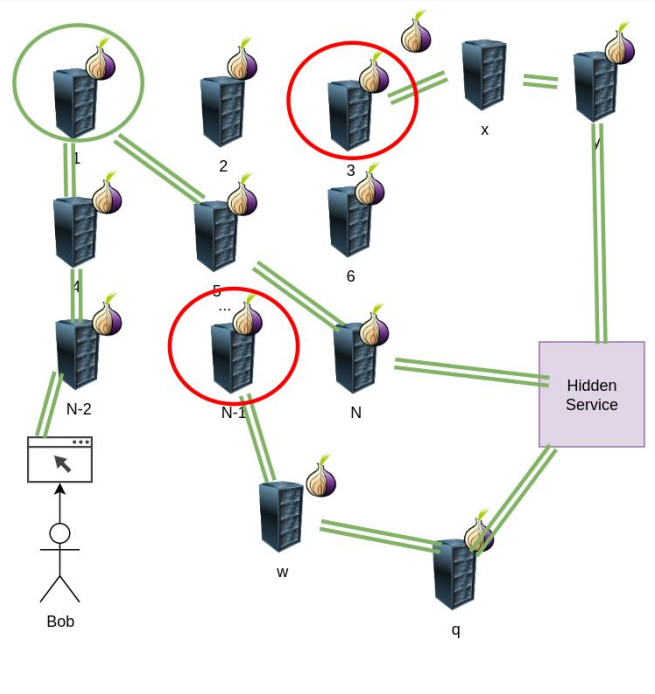
TOR Hidden services aka “The dark web”

- A hidden service creates circuits to a list of random relay nodes in the node circuits
- Each node in this list is known as “introduction point”
- Each “introduction point” does not know that it an introduction point
- The list of introduction points is then sent to the directory authority



TOR Hidden services aka “The dark web”

- A client wishing to connect to the hidden service queries the directory authority for a introduction point
- It creates a circuit known as introduction point ,sends details to random introduction point
- The hidden service then creates a circuit to the introduction point and then connects to the hidden service



TOR onion address

- Look different to regular website address
- Tor onion services are for hidden services only
- Onion services end with `.onion`
- Onion addresses have the following format:
  - Base32(public long term key| checksum of key | protocol version)

Site	Address
Facebook	https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/
bbc	https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/
nytimes	https://ej3kv4ebuugcmuwxctx5ic7zxh73rnxt42soi3tdneu2c2em55thufqd.onion/

TOR descriptor

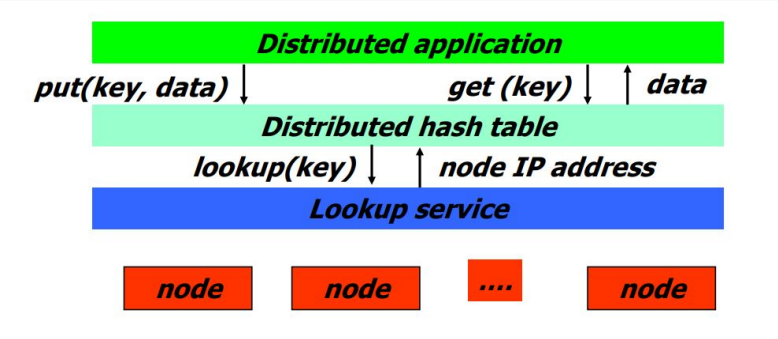
- A document that specifies information about a hidden service
  - This includes a list of all introduction points
  - This includes other parameters such as requirements for authentications
- The descriptor is published and is saved inside the HSDIR database

HSDir

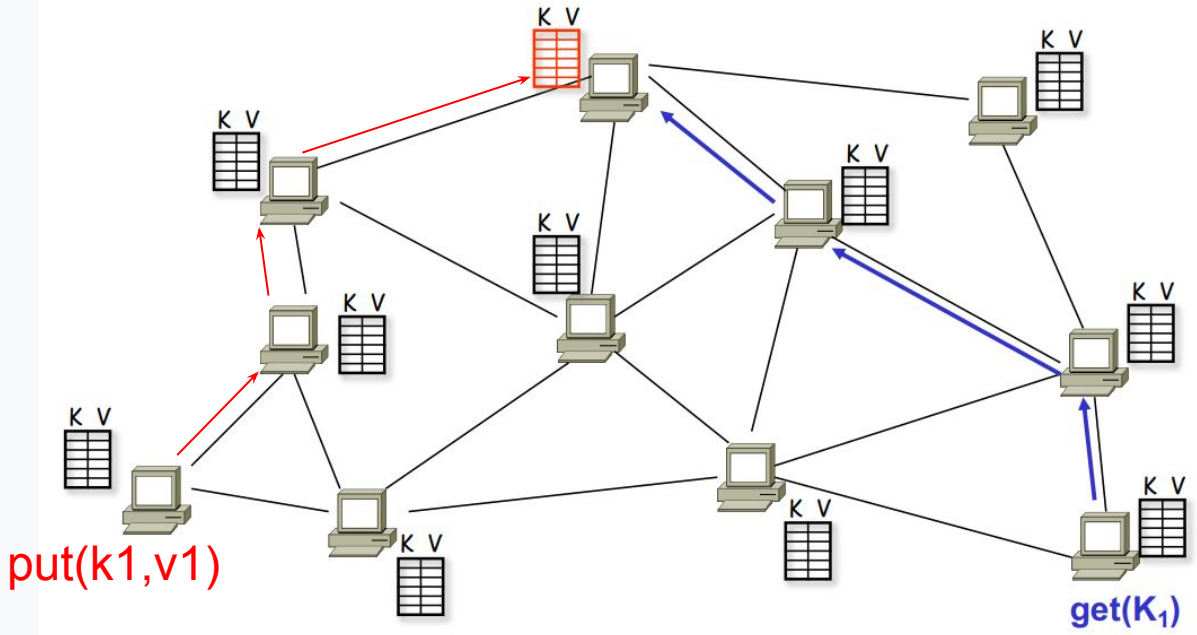
- Short for hidden service director server
- This is a distributed hash table database that keeps hidden service descriptors(a list of introduction points for hidden service)
- Client queries the table and can receive the descriptor

Theory: Distributed Hash Table

- Also sometimes known as key value store
- A type of distributed system that provides lookup services
- DHT may be distributed over many nodes(scalable)
- DHT are fault tolerant
- DHT do not have a central authority
- Supports put/get/delete/update API
- Does not impose any structure on keys



Theory: Distributed Hash Table

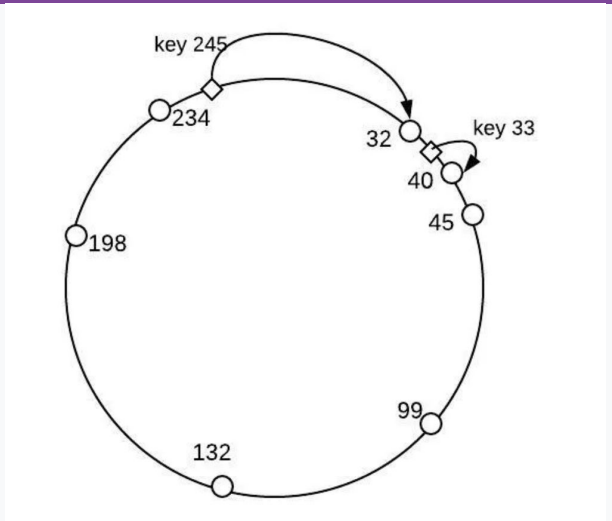


Theory: Distributed Hash Table

- The most popular DHT algorithms are Kademlia,Chord and Pasttry
- Most distributed DHT have an imaginary namespace geography:
  - Keys are mapped into some abstract geographic space
  - Routing is done by “closeness”

Theory: Distributed Hash Table

- Lets look for example at the Chord algorithm
- Each node has n-bit ID
- ID space is circular
- Date keys are also IDs
- Key is stored on next higher nod
- Consistent hashing
- Easy to find keys slowly by following chain of successors

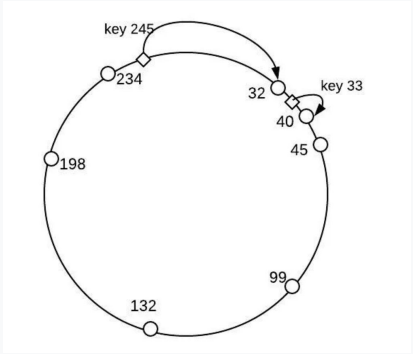


Theory: Distributed Hash Table

- The naive method has linear search time
- Chord improves it by holding a small “finger” table of size n
- Run time to find entry becomes O(log (# of nodes))
- Each entry i for node m holds the closest node by formula:
  - m+2^(i-1) mod 2^n

32

	position	node
0	32+2^0=33	40
1	32+2^1=34	40
2	32+2^2=36	40
3	32+2^3=40	40
4	32+2^4=48	99
5	32+2^5=64	99
6	32+2^6=96	99
7	32+2^7=160	198

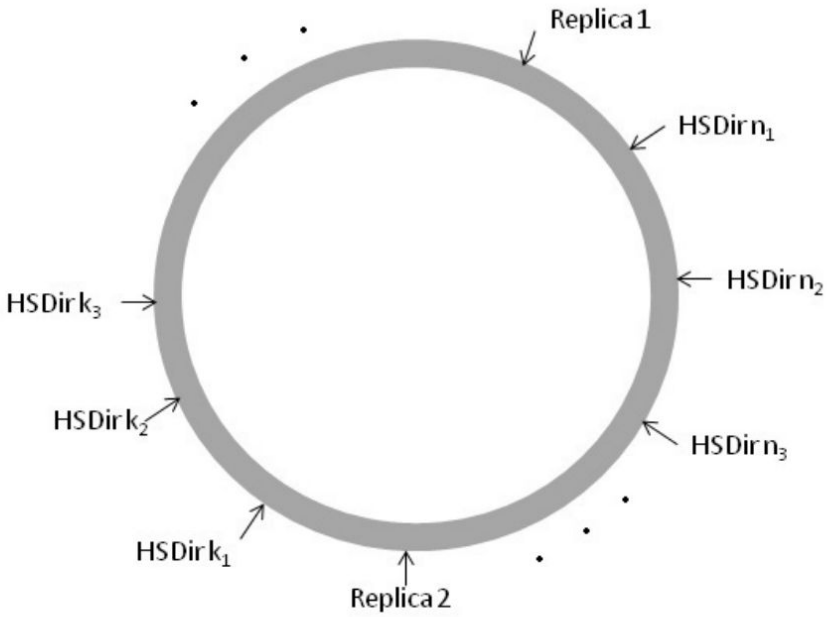


45

	position	node
0	45+2^0=46	99
1	45+2^1=47	99
2	45+2^2=49	99
3	45+2^3=53	99
4	45+2^4=61	99
5	45+2^5=77	99
6	45+2^6=109	132
7	45+2^7=173	198

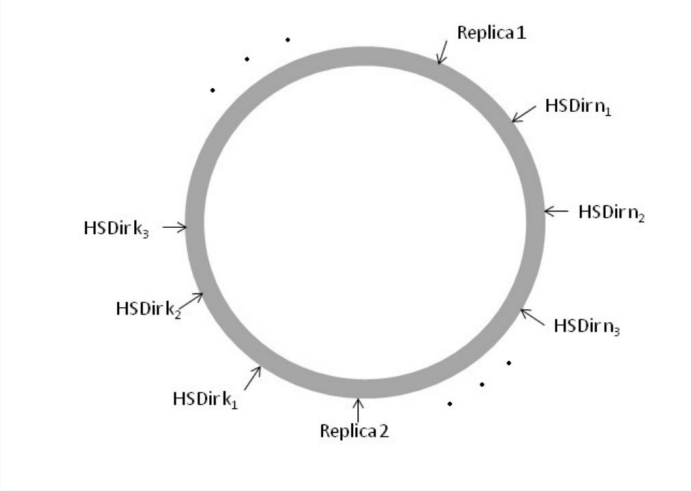
TOR DHT

- Tor uses a distributed hash table with a circular DHT space
- The space size is n=256
- The DHT space changes every 24 hours



Onion service creation and publication

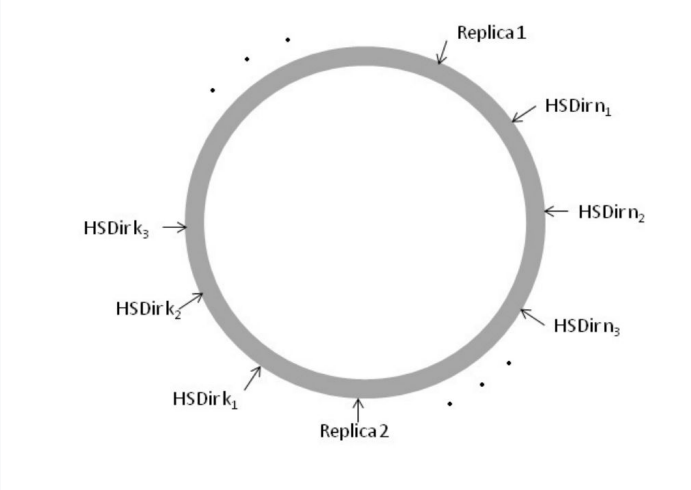
- To publish an onion service descriptor the onion service the service must find the responsible hsdir
- The index of HSDir on the DHT can be found by :
  - Index=Hash(“node-idx”|pub_{id}|S|N_{p}|T)
    - pub_{id}= public key of the known hsdir
    - S = shared random value
    - N_{p}= number of time period
    - T = default time period



Onion service creation and publication

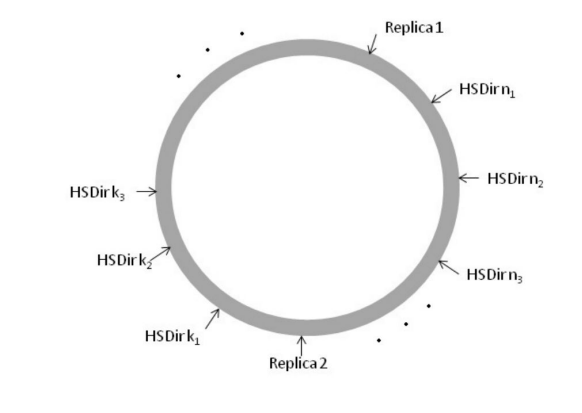
- Then the hidden service calculates the indices of its description
- The indices of the descriptors are calculated by:
  - for r in 1…R:

    Index=Hash(“store-at-idx”|pub_{b}|r|T|N_{p})
    - R=2
    - pub_{b}= blinded public key
    - r = number of dir
    - T = default time period
    - N_{p}= number of time period



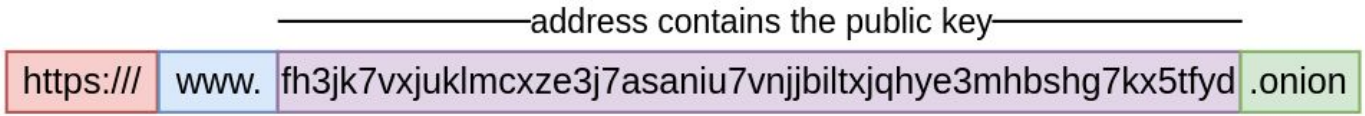
Onion service creation and publication

- After performing the calculation the onion service selects 4 HSDIRS on the DHT as the responsible dirs
- Notice that 2 replicase are selected
- The service then uploads the descriptor to the responsible table
- The blinded key is used as table index for the descriptor



how access to hidden service is done?

- Step 1 : The user discovers the onion address in some way
  - The address contains the public key of the website



how access to hidden service is done?

- Step 2: The user enters the address in the browser
  - The browser extracts the public key and computes the blinded public key
  - The browser then computes the DHT using S and T

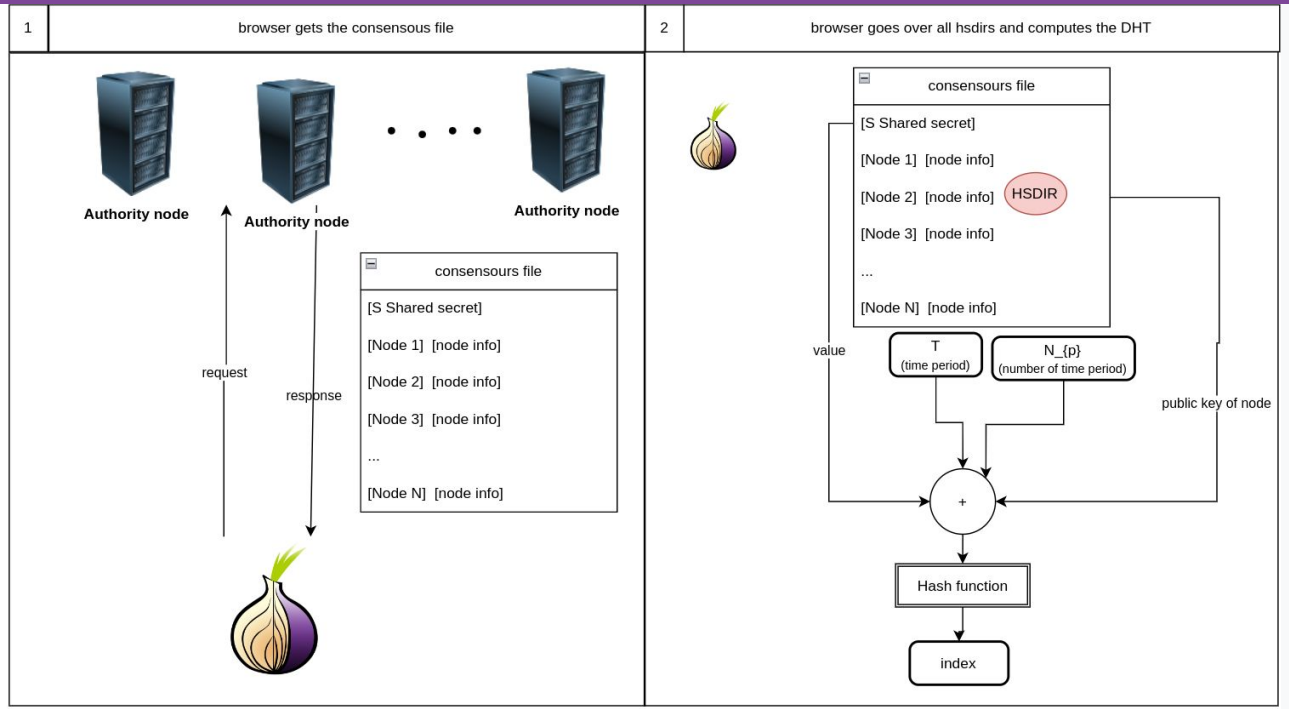
how access to hidden service is done?

- Step 3: The browsers finds out the introduction points
  - The browser requests the descriptor from the HSDIR using the blinded key as index
  - The browser then extracts from the descriptor the introduction point

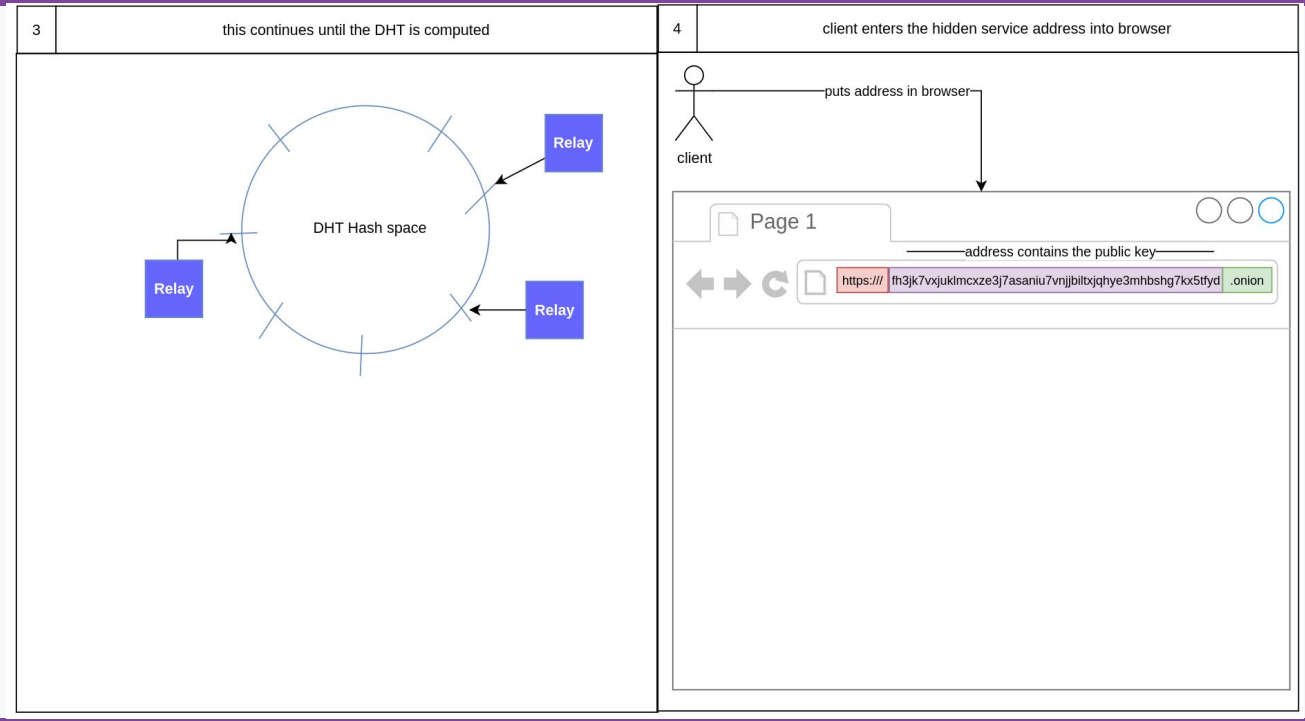
how access to hidden service is done?

- Step 4: The browsers creates a rendezvous point
  - It chooses the node at random
- Step 5 : The browser generates a special cookie with details about the rendezvous point
- Step 6: The browser sends a request to the introduction point
- Step 7: a circuit is created to the hidden service

Process summary



Process summary



Process summary

5	browser computes the blinded public key from the address + queries the HSDIR	6	browser retries the list of introdcution points from the descriptors

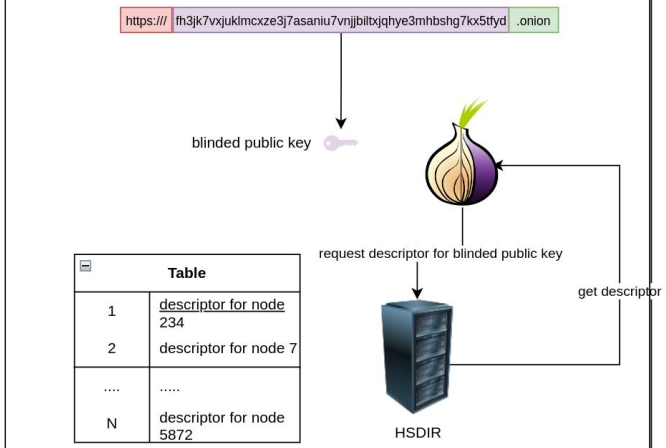
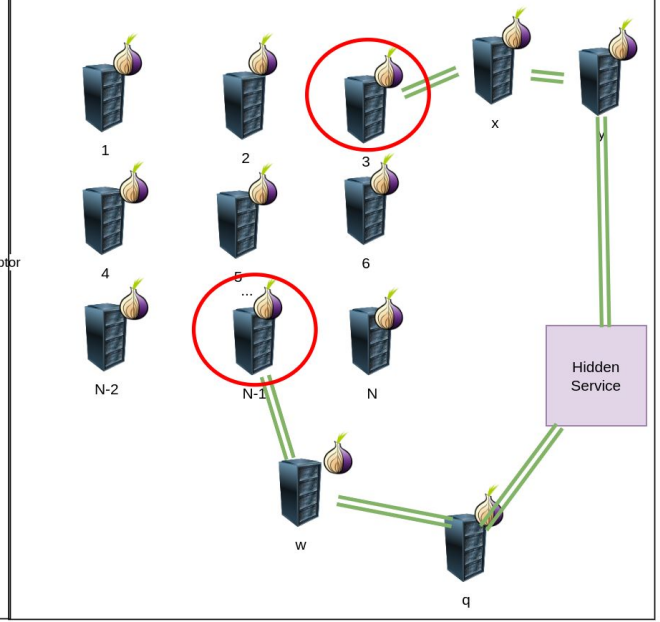
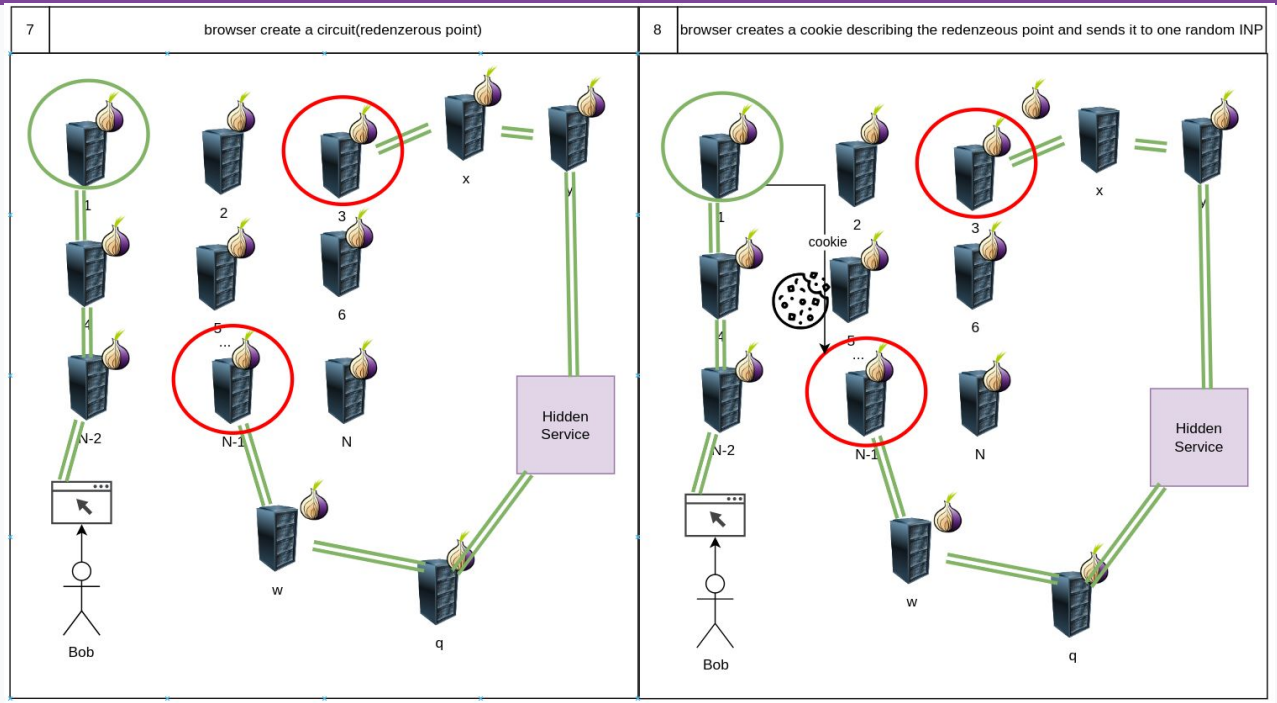


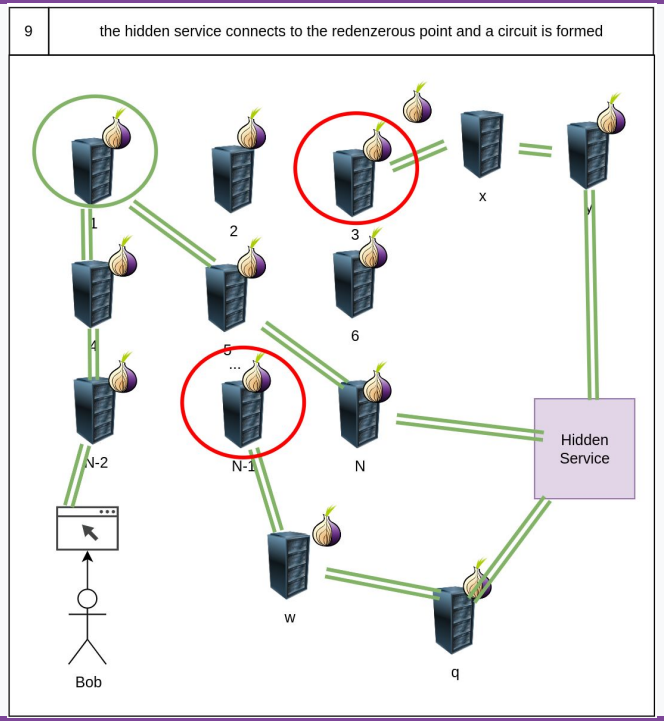
Table	
1	descriptor for node 234
2	descriptor for node 7
....	.....
N	descriptor for node 5872



Process summary



Process summary



TOR problems

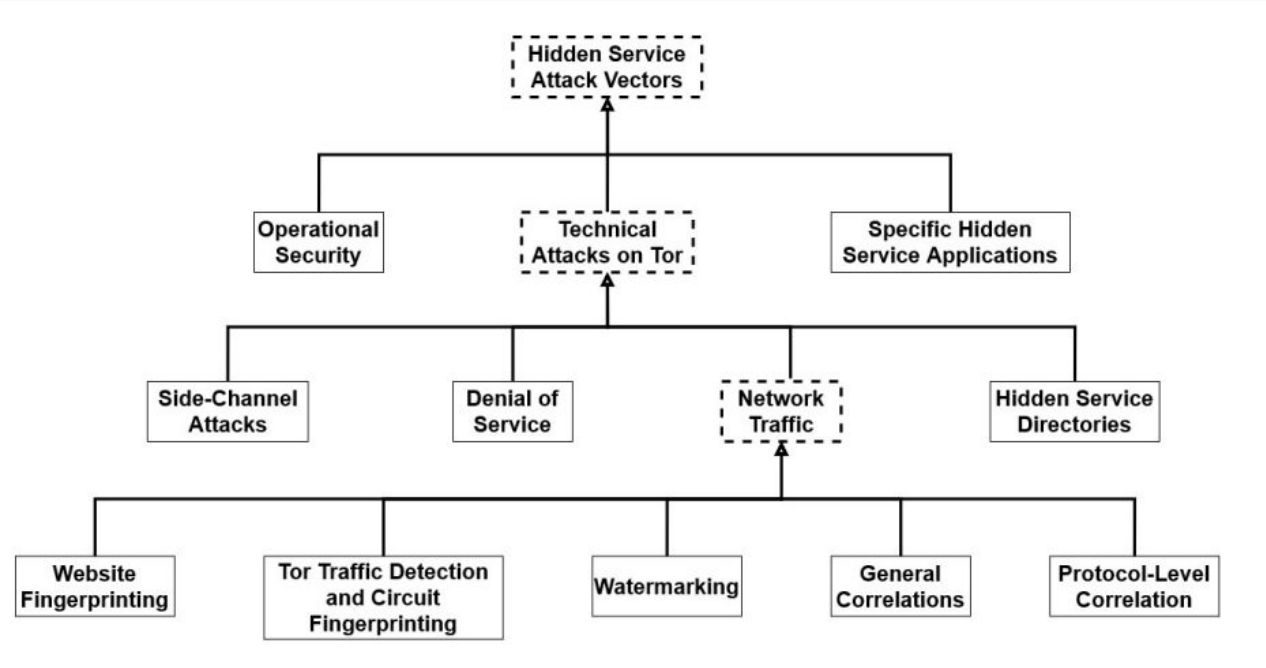
Known Tor design problems

- Although TOR is better then regular Internet it is still contains some known problems
  - If an attack controls all three nodes she can identify the user
  - If an attack controls both guard and exit node she can with high probability deanonymize the user
    - “Traffic correlation attack”
    - Works regardless of circuit length
    - Can be used by a powerful adversary who can observe large number tor nodes

Known Deanonymization techniques

- Also Tor is vulnerable in implementation level
  - SOCKS5 might leak DNS requests and reveal your identity
  - /server-status attack
  - hidden service certificate might listed on regular internet
  - Downgrade HTTP protocol attack
  - SSL heartbleed attack

Classification of attack vectors



Honorable mentions

Honorable mentions

There are couple of interesting topics in TOR which were not covered

- OnionBalance
- Bridges
- Proof of work, rate limiting and digital signatures mechanisms for anti ddos protection
- Vanguards
- Pluggable Transports
- How to actually use TOR
- How to use TOR and remain anonymous
- Famous sites in the dark web

Resources

- See attached links

Thank you!

Bonus: podcasts about TOR

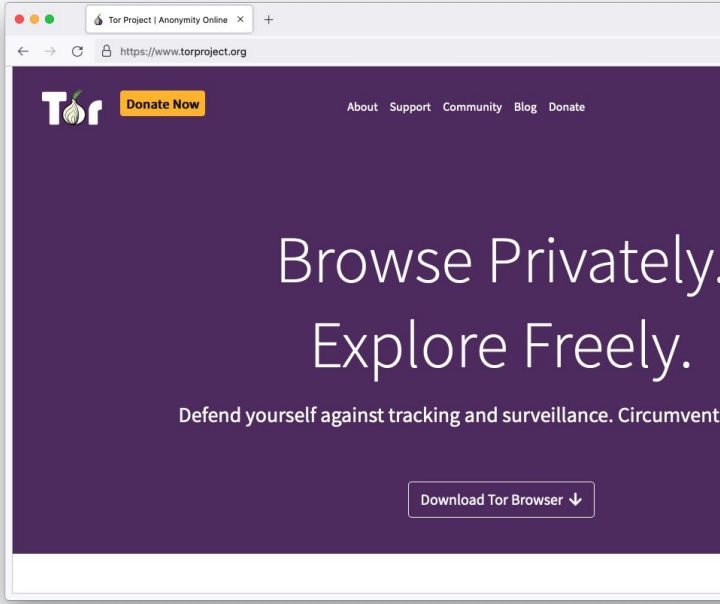
Podcast

Podcast name	episode	Description	Link
Darknet dairies	131: welcome to video	• The largest minor sex trafficking website	https://open.spotify.com/episode/5MHPoDQKo59beLkISWDscT?si=sGUGLe2GRy6C4pB028ztDw
Darknet dairies	104: arya	• This episode focuses on the life of a young man who used Tor to access darknet marketplaces and purchase drugs. • It provides a personal perspective on the risks and allure of navigating the darknet through Tor.	https://open.spotify.com/episode/3bapFgoW8rrq2YftGN5aHj
Darknet dairies	24: operation bayonet	• This episode delves into the takedown of AlphaBay, a major darknet marketplace. • It sheds light on how Tor is used by darknet vendors and marketplaces to mask their identities and locations.	https://open.spotify.com/episode/4sMVVjgOfN4DixQkk3pUcu

Bonus: About Tor Browser

What is Tor Browser?

- Just like any other browser (Chrome, Firefox, Safari, Yandex) except it does not expose traffic.
- Traffic is encrypted and bounces through three random volunteer-run nodes called **relays**.



What is Tor Browser?

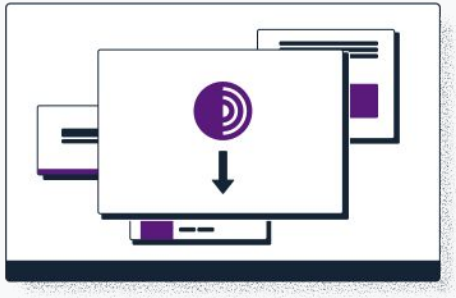
- Tor Browser = little-t tor + patched Firefox
- Anyone snooping can’t see the websites you visit.
- Websites can’t track you or see other sites you visit (cross-tracking).
- Prevents other privacy violations like fingerprinting or third-party cookies.
- Writes nearly nothing to disk.
- No browser history.
- Cross platform: Windows, macOS, Linux and Android.

Multilingual Browser

- Tor Browser is available in 37 languages in a **single multi-locale download**, which can be changed using the menu in General settings: https://www.torproject.org/download/languages/
- Tor Browser manual is a user-friendly guide for novice users and is also multilingual: https://tb-manual.torproject.org/

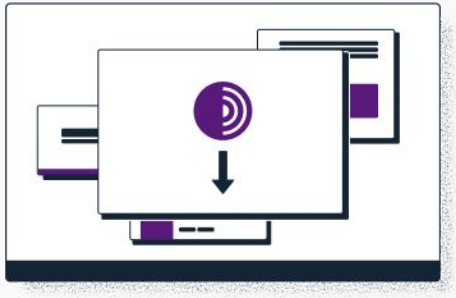
Downloading Tor Browser

- The safest way to download is from: https://torproject.org
- Downloading Tor Browser from a non-official source is dangerous!
- If https://torproject.org is blocked, try mirrors
  - https://tor.eff.org/
  - http://tor.calyxinstitute.org/ (if HTTPS is blocked)

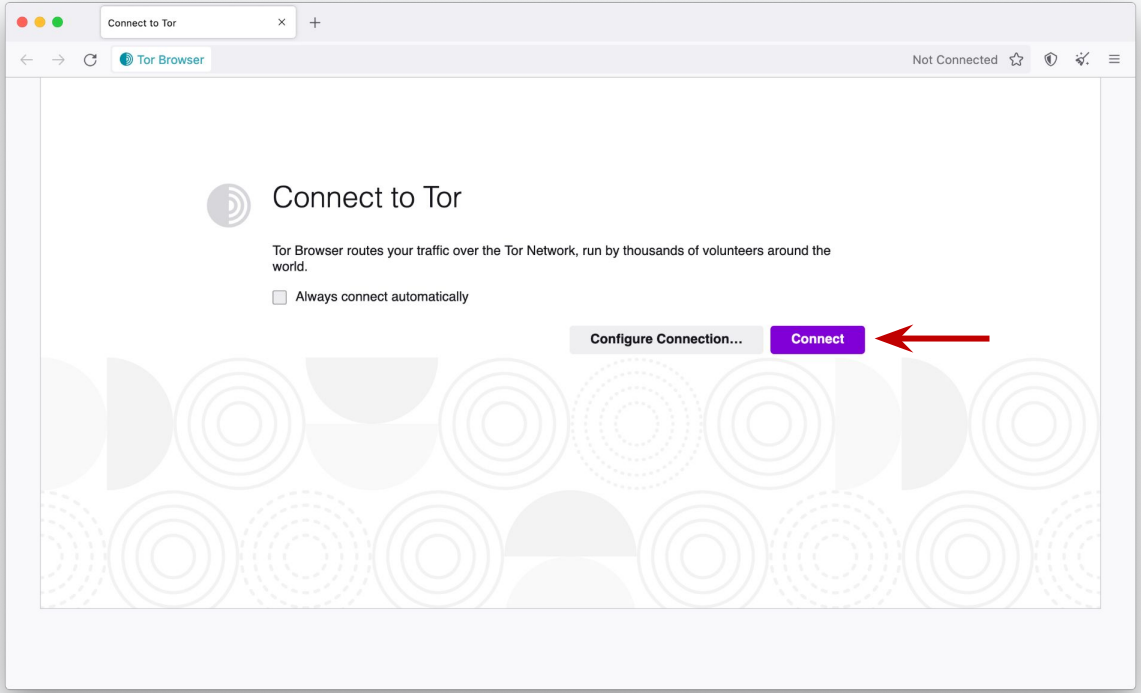


Bypassing censorship of torproject.org

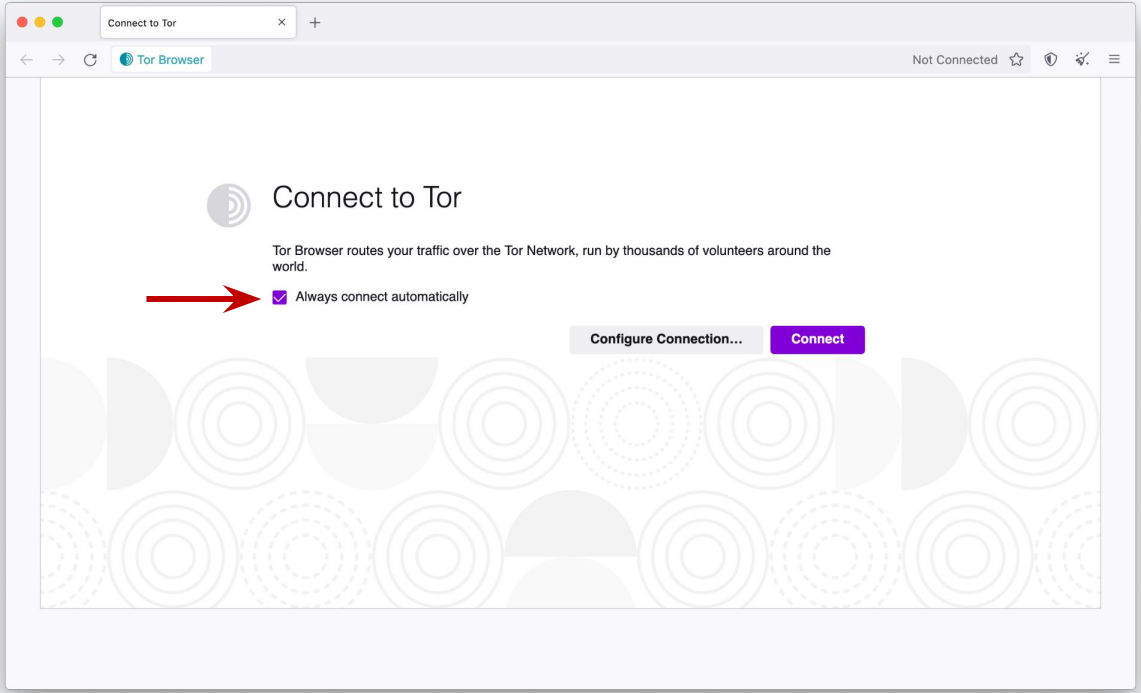
- Tor Project website and mirrors could be blocked on your network making it more difficult to download Tor Browser.
- Alternative
  - Emailing GetTor to receive links to download Tor browser: gettor@torproject.org (from a Gmail or Riseup email)
  - Messaging @GetTor on Telegram: https://t.me/gettor_bot



Running Tor Browser for the first time



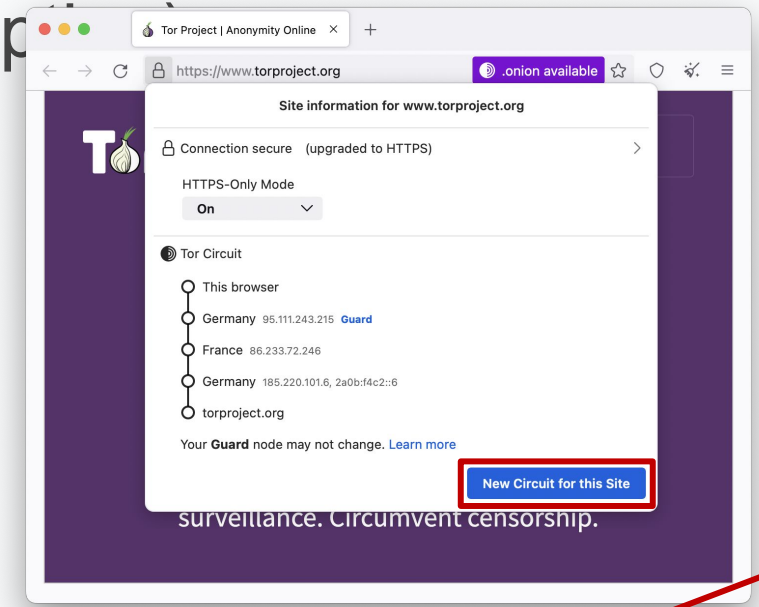
Choose to connect to Tor automatically

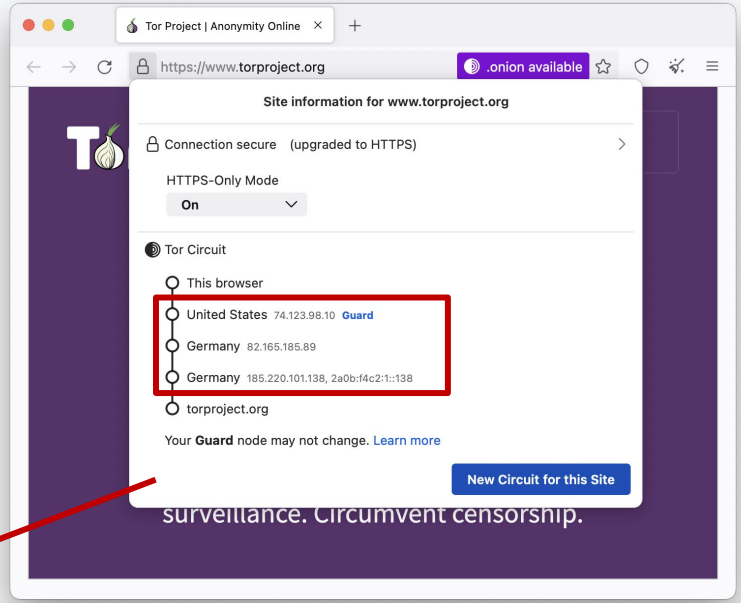


Using Tor Browser

- Default search engine: DuckDuckGo
- Bundled with privacy-preserving extensions such as NoScript.
- You should not add any other extensions nor enable any plugins!
- Advice: websites won’t know anything about you unless you login and tell them (e.g. logging into Facebook).

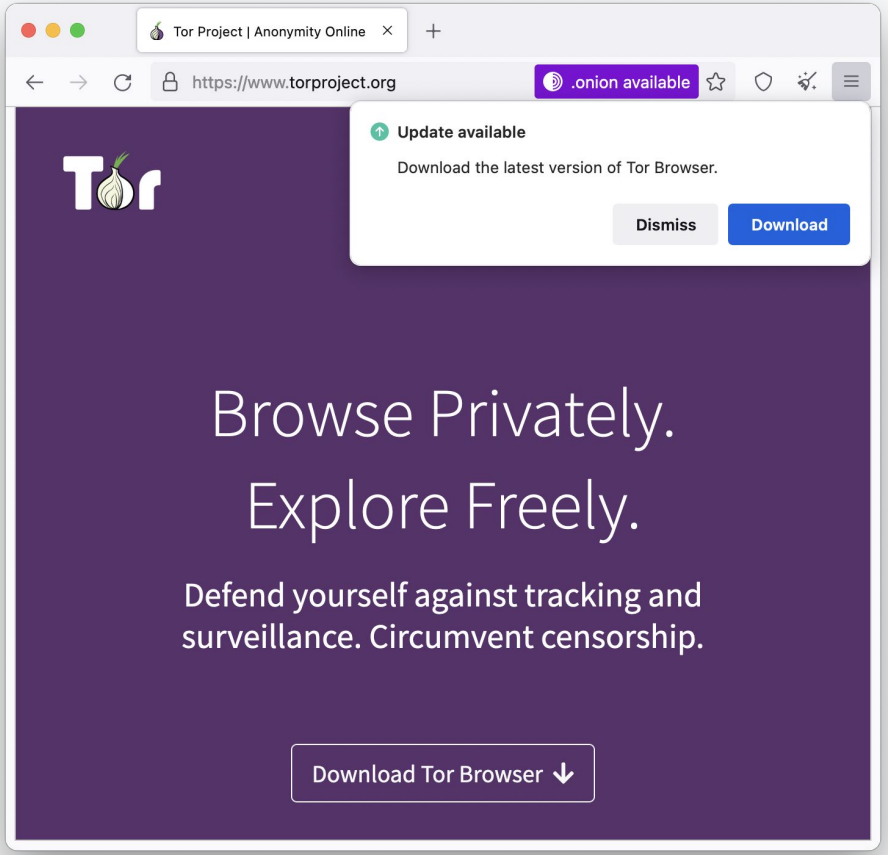
Clicking on the padlock will show your current Tor circuit (and “New Circuit for this Site” op





Updating Tor Browser

Every update brings new features and resolves security vulnerabilities.



Uninstalling Tor Browser

- Uninstalling Tor Browser is as easy as moving the folder to the trash! Then, emptying the trash.
- Default Tor Browser folder locations:
  - **Windows:** Desktop
  - **Linux:** home, or look for a name like “tor-browser_en-US”
  - **MacOS:** Move the Tor Browser application to Trash and also the TorBrowser-Data folder (~/Library/Application Support/)

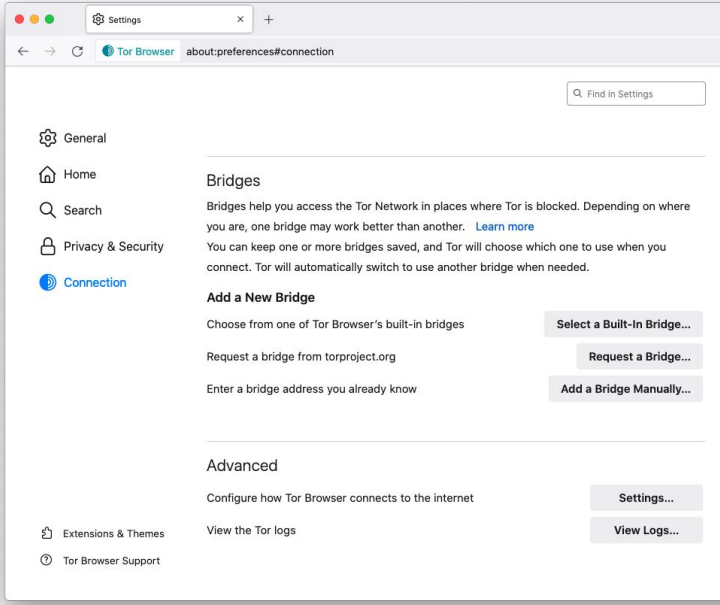
Troubleshooting Tor Browser

- Is your system clock correct?
- Is the browser already running?
- Are you being censored?
- Is your antivirus or firewall blocking Tor?
- Do you have a very old operating system?
- Try uninstalling and reinstalling
- Get help at https://support.torproject.org

What to do when Tor is blocked

When the connection to Tor is censored

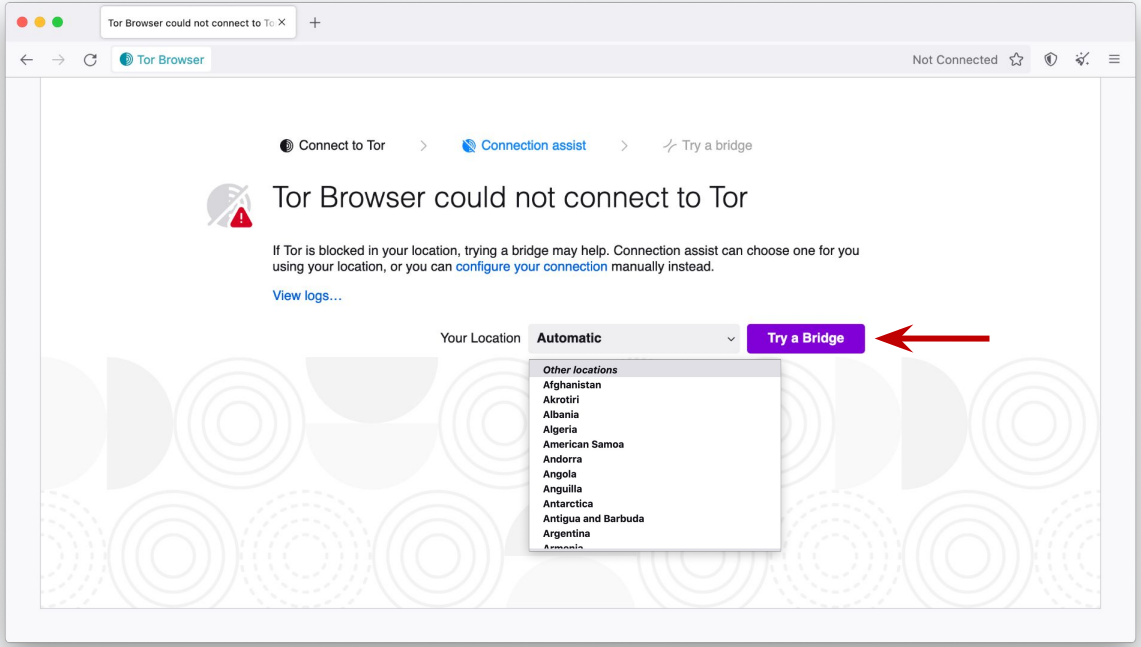
- Direct access to Tor may be blocked by some Internet Service Providers and governments.
- Tor Browser includes circumvention tools for getting around these blocks called **bridges**.
- Bridges are **relays that are private** and harder to block.

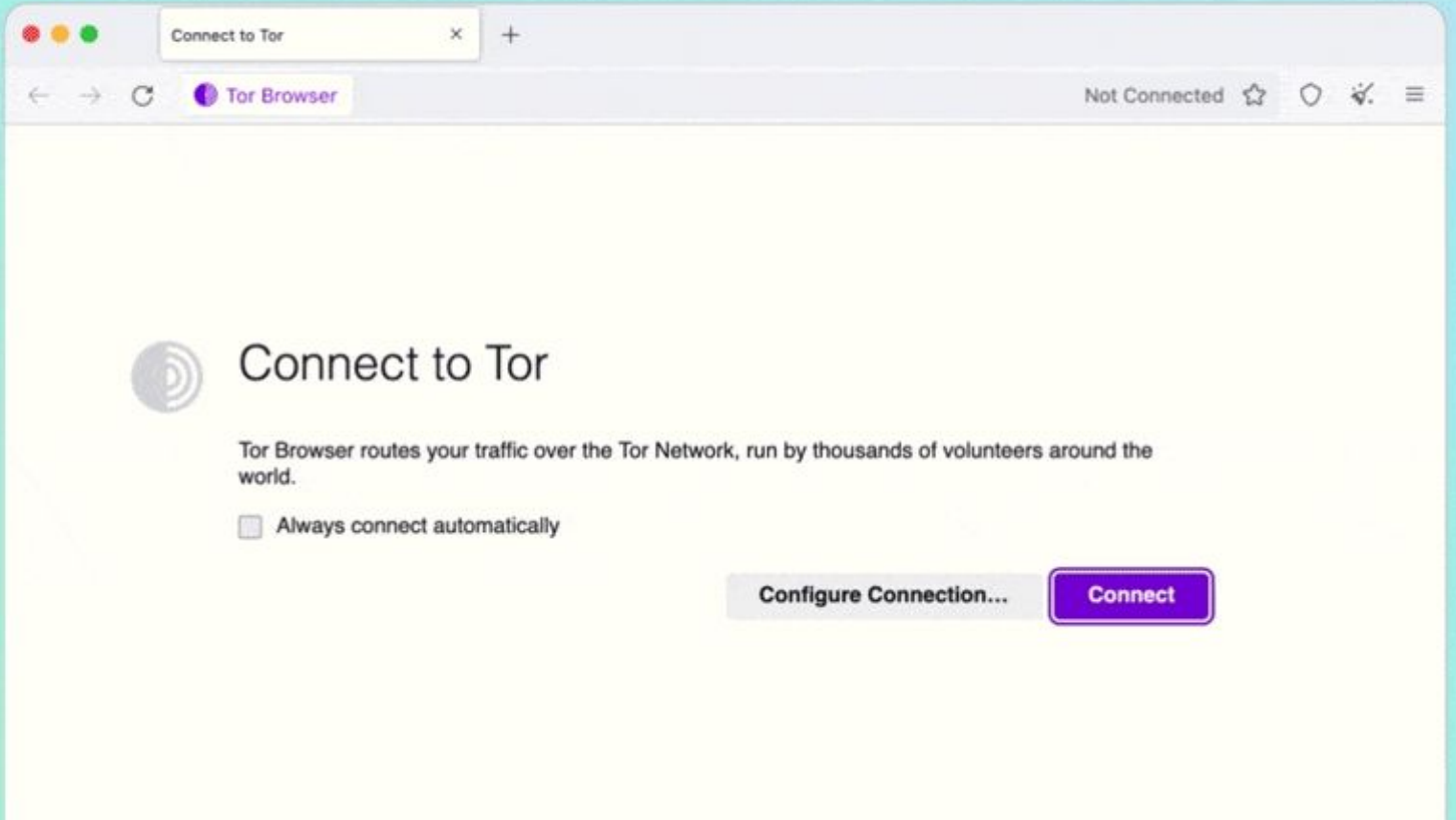


Meet “Connection Assist”

- Connection Assist is a new feature for users burdened by censorship.
- When Tor is blocked, Connection Assist will offer to automatically apply bridge configurations that might work best in a user’s location.
- Users can still configure settings manually!

“Connection Assist” helps users configure bridges




Connect to Tor
Tor Browser
Not Connected
Connect to Tor
Tor Browser routes your traffic over the Tor Network, run by thousands of volunteers around the world.
Always connect automatically
Configure Connection...
Connect

Configuring bridges manually

- You can get bridges from:
  - Tor Browser: “Select a Built-In Bridge” on Tor Browser
  - Tor website: https://bridges.torproject.org
  - From a trusted source:
    - Telegram: https://t.me/getbridgesbot
    - By sending an email to bridges@torproject.org from Gmail or Riseup

Pluggable transports

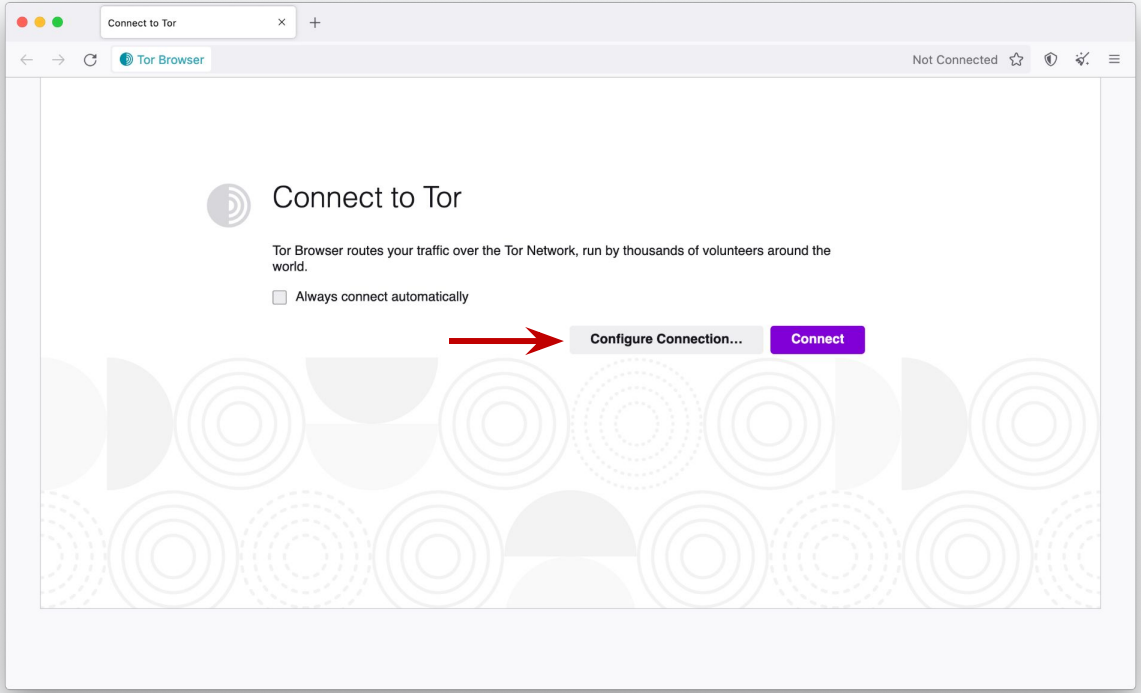
Pluggable transports can be used like bridges to disguise Tor traffic (also called “built-in bridges”). Main types of pluggable transports:

- **obfs4:** makes Tor traffic look random; works in many situations (if not, try meek-azure).
- **meek-azure:** makes it look like Microsoft traffic; works in China.
- **snowflake:** proxies traffic through temporary proxies using WebRTC. See: https://snowflake.torproject.org.

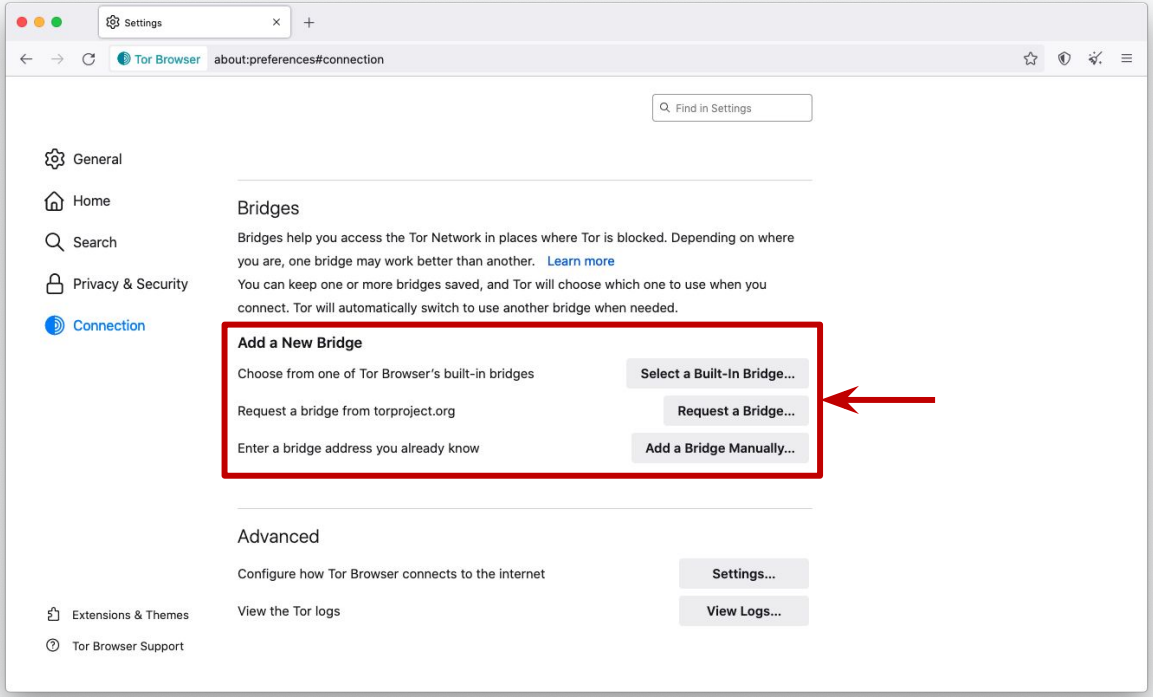
Snowflake

- Snowflake helps you avoid being noticed by Internet censors by making your Internet activity appear as though you're using the Internet for a regular video or voice call.
- Unlike VPNs, you do not need to install a separate application to connect to a Snowflake proxy and bypass censorship.
- It is usually a circumvention feature embedded within existing apps: Tor Browser, Onion Browser, and Orbot.

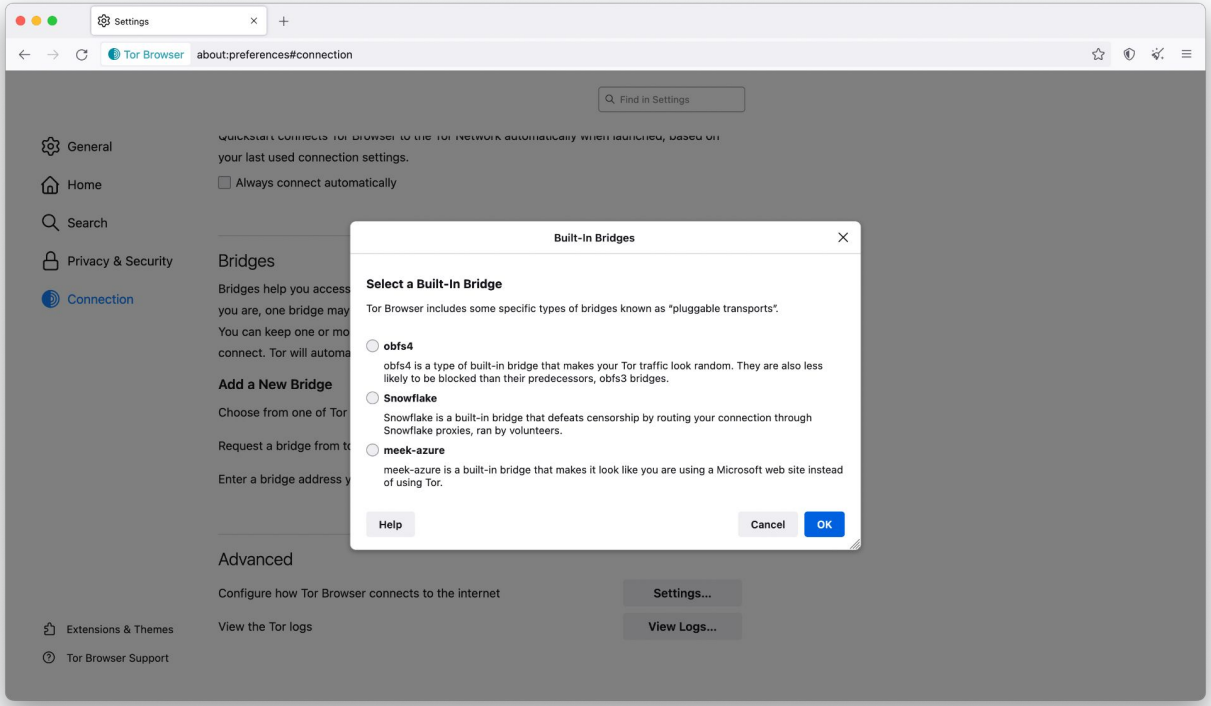
Bridges and pluggable transports



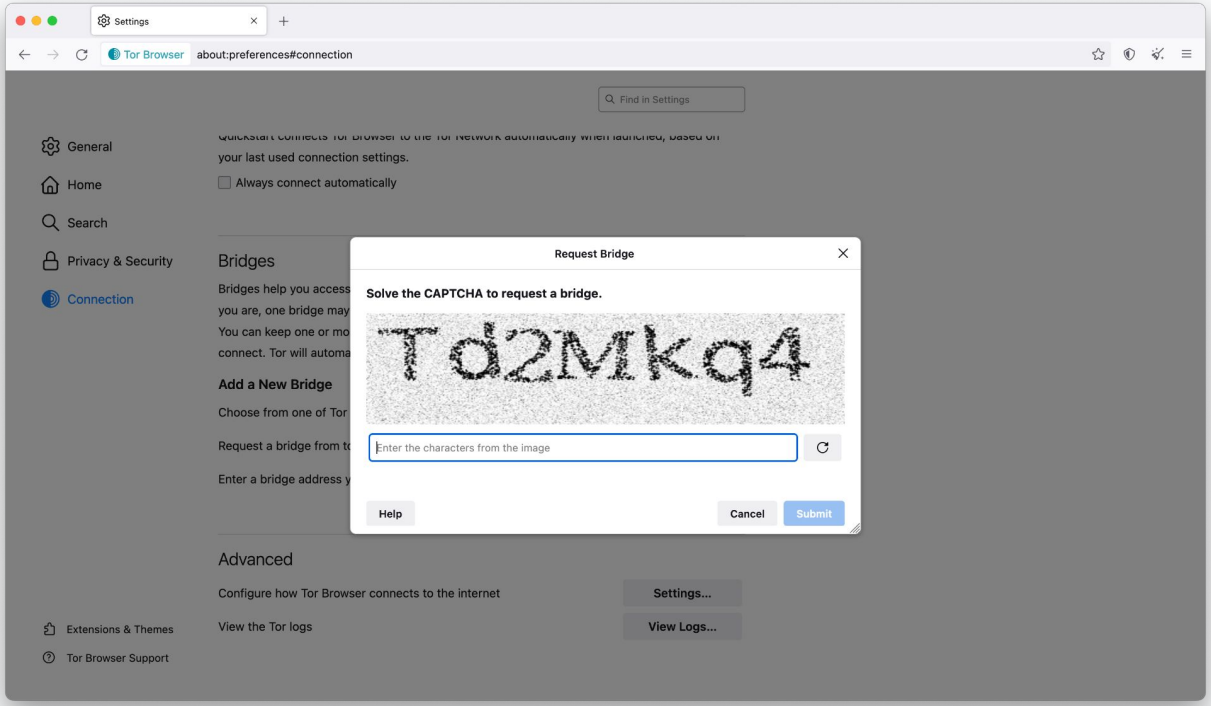
Bridges and pluggable transports



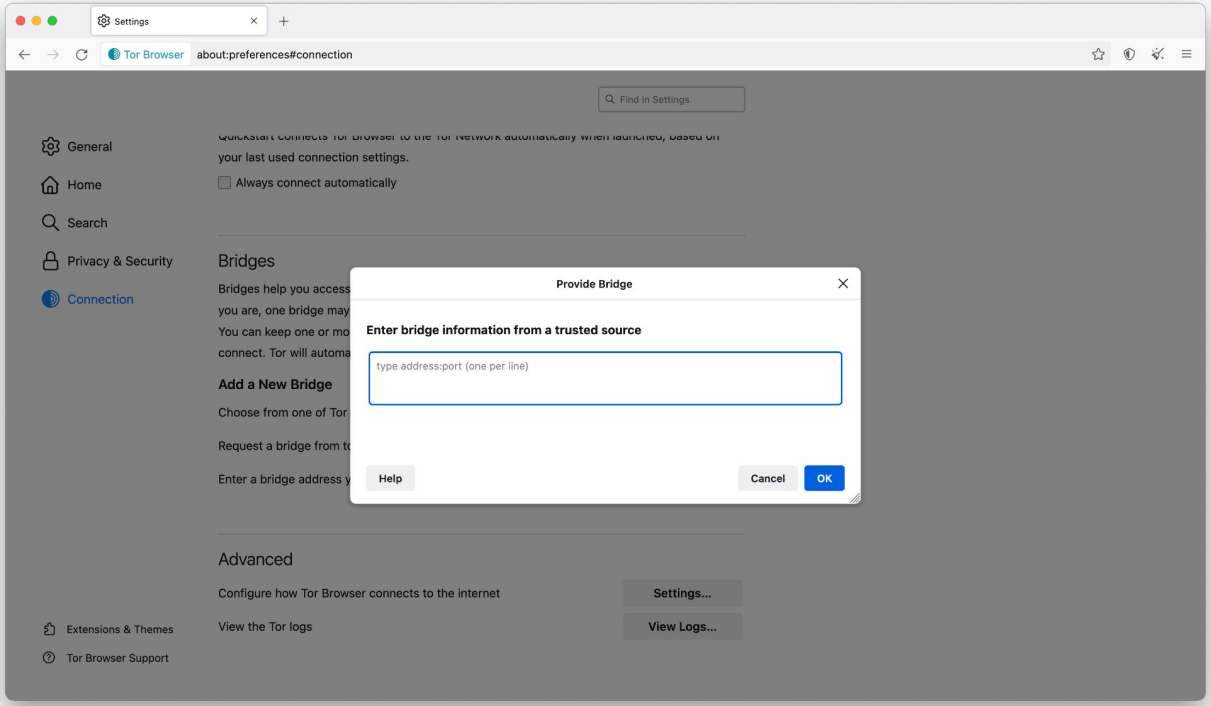
Choose a bridge from one of Tor's built-in bridges



Request a bridge from torproject.org

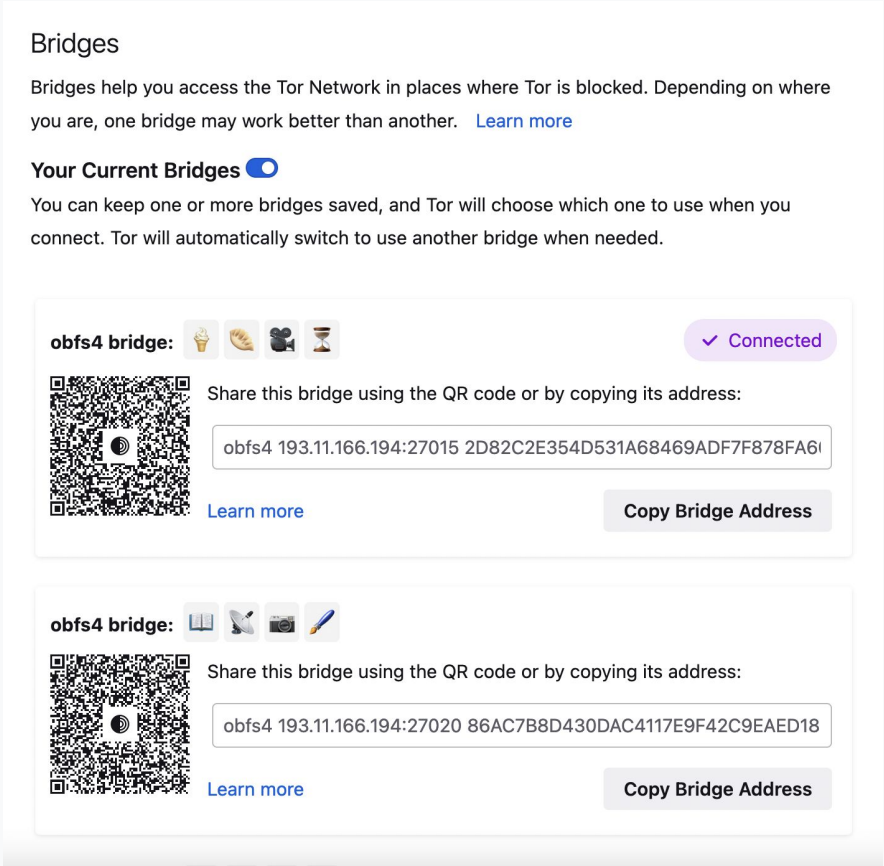


Enter a bridge address you already know



Bridge cards

Saved bridges appear in a handy stack of bridge cards including new options for sharing bridges too.



Open Observatory of Network Interference

- Open Observatory of Network Interference: https://ooni.org/
- Country-level reports of specific online censorship tools in use.
- Explore aggregated reports: https://explorer.ooni.org/
- Or use your own OONI Probe to measure Internet censorship: available in App Store and Google Play.

More Tor Browser

Obscures your Real IP Address

Prevents Network Observation

Prevents Location Determination

Prevents Fingerprinting

Prevents Cross-Site Correlation

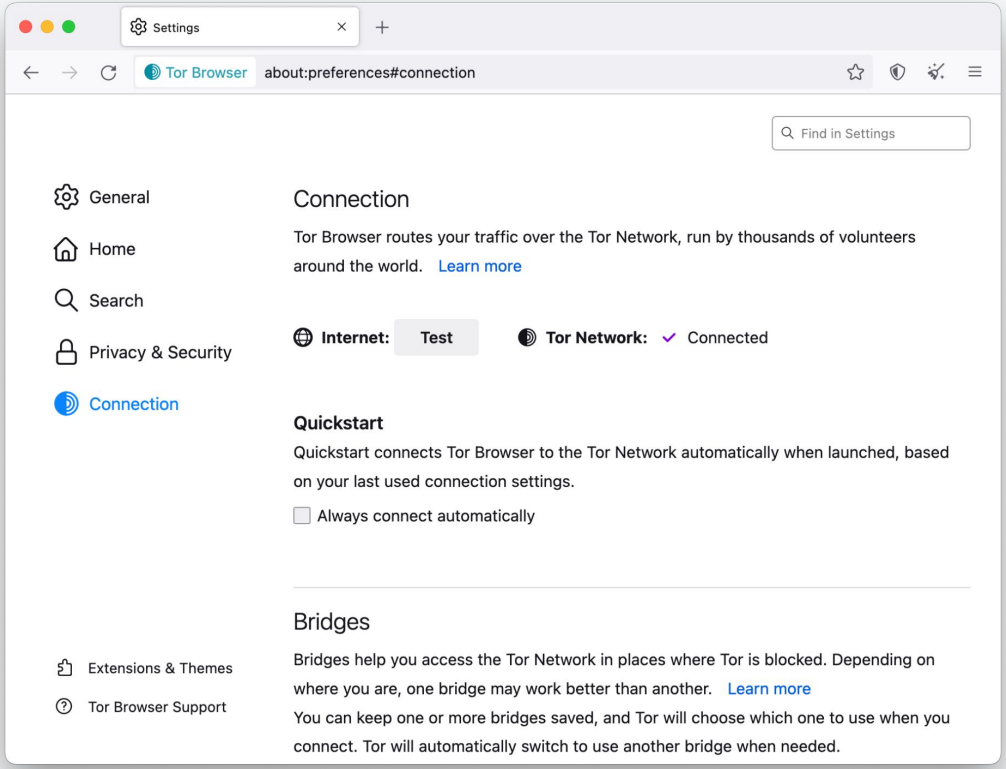
Isolates Cookies & Scripts

Writes Nothing to Disk

No Browser History

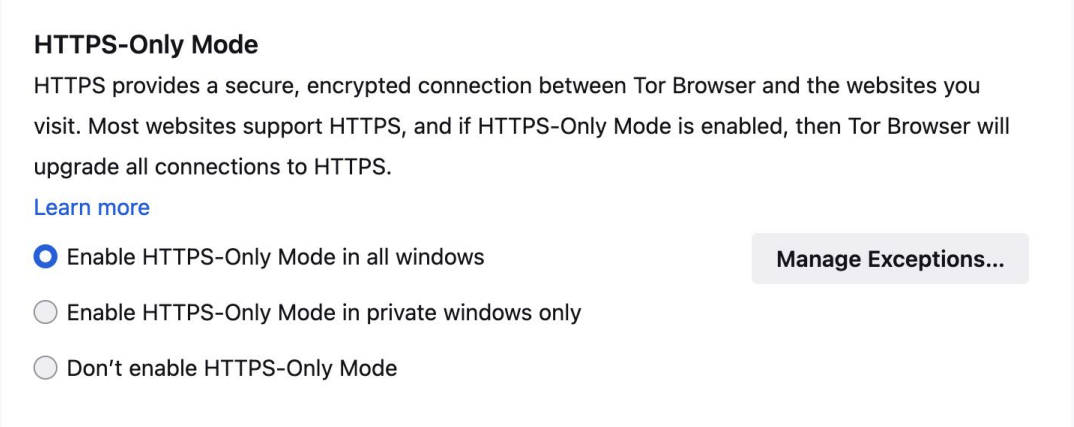
Connection Settings

Connection settings include connection statuses, censorship mitigation options, access to Tor log, etc.



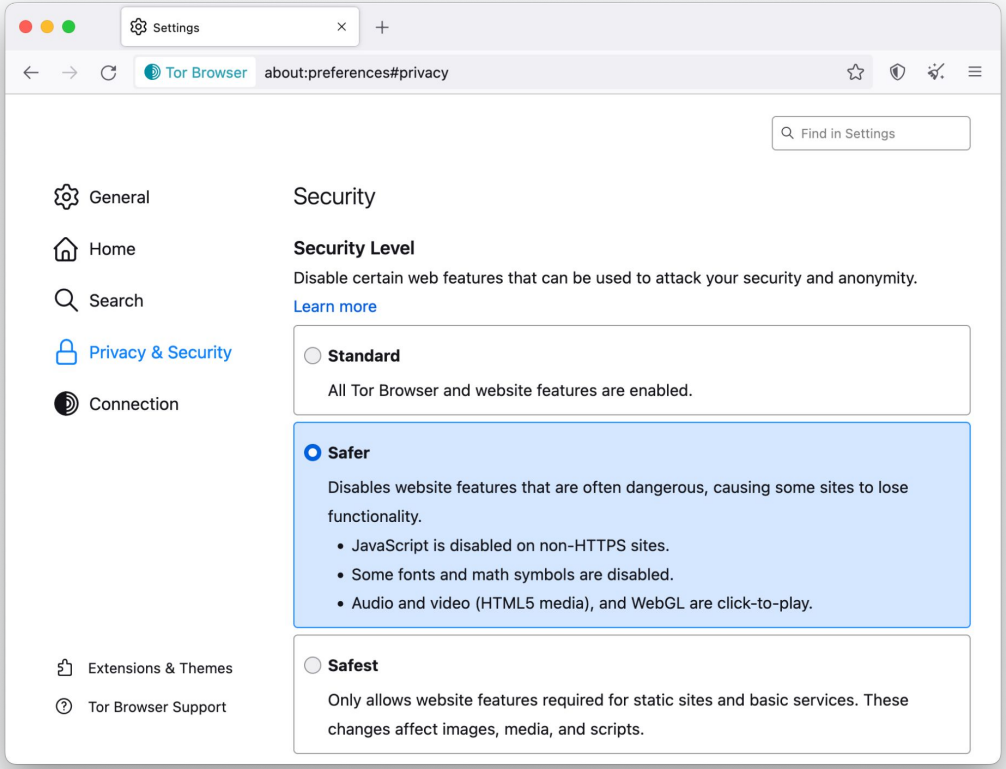
HTTPS-only mode

HTTPS-Only Mode is enabled by default for desktop and HTTPS-Everywhere is no longer bundled with Tor Browser.



Security Slider

Recommended security level: safer or safest.

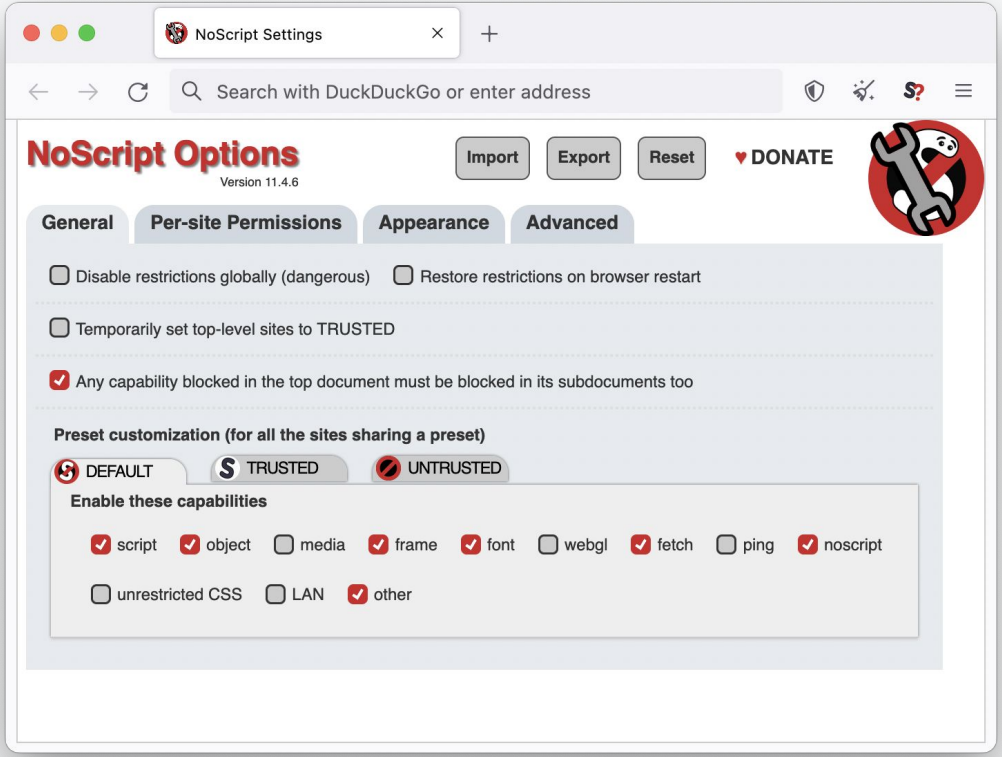


NoScript

Not advisable to change settings in the NoScript “options” menu.

Adding sites to the “whitelist” can result in fingerprinting.

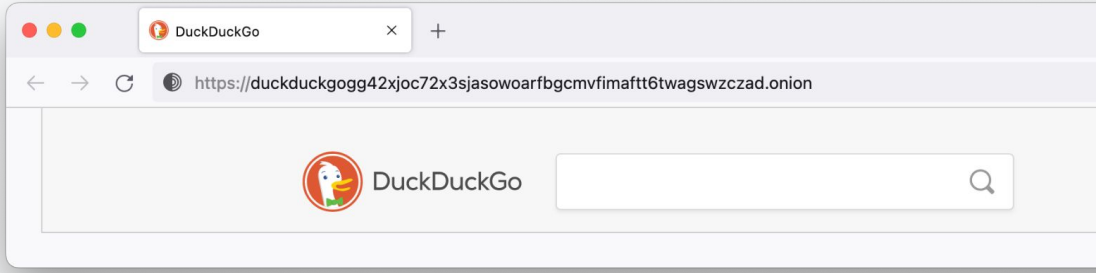
Instead, “temporarily trust” blocked objects, or use security slider (Standard, Safer, Safest).



DuckDuckGo

DuckDuckGo is the default search engine in Tor Browser.

Using Tor Browser prevents DuckDuckGo from tracking users, even if they wanted to (they claim not to).



https://www.duckduckgo.com/ or
https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/

Plugins, add-ons, JavaScript

- Do not add any new add-ons/extensions to Tor, and don’t enable any plugins.
- JavaScript is enabled by default, but is sanitized to preserve anonymity.
- To prevent possible JavaScript vulnerabilities, use the “safest” setting in the security slider.

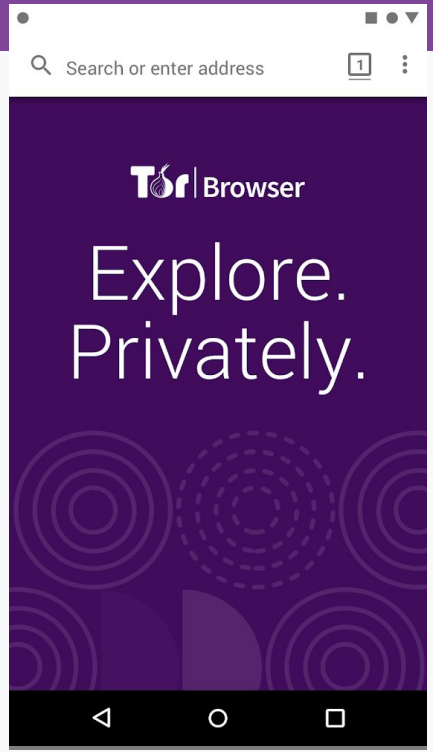
Mobile Tor: Tor-powered apps

Things to know about mobile Tor

- The design of mobile devices makes full privacy impossible.
- Mobile Tor is best for censorship prevention.
- Can also provide better privacy for some threat models.
- We’re making it better all the time and better options for mobile devices are coming out soon.

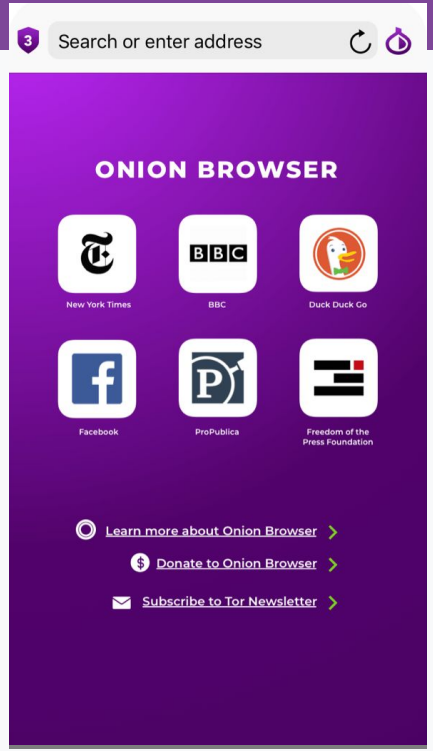
Tor Browser for Android

- You don’t need to install two applications (Orbot and Orfox) anymore!
- Find it in the Play Store or in the Guardian Project repository in F-Droid.
- Or download .apk from: https://torproject.org/download/



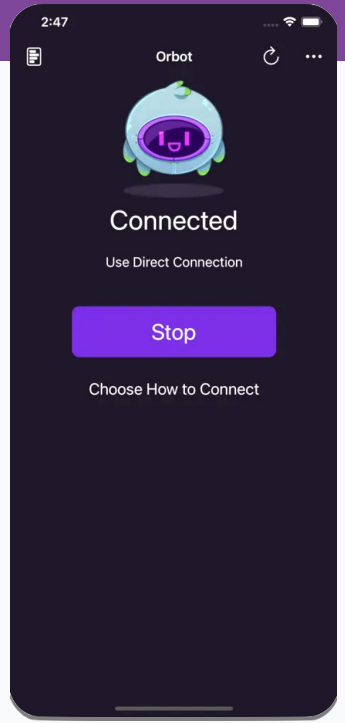
Onion Browser for iOS

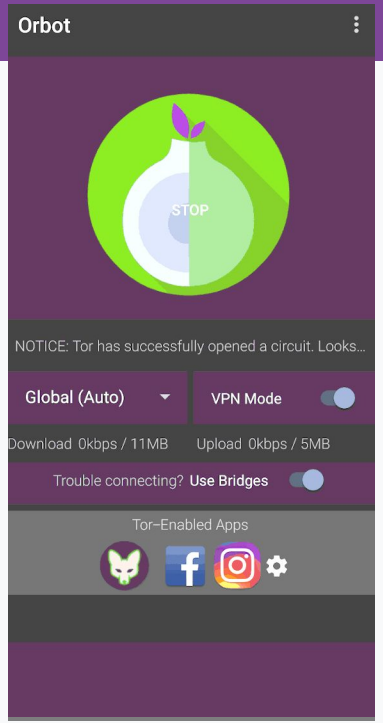
- Onion Browser is the Tor Browser for iOS.
- You can find it in the App Store.
- Be careful: lots of fake Tor Browsers available for iOS!
- Notes: app is rudimentary and tends to crash on sleep.



Orbot: Tor VPN

- Orbot routes mobile apps' traffic through Tor, you can select specifically which apps to run through Tor.
- Orbot is available on iOS and Android.
- Developed and maintained by the Guardian Project: https://orbot.app/





More on Orbot

- Toggle “VPN mode” on main screen.
- Then click “Orbot-enabled apps”.
- Then select the apps you want to proxy with Tor.
- You can also choose your exit country if you want (but note that some countries don’t have exits relays).

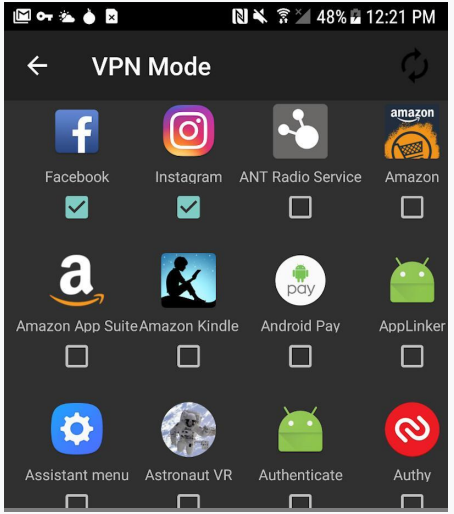
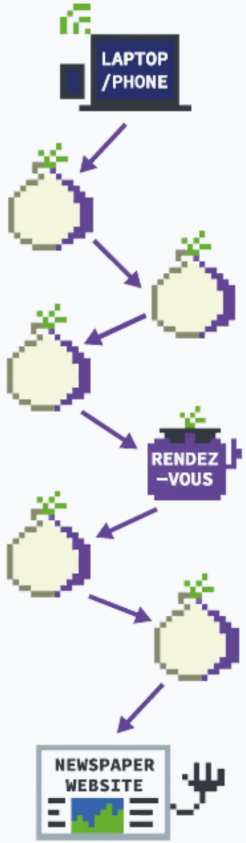


Image source: Guardian Project

What are Onion Services?

- The regular internet allows adversaries to see what you are sharing and with whom, whether you're using Dropbox etc, downloading it from email or through your browser...
- ...so Tor devised a sneaky way to hide both the file data and the related metadata!

- Onion Services are online services that are only available through the Tor network.
- An Onion Service connects to a rendez-vous node/relay inside the Tor network; and the user wanting to connect to it does the same.
- As a user, you never leave the Tor network when visiting an Onion Service.
- Onion Services provide end-to-end encryption: both visitor and website use Tor (without HTTPS).

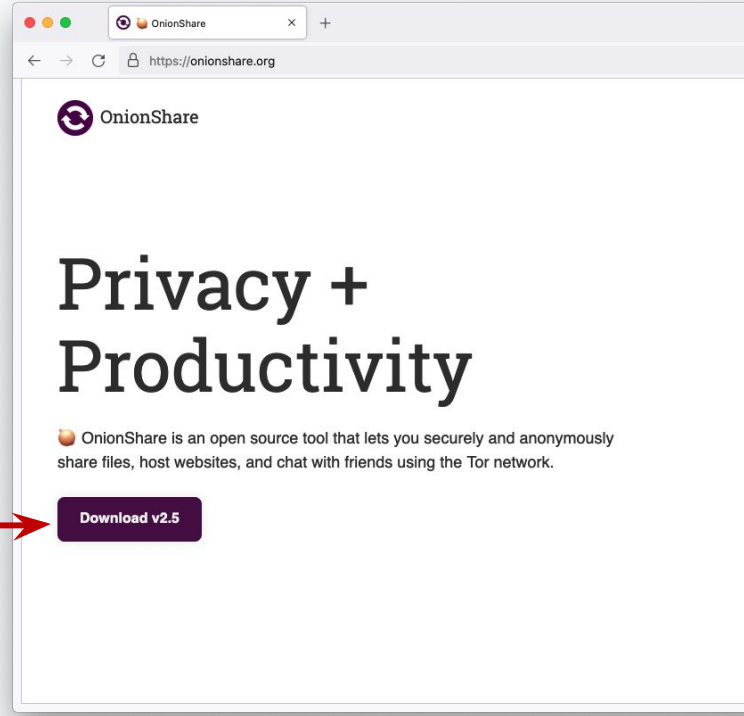


OnionShare

- Secure, private, anonymous file sharing done easy, built on top of the Tor network.
- Uses onion services to securely send files.
- Creates an onion service where the file can be downloaded.
- No need to trust third parties like Dropbox.
- All communication happens on the Tor network.
- Download from: https://onionshare.org/

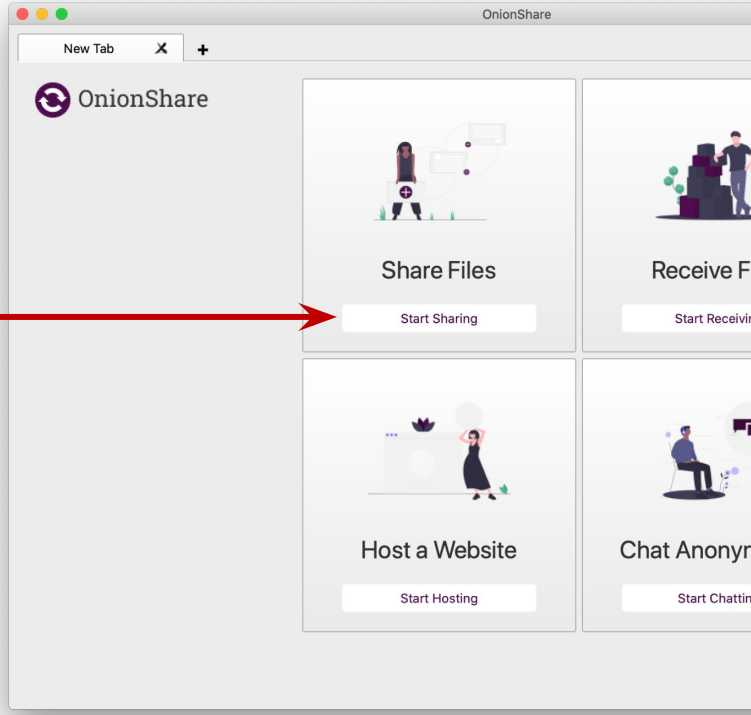
Step 1: Download OnionShare

- Available on: Windows, macOS, Linux.
- Download: https://onionshare.org/



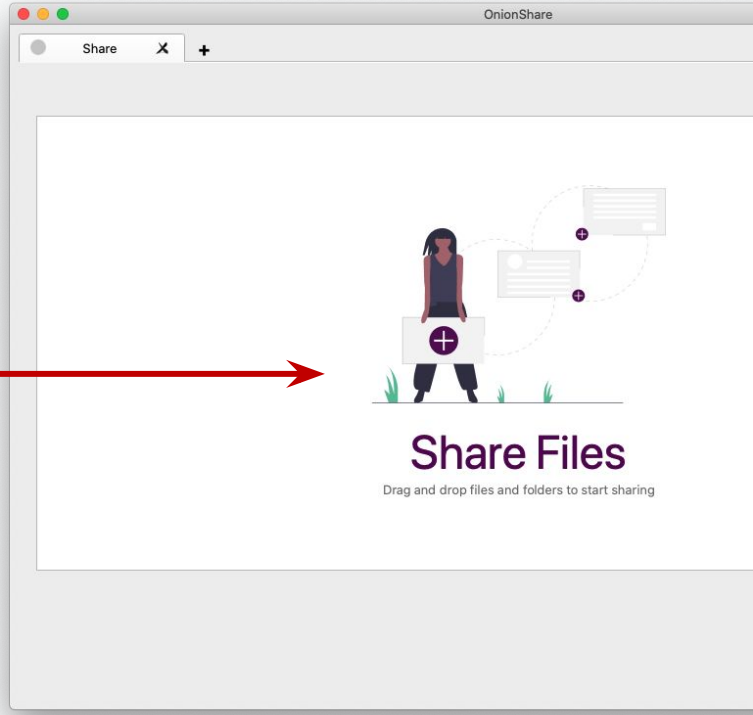
Step 2: Select “Share Files”

- In the “Share Files” section, click “Start Sharing”.
- Your contacts only need to have Tor Browser installed.



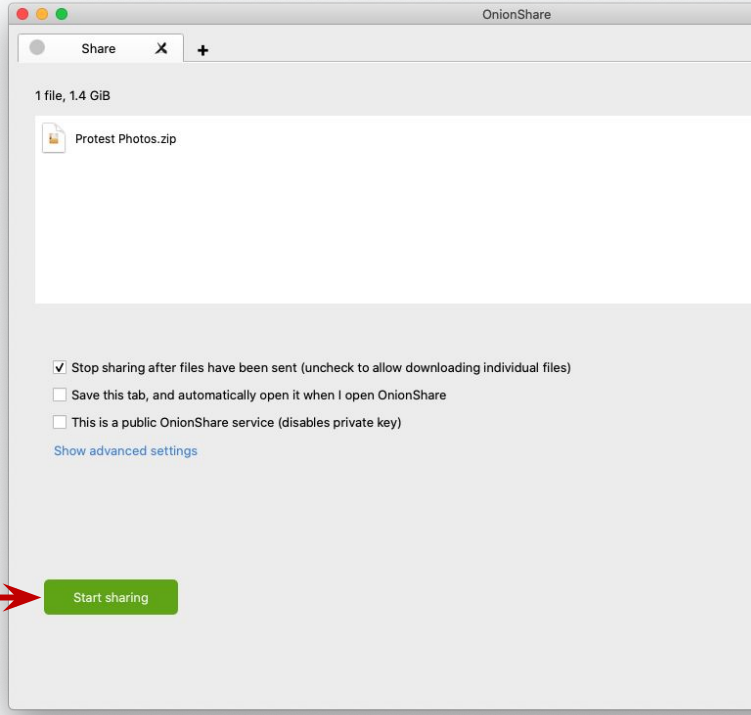
Step 3: Upload your file

- Drag and drop the file into the folder into the section.



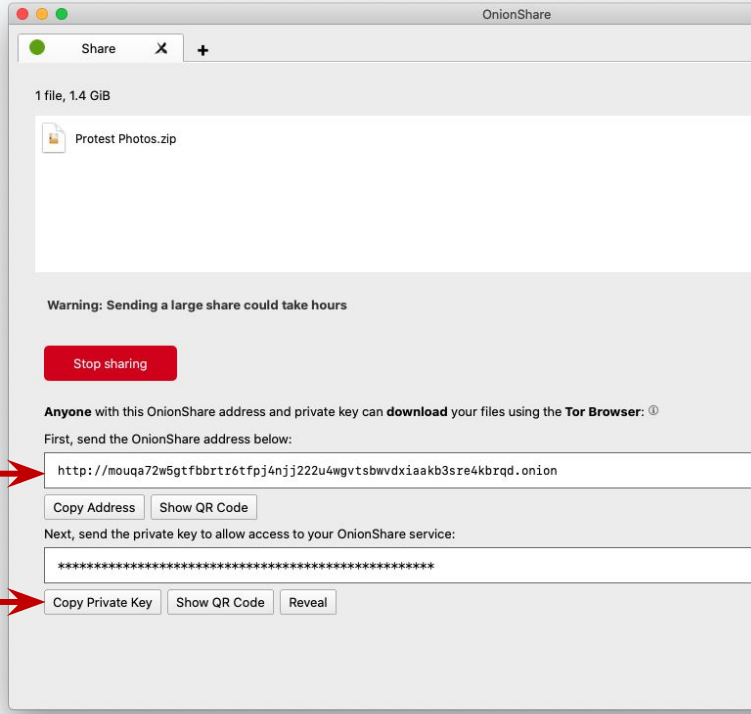
Step 4: Share your file

- Once the file is added, click on “start sharing”
- Tip: To allow downloading more than once, e.g. for you group, uncheck the first box.



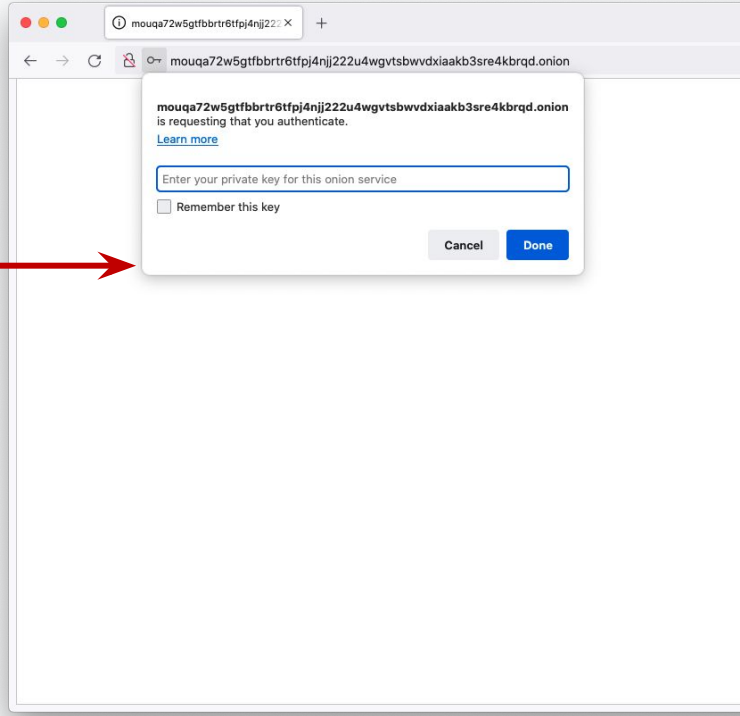
Step 5: Copy and share the address and key

- Copy the address and share it with the intended recipient (e.g. via email).
- Copy the private key and share it to the same recipient, preferably through a different channel (e.g. via instant messaging).



Step 6: Download through Tor Browser

- The recipient can download the file through Tor Browser by entering the address and key in the URL bar.
- Tip: you must keep your OnionShare window on your device open as long as you want people to download your file.



Step 7: Check download progress

- When they finish downloading, you'll see a notification alert in OnionShare's history.