Anonymity

Matěj Grégr
mgregr@fit.vutbr.cz

Agenda

- Anonymity
- IP Addresses
- Onion, garlic routing
- Interesting projects

Anonymity?

- The IP address can be bound directly to the user
  - ISP stores communication information
  - Typically stored for a certain time (Data Retention)
  - Law enforcement agency
- Browser fingerprinting
  - Cookies, Flash Cookies, E-Tags, HTML5 Storage
  - Browser fingerprinting
  - Lightbeam extension in FF
- User fingerprinting
  - User Activities - which application it uses, which sites it accesses

Fingerprinting – OS DNS

au.download.windowsupdate.com
watson.microsoft.com ipv6.msftncsi.com
gadgets.live.com weather.service.msn.com
money.service.msn.com

Windows 7

swscan.apple.com swdist.apple.com
swcdnlocator.apple.com su.itunes.apple.com
time.euro.apple.com radarsubmissions.apple.com
internalcheck.apple.com identity.apple.com
configuration.apple.com init.ess.apple.com init-
p[x]md.apple.com p[x]-contacts.icloud.com p[x]-
caldav.icloud.com p[x]-imap.mail.me.com [x].guzzoni-
apple.com.akadns.net ax.init.itunes.apple.com
a[x].phobos.apple.com keyvalueservice.icloud.com

MacOS X 10.8.5

au.v4.download.windowsupdate.com ds.download.windowsupdate.com
bg.v4.emdl.ws.microsoft.com definitionupdates.microsoft.com
spynet2.microsoft.com watson.telemetry.microsoft.com
sqm.telemetry.microsoft.com clientconfig.passport.net ssw.live.com
client.wns.windows.com appexbingfinance.trafficmanager.net
appexbingweather.trafficmanager.net appexsports.trafficmanager.net
appexdb[x].stb.s-msn.com de-de.appex-rf.msn.com
finance.services.appex.bing.com financeweur[x].blob.appex.bing.com
weather.tile.appex.bing.com

Windows 8

similar for iOS, Windows Phone and Android OS

mirrorlist.centos.org
[x].centos.pool.ntp.org

CentOS 6

changelogs.ubuntu.com ntp.ubuntu.com geoip.ubuntu.com
daisy.ubuntu.com _https._tcp.fs.one.ubuntu.com fs-
[x].one.ubuntu.com

Ubuntu 12.04

Fingerprinting – browser DNS

aus3.mozilla.org download.cdn.mozilla.net fhr.data.mozilla.com
services.addons.mozilla.org versioncheck-bg.addons.mozilla.org
versioncheck.addons.mozilla.org *addons.mozilla.org cache.pack.google.com*
download.mozilla.org [x].pack.google.com safebrowsing-cache.google.com
safebrowsing.clients.google.com tools.google.com

Firefox

safebrowsing.google.com translate.googleapis.com [xxxxxxxxxx].
[domain] *apis.google.com cache.pack.google.com clients[x].google.com*
[x].pack.google.com safebrowsing-cache.google.com
safebrowsing.clients.google.com ssl.gstatic.com tools.google.com
www.google.com www.google.de www.gstatic.com

Chrome

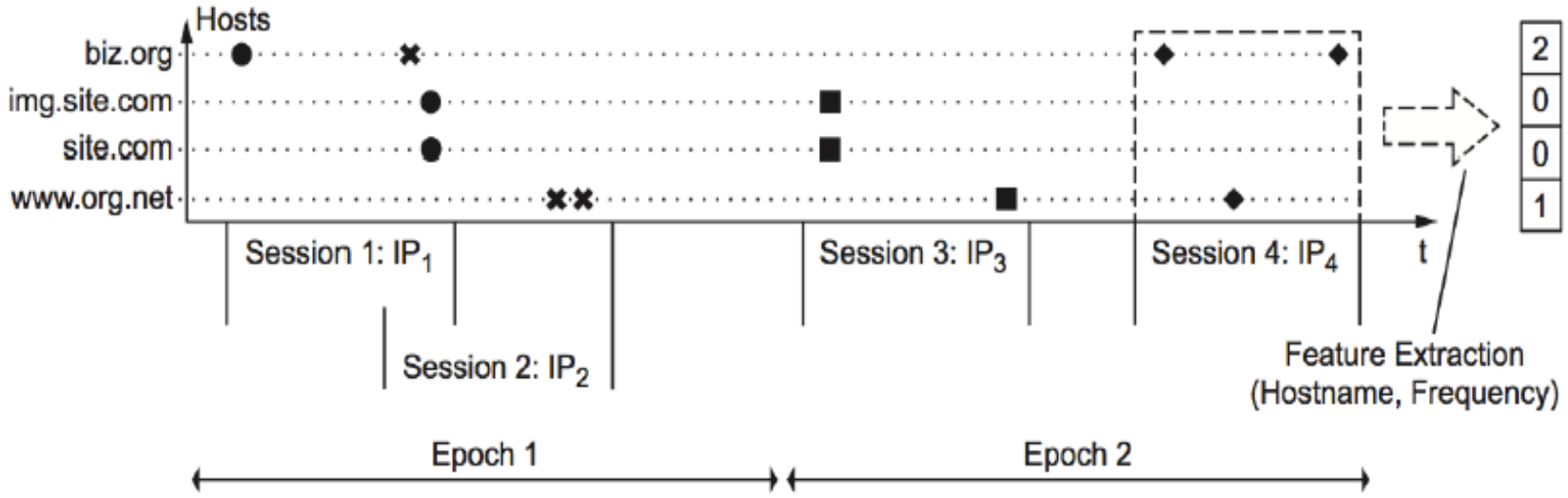
apis.google.com clients.l.google.com clients1.google.com
safebrowsing-cache.google.com
safebrowsing.clients.google.com ssl.gstatic.com
www.google.com www.google.de www.gstatic.com

Safari

ctldl.windowsupdate.com iecvlist.microsoft.com
t.urs.microsoft.com

Internet Explorer

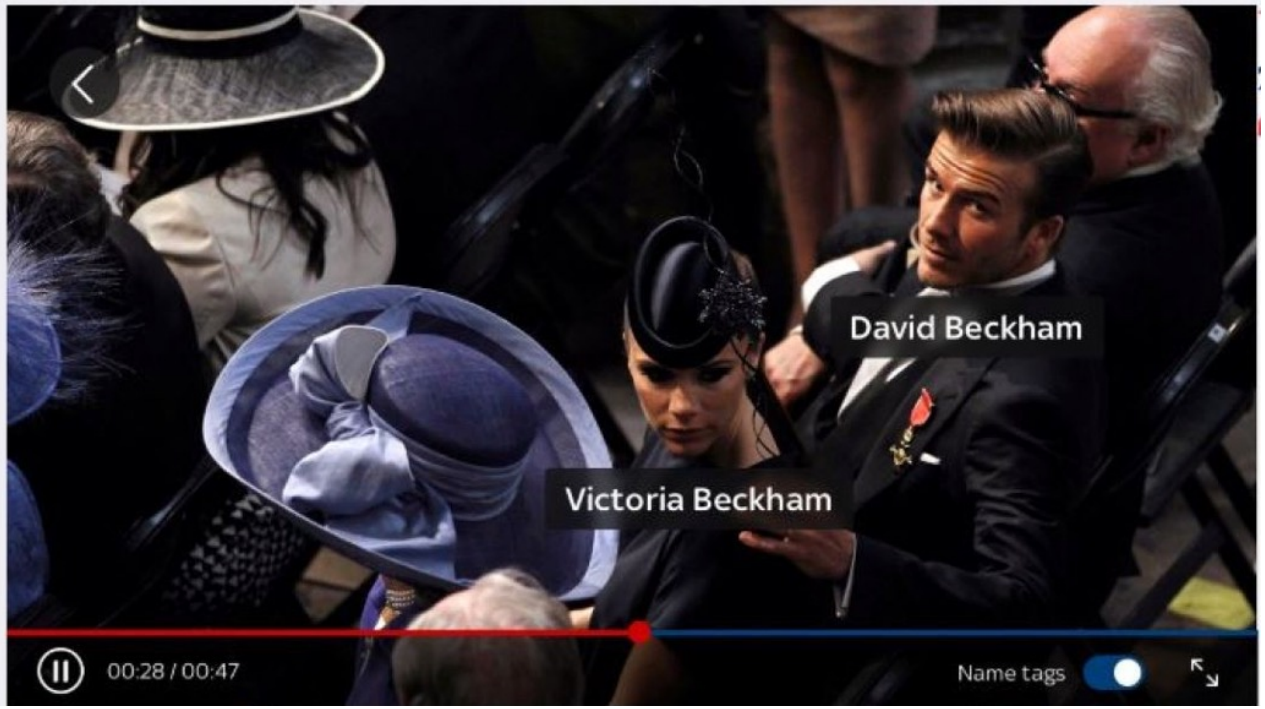
Fingerprinting – user behavior



Dominik Herrmanna,Christian Banseb, Hannes Federratha: Behavior-based tracking: Exploiting characteristic patterns in DNS traffic

Anonymity in crowds

- China surveillance
- Amazon Face recognition
  - Royal wedding: https://news.sky.com/whoswho



Who uses anonymous access?

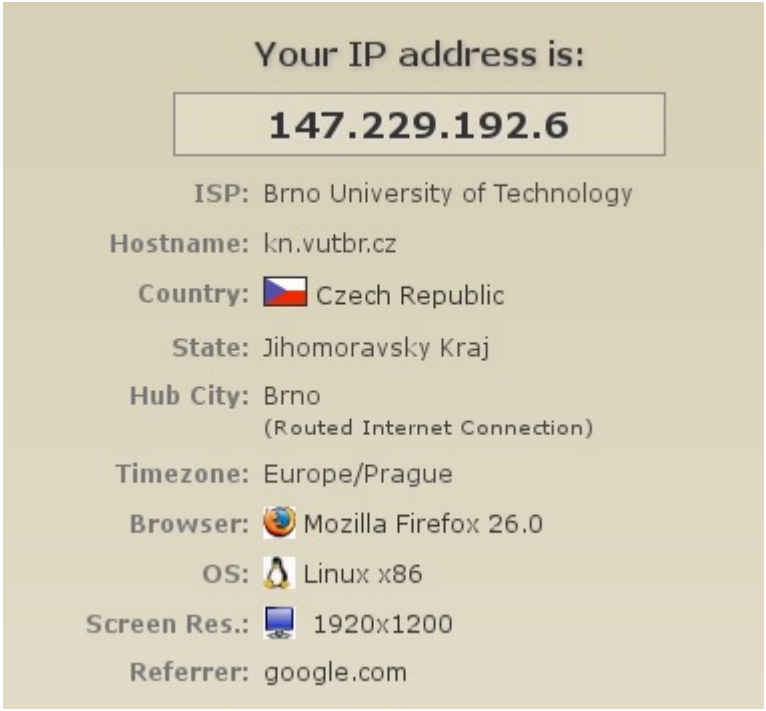
- "If you do nothing wrong, you have nothing to hide."
  - Anonymous only want to be criminals?
  - Journalists
  - Law enforcement
  - Promoting human rights
- Avoiding sanctions
  - Not every country permits the right to freedom of expression
- Avoiding "chilling-effects"
  - Controversial, unpopular thoughts

Definition?

- Unlinkability
  - Inability to link two events
    - E.g. packets, web access, people, actions
  - Three parts:
    - Sender anonymity (Who sent it?)
    - Receiver anonymity (Who is the recipient?)
    - Relationship anonymity (Are A and B in some connection?)
- Unobservability
  - Monitored events cannot be distinguished from others

IP address

- IP - globally unique identifier
- Network entry point



IP address – allocation IANA to RIR ①

- Internet Assigned Numbers Authority (IANA)
- http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml

IP address–RIR to LIR to ISP ②

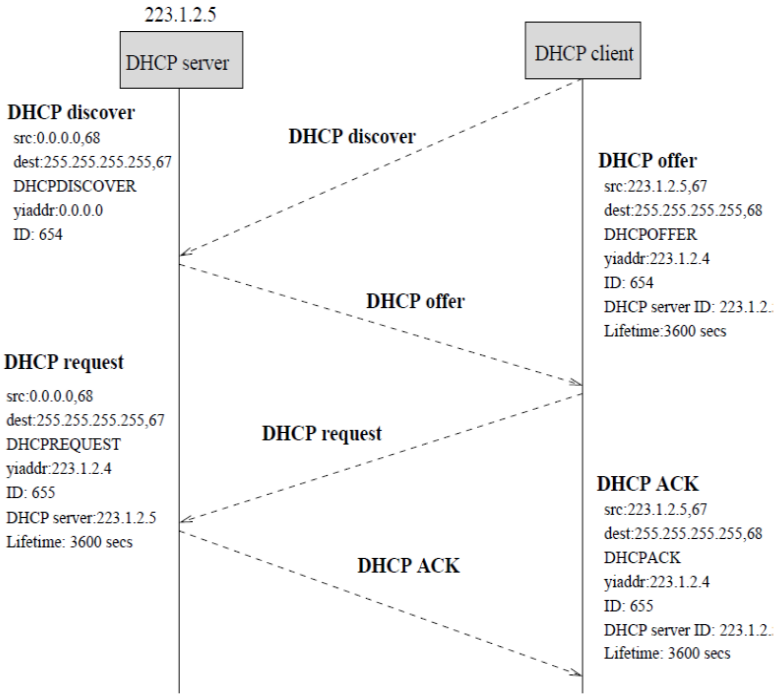
- Provider independent / aggregatable addresses
- Who is the ISP of the address - country, city

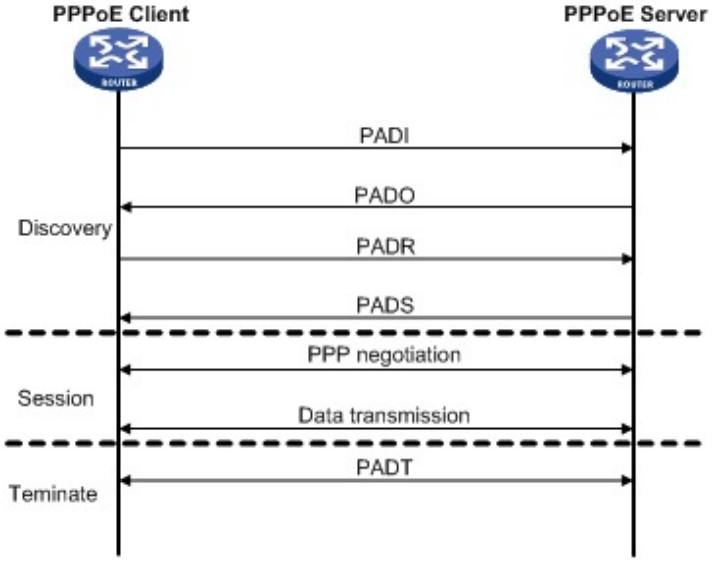
```
inetnum:        77.48.138.0 - 77.48.141.255
netname:        NUMERI-VM-NET
descr:          Josef Barton - REX
country:        CZ
admin-c:        JB5596-RIPE
tech-c:         PS6810-RIPE
tech-c:         TT1633-RIPE
status:         ASSIGNED PA
mnt-by:         SLOANE-MNT
mnt-lower:      SLOANE-MNT
source:         RIPE # Filtered

person:         Josef Barton
address:        Josef Barton - REX (Numeri)
address:        Prehrada 29
address:        Bystricka
address:        756 24
address:        Czech Republic
phone:          +420 777737500
nic-hdl:        JB5596-RIPE
source:         RIPE # Filtered

person:         Petr Siska
address:        Josef Barton - REX (Numeri)
address:        Prehrada 29
address:        Bystricka
address:        756 24
address:        Czech Republic
phone:          +420 777737503
nic-hdl:        PS6810-RIPE
source:         RIPE # Filtered

person:         Tomas Taborsky
address:        Josef Barton - REX (Numeri)
address:        Prehrada 29
address:        Bystricka
address:        756 24
address:        Czech Republic
phone:          +420 777737622
nic-hdl:        TT1633-RIPE
source:         RIPE # Filtered

route:          77.48.128.0/17
descr:          UPC Czech
origin:         AS6830
mnt-by:         AS6830-MNT
source:         RIPE # Filtered
```

```
inetnum:        147.229.0.0 - 147.229.255.255
netname:        VUTBR-TCZ
descr:          Brno University of Technology
descr:          Brno
country:        CZ
admin-c:        VS47
tech-c:         VZ36-RIPE
status:         ASSIGNED PI
mnt-by:         VUTBR-MNT
mnt-routes:     VUTBR-MNT
remarks:        Please report network abuse -> abuse@vutbr.cz
source:         RIPE # Filtered

person:         Vit Slama
address:        Brno University of Technology
address:        Center of Computing and Information Services
address:        Antoninska 1
address:        Brno
address:        601 90
address:        The Czech Republic
phone:          +420 541145630
fax-no:         +420 541145419
nic-hdl:        VS47
mnt-by:         DKI-MNT
source:         RIPE # Filtered

person:         Vladimir Zahorik
address:        Brno University of Technology
address:        Antoninska 1
address:        Brno
address:        601 90
address:        The Czech Republic
phone:          +420 541 145 631
fax-no:         +420 541 145 419
abuse-mailbox:  abuse@vutbr.cz
nic-hdl:        VZ36-RIPE
mnt-by:         TENCZ-MNT
source:         RIPE # Filtered

route:          147.229.0.0/16
descr:          VUTBR-TCZ
origin:         AS197451
mnt-by:         VUTBR-MNT
source:         RIPE # Filtered
```

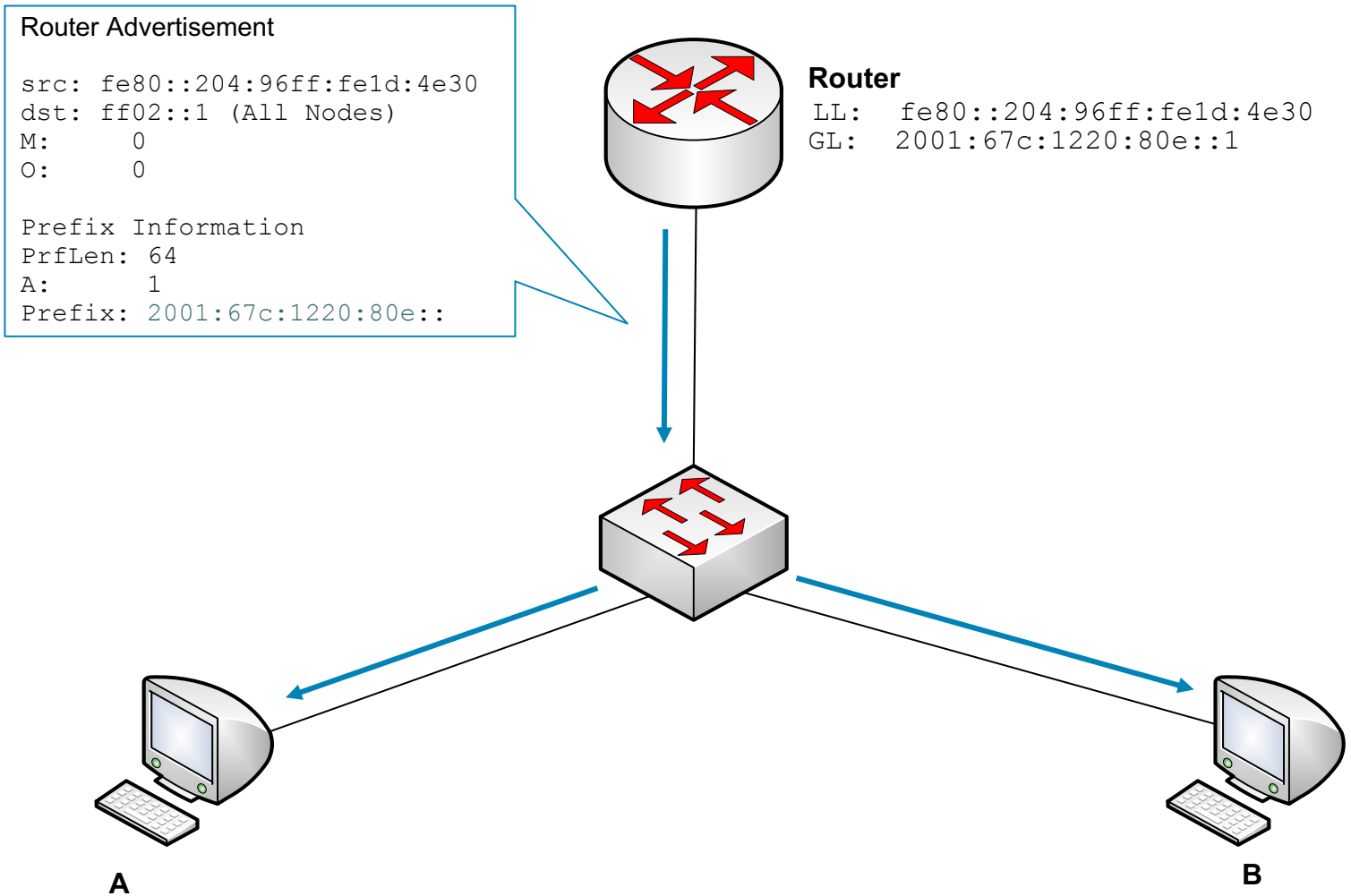
IPv4 address – assigned to the user

- DHCP, PPPoE
- The ISP stores the information asked (MAC, DHCP82, username) and what address has been assigned
-





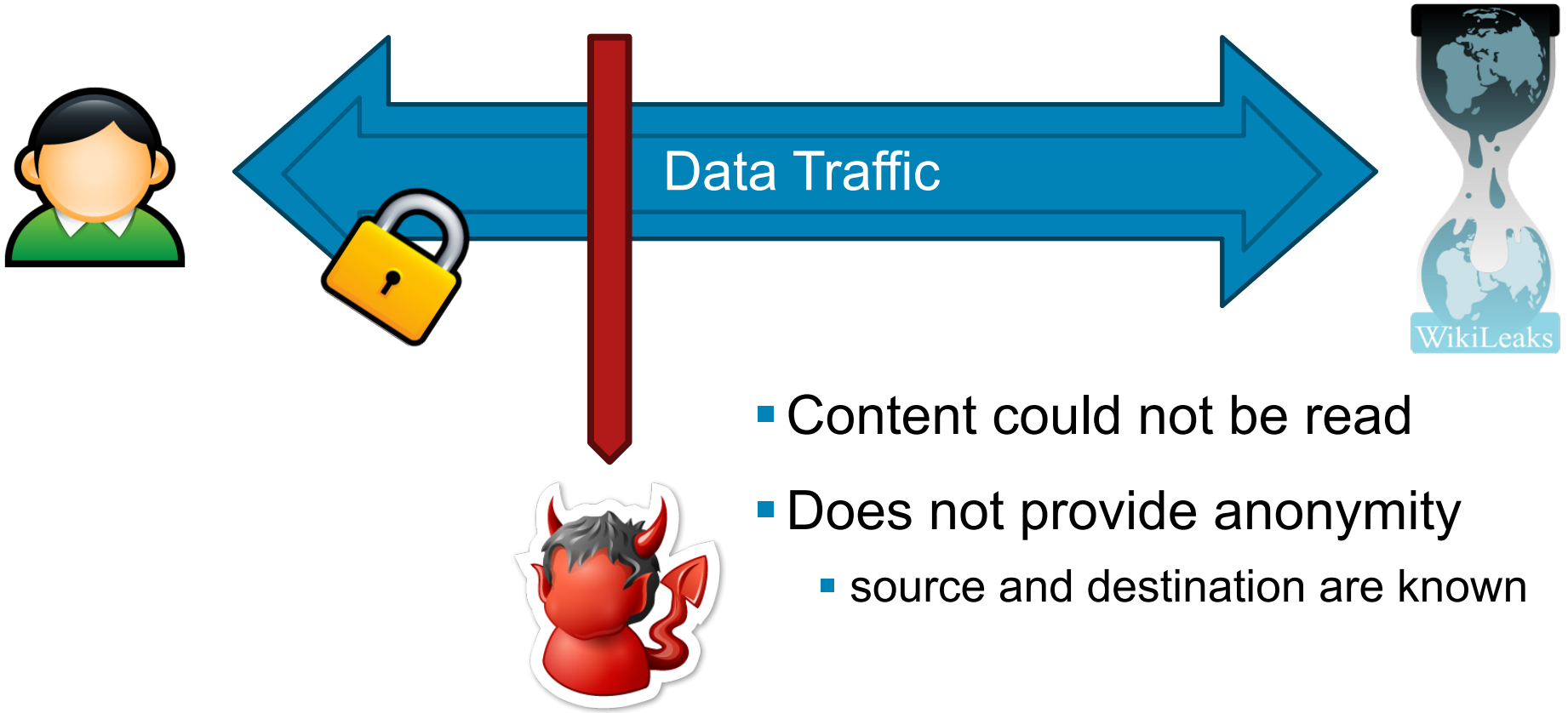
IPv6 address - assigned to the user



IP address

- IPv4
  - Typically, an ISP always has information about which user has assigned which IPv4 address
- IPv6
  - Prefix allocation - similar to IPv4
  - Address allocation (metro Ethernet) - more problematic information retrieval
- ISP keeps this information almost always even **without** DR
  - Tracing problems, billing…

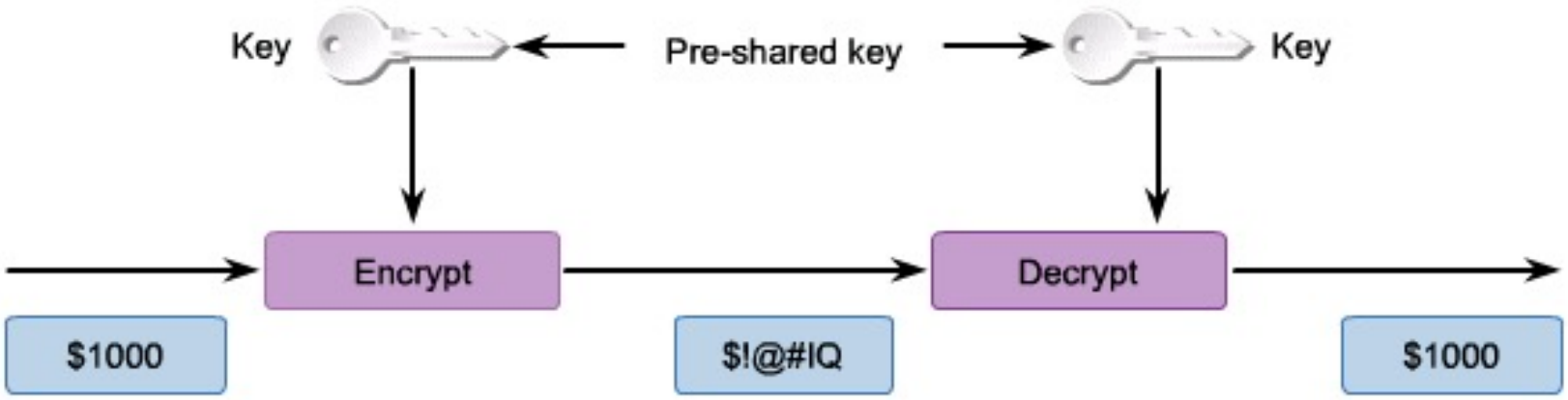
Encryption?



- Content could not be read
- Does not provide anonymity
  - source and destination are known

Symmetric cryptography

- Shared Key Algorithms, used for both encryption and decryption
- The same key is known to both sides, the security lies in key protection



Symmetric cryptography

- Plaintext message *M*
  - E - symmetric encryption algorithm
  - K - key

$$M \rightarrow E(K, M) = C \rightarrow E(K, C) = M$$

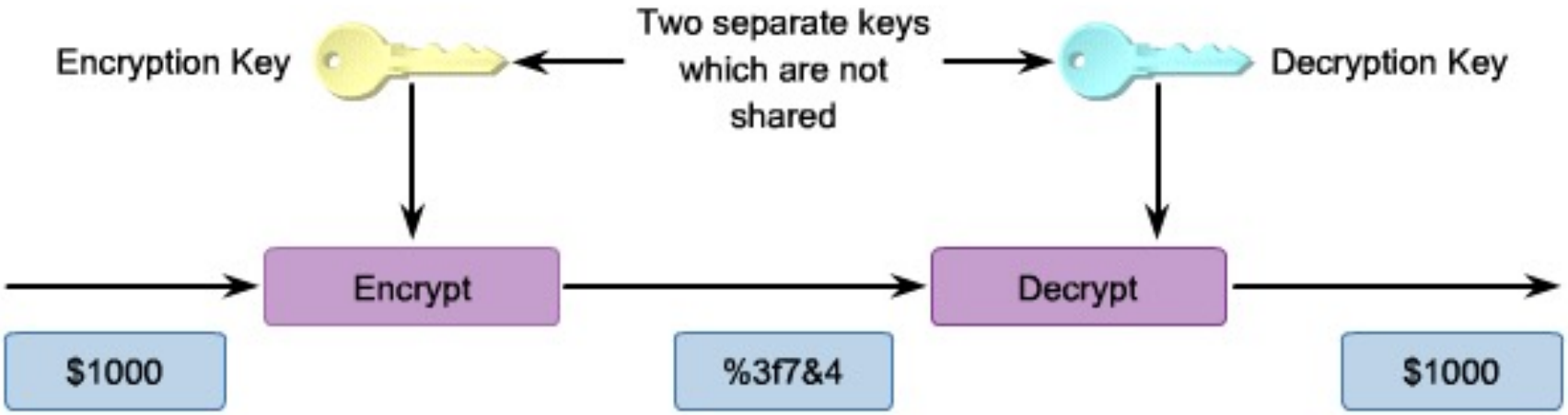
- Advantages
  - Speed, simplicity
- Disadvantages
  - Key distribution

Symmetric cryptography

Symmetric Encryption Algorithm	Key length (in bits)	Speed	Time to Crack	Description
DES 1976	56	Medium	Hours Days	Designed at IBM during the 1970s and adopted as the NIST standard until 1997. Although considered outdated, DES remains widely in use. DES was designed to be implemented only in hardware, and is therefore extremely slow in software.
3DES 1977	112 and 168	Low	Days Months	Based on using DES three times which means that the input data is encrypted three times and therefore considered much stronger than DES. However, it is rather slow compared to some new block ciphers such as AES.
AES 2001	128, 192, and 256	High	Years	AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.
SEAL 1997	160	High	Years	SEAL is an alternative algorithm to DES, 3DES, and AES. It uses a 160-bit encryption key and has a lower impact to the CPU when compared to other software-based algorithms.
The RC series 1987,94,98	RC2 (40 and 64) RC4 (1 to 256) RC5 (0 to 2040) RC6 (128, 192, and 256)	Fast	Years	RC algorithms are a set of symmetric-key encryption algorithms invented by Ron Rivest. RC1 was never published and RC3 was broken before ever being used. RC4 is the world's most widely used stream cipher. RC6, a 128-bit block cipher based heavily on RC5, was an AES finalist developed in 1997.

Asymmetric cryptography

- A pair of linked keys - public and private
- Compared to symmetric algorithms, the key length is much larger to provide the same level of security
- Asymmetric algorithms are computationally intensive (100x to 1000x slower)



Private and public key

- Only the owner knows and owns the private key
- The public key is available to anyone
- Both keys are different and it is computationally "impossible" to derive the one key from the other
- Each key can be used for both encryption and decryption
  - private encrypts, public decrypts
  - public encrypts, private decrypts

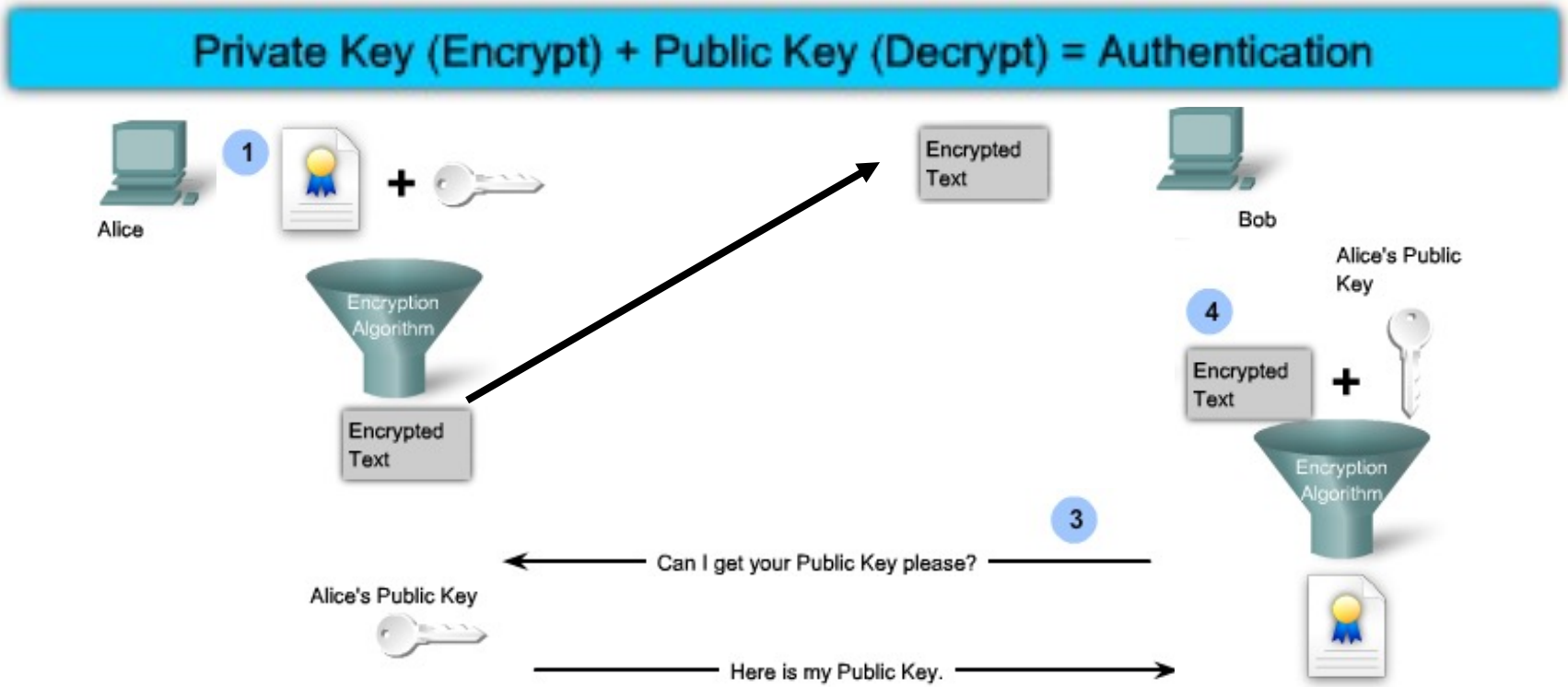
Asymmetric cryptography

- Plaintext message *M*
  - F - asymmetric encryption algorithm
  - *KP* (public key), *KS* (private key)

$$M \rightarrow F(K_P, M) = C \rightarrow F(K_S, C) = M$$

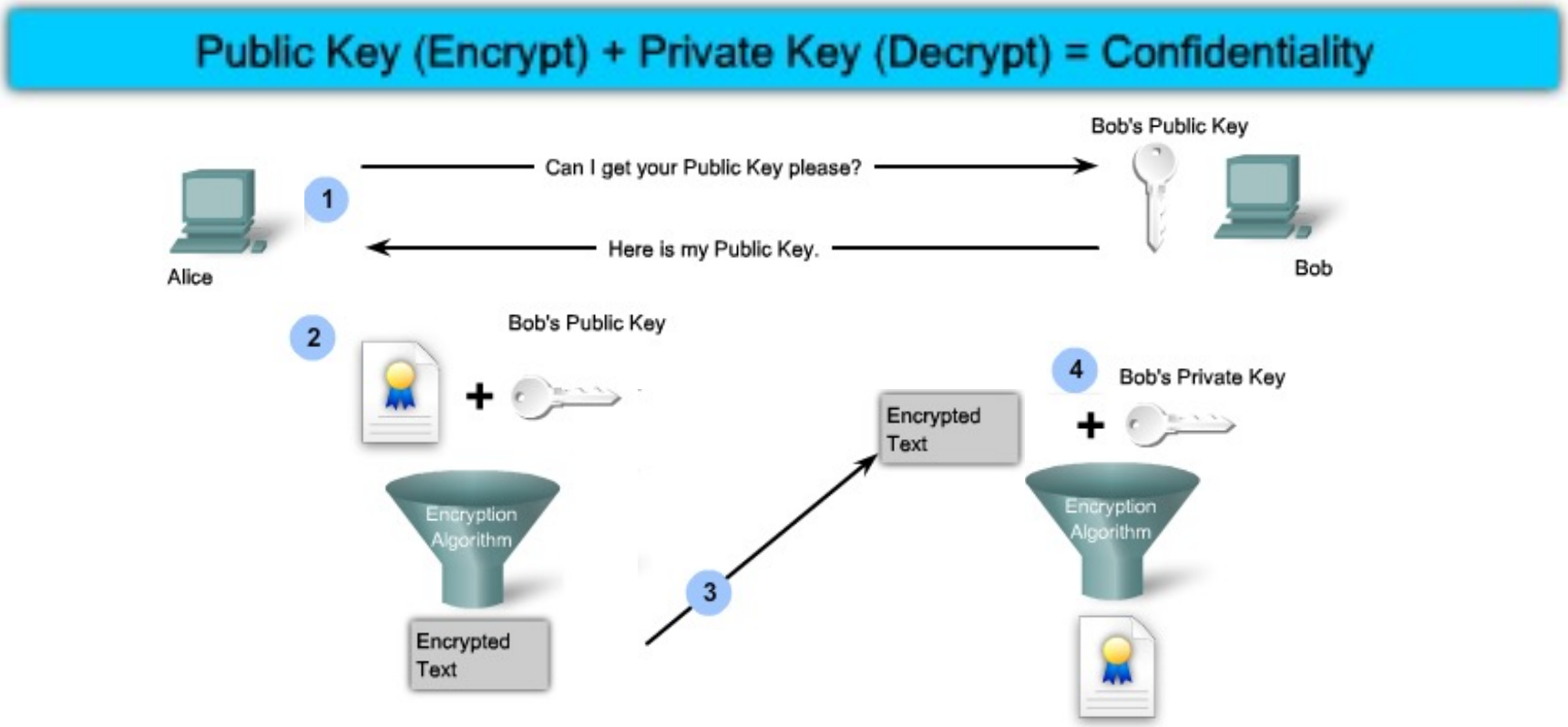
$$M \rightarrow F(K_S, M) = C \rightarrow F(K_P, C) = M$$

Authentication



1. Alice encrypts the message with its own private key.
2. Alice sends cipher-text to Bob
3. Bob asks for Alice's public key to verify the message.
4. To verify that the message comes from Alice, Bob uses Alice's public key to decipher it. If the message is readable, it is undeniable that Alice sent the message

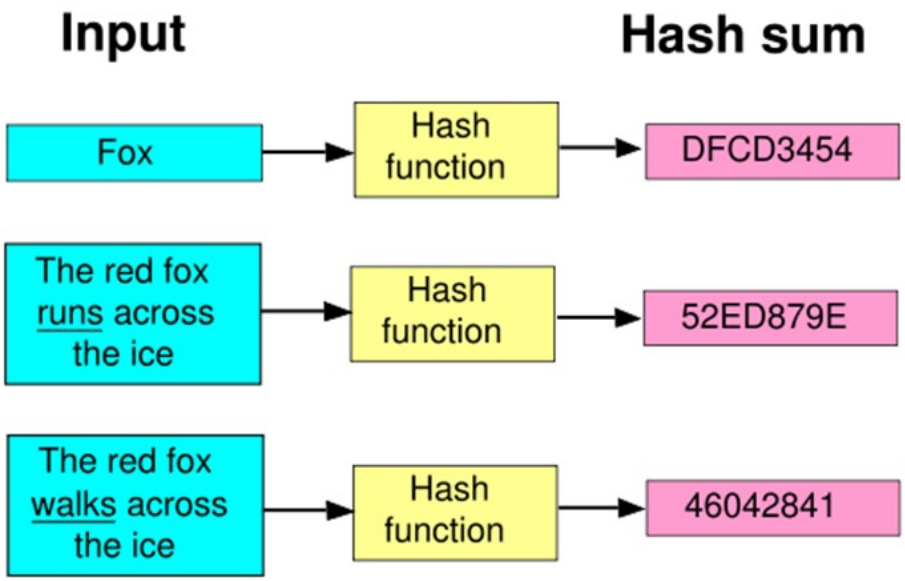
Confidentiality

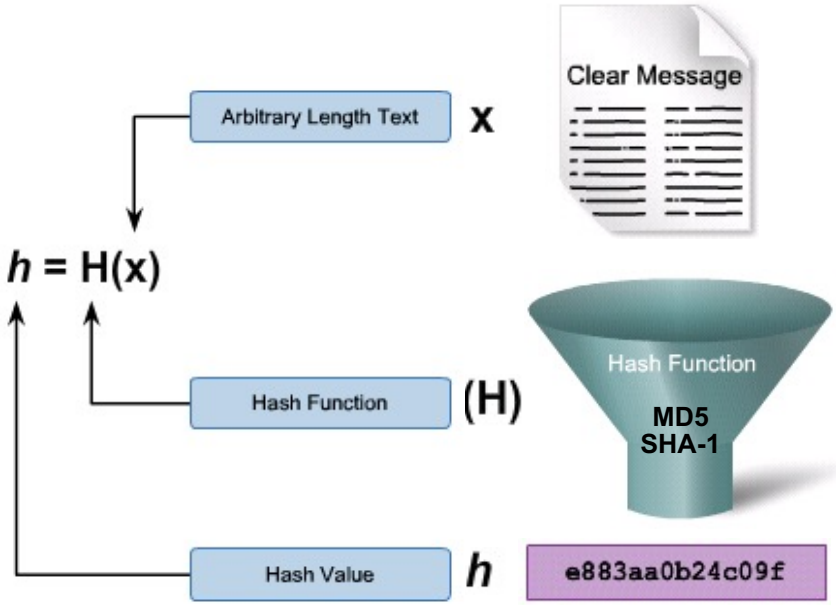


1. Alice asks Bob for his public key.
2. Alice uses Bob's public key to encrypt the message
3. Alice sends cipher-text to Bob.
4. Bob uses his private key to decrypt the message.

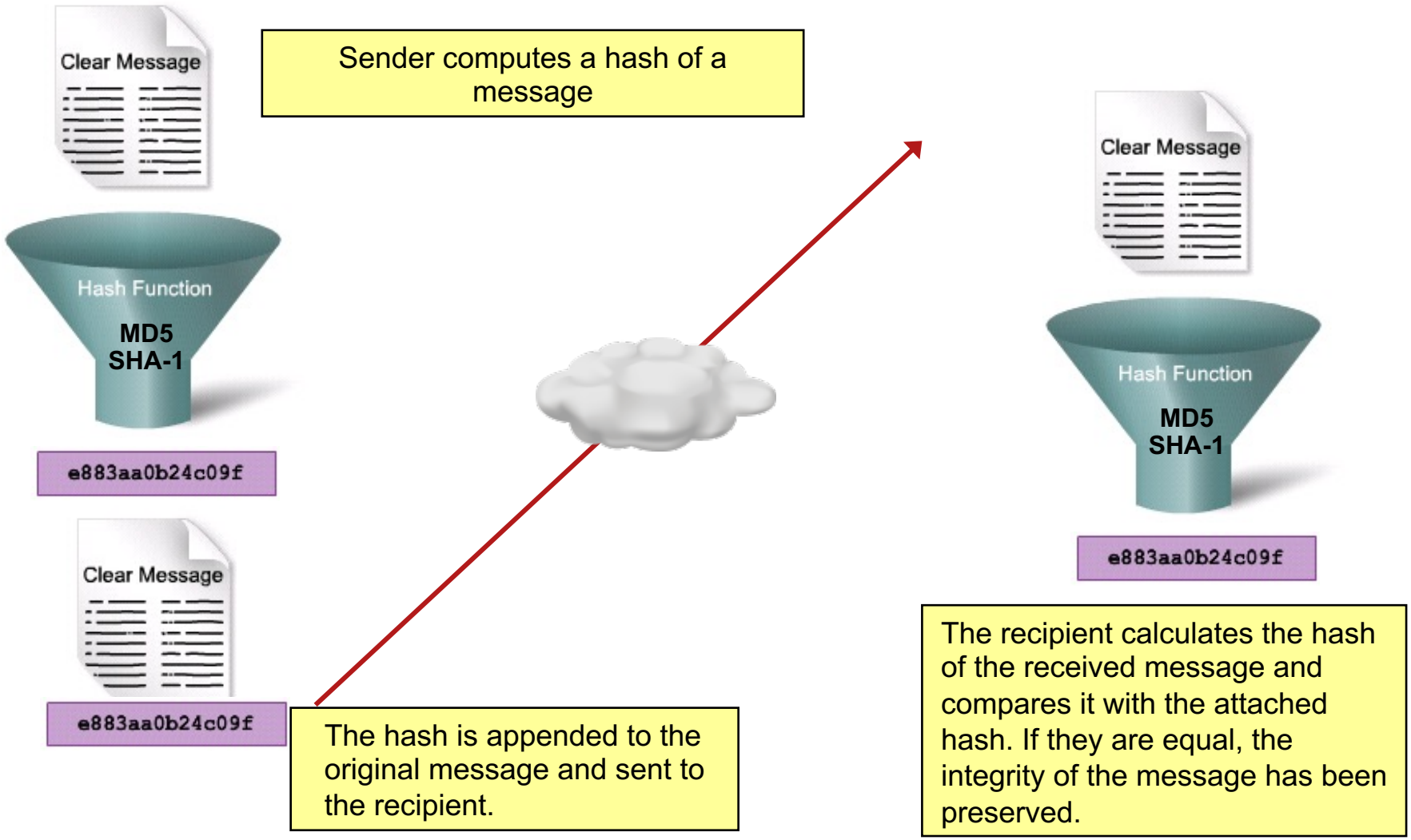
Hash

- A one-way mathematical hash function: takes binary data of arbitrary length as its input and produces a fixed-length output called a hash
- Hash is used to ensure integrity
- Hash function should be resistant to collisions

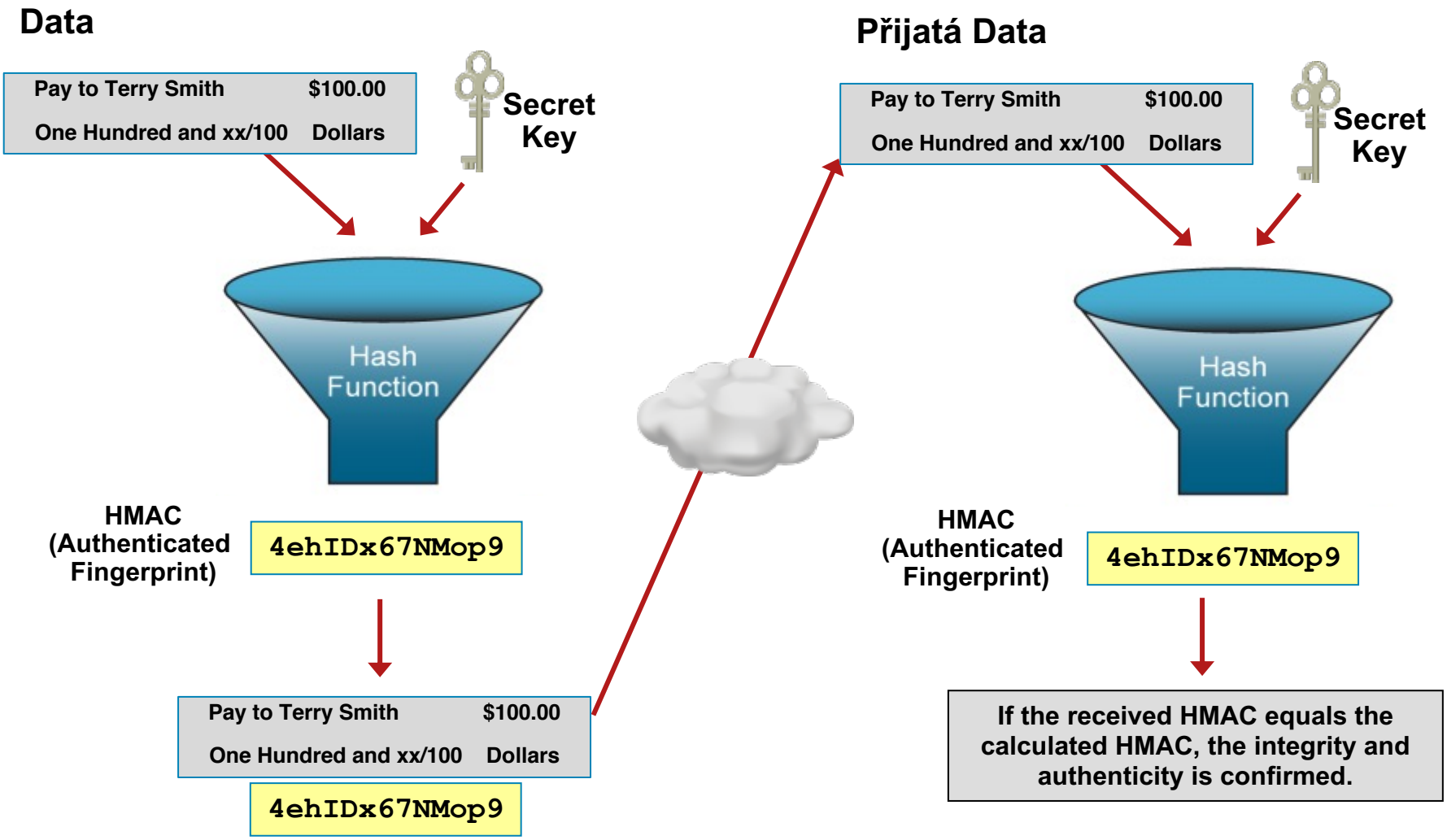




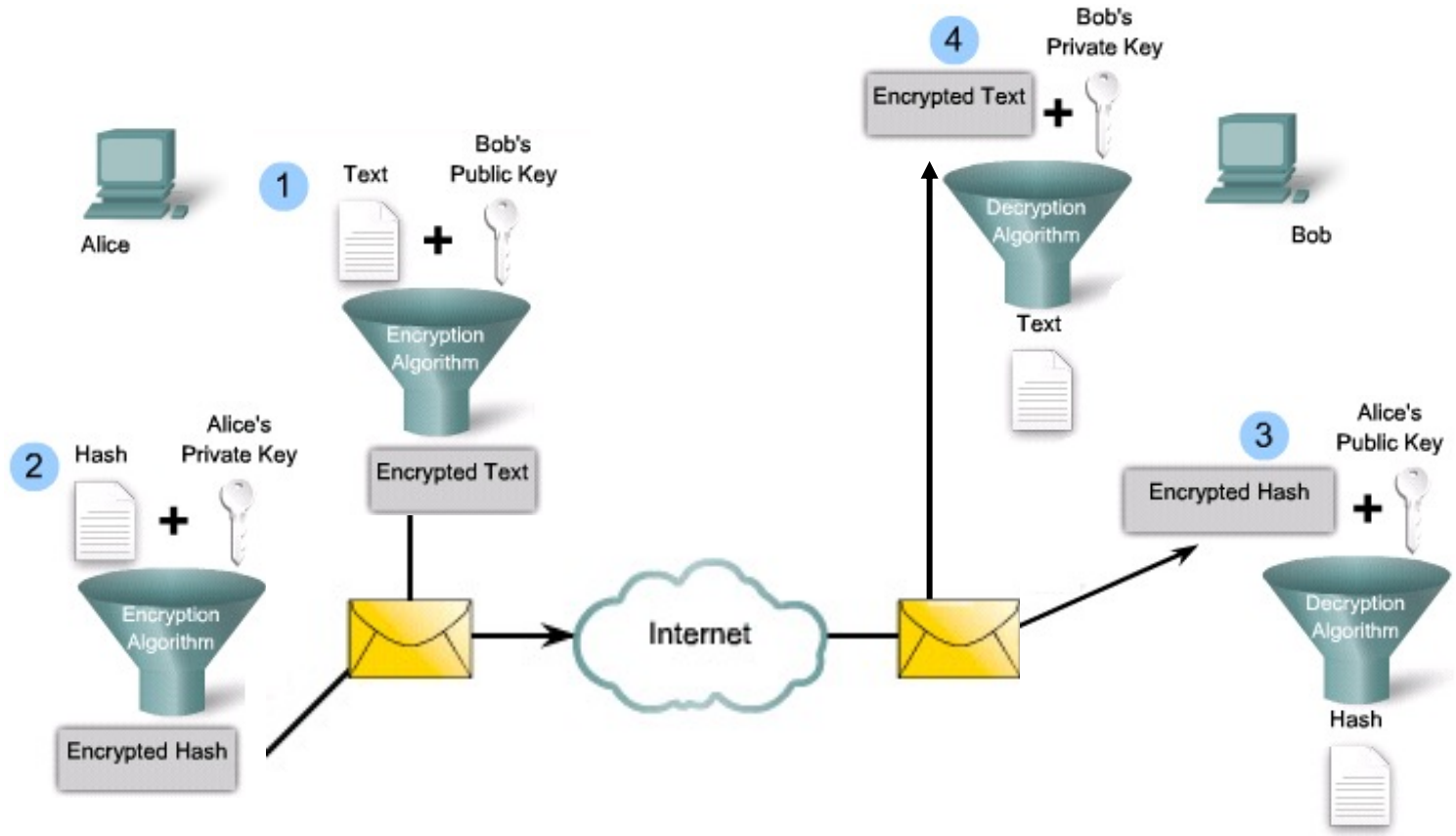
Integrity


Clear Message
Sender computes a hash of a message
Hash Function
MD5
SHA-1
e883aa0b24c09f
Clear Message
e883aa0b24c09f
The hash is appended to the original message and sent to the recipient.
Clear Message
Hash Function
MD5
SHA-1
e883aa0b24c09f
The recipient calculates the hash of the received message and compares it with the attached hash. If they are equal, the integrity of the message has been preserved.

Hash-based message authentication code



Assymetric cryptography + HMAC



1. Alice encrypts the message using Bob's public key.
2. Alice encrypts HMAC with its own private key.
3. Bob uses Alicia's public key to validate the HMAC message.
4. Bob uses his private key to decipher the cipher-text.

Asymetric algorithms

Algorithm	Key length (in bits)	Description
Diffie-Hellman (DH) 1976	512, 1024, 2048	Public key algorithm invented in 1976 by Whitfield Diffie and Martin Hellman that allows two parties to agree on a key that they can use to encrypt messages. Security depends on the assumption that it is easy to raise a number to a certain power, but difficult to compute which power was used given the number and the outcome.
Digital Signature Standard (DSS) and Digital Signature Algorithm (DSA) 1994	512 - 1024	Created by NIST and specifies DSA as the algorithm for digital signatures. DSA is a public key algorithm based on the ElGamal signature scheme. Signature creation speed is similar with RSA, but is 10 to 40 times as slow for verification.
RSA encryption algorithms 1977	512 to 2048	Developed by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT in 1977. It is an algorithm for public-key cryptography based on the difficulty of factoring very large numbers. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. Widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.
ElGamal	512 - 1024	An asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie-Hellman key agreement. Developed in 1984 and used in GNU Privacy Guard software, PGP, and other cryptosystems. A disadvantage is that the encrypted message becomes very big, about twice the size of the original message and for this reason it is only used for small messages such as secret keys.
Elliptical curve techniques	160	Elliptic curve cryptography was invented by Neil Koblitz in 1987 and by Victor Miller in 1986. Can be used to adapt many cryptographic algorithms, such as Diffie-Hellman or ElGamal. The main advantage of elliptic curve cryptography is that the keys can be much smaller.

Public Key Infrastructure (PKI)

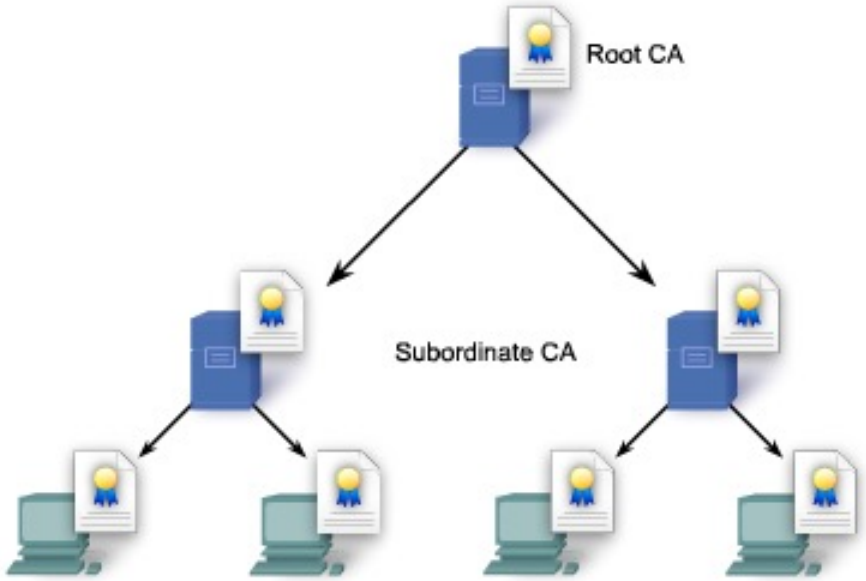
- Verifying that the private/public keys are actually owned by the user = certificate
- Hierarchy of certificate holders and certification authorities
- Certification Authority = a trusted organization that issues certificates

VeriSign

Go Daddy.com

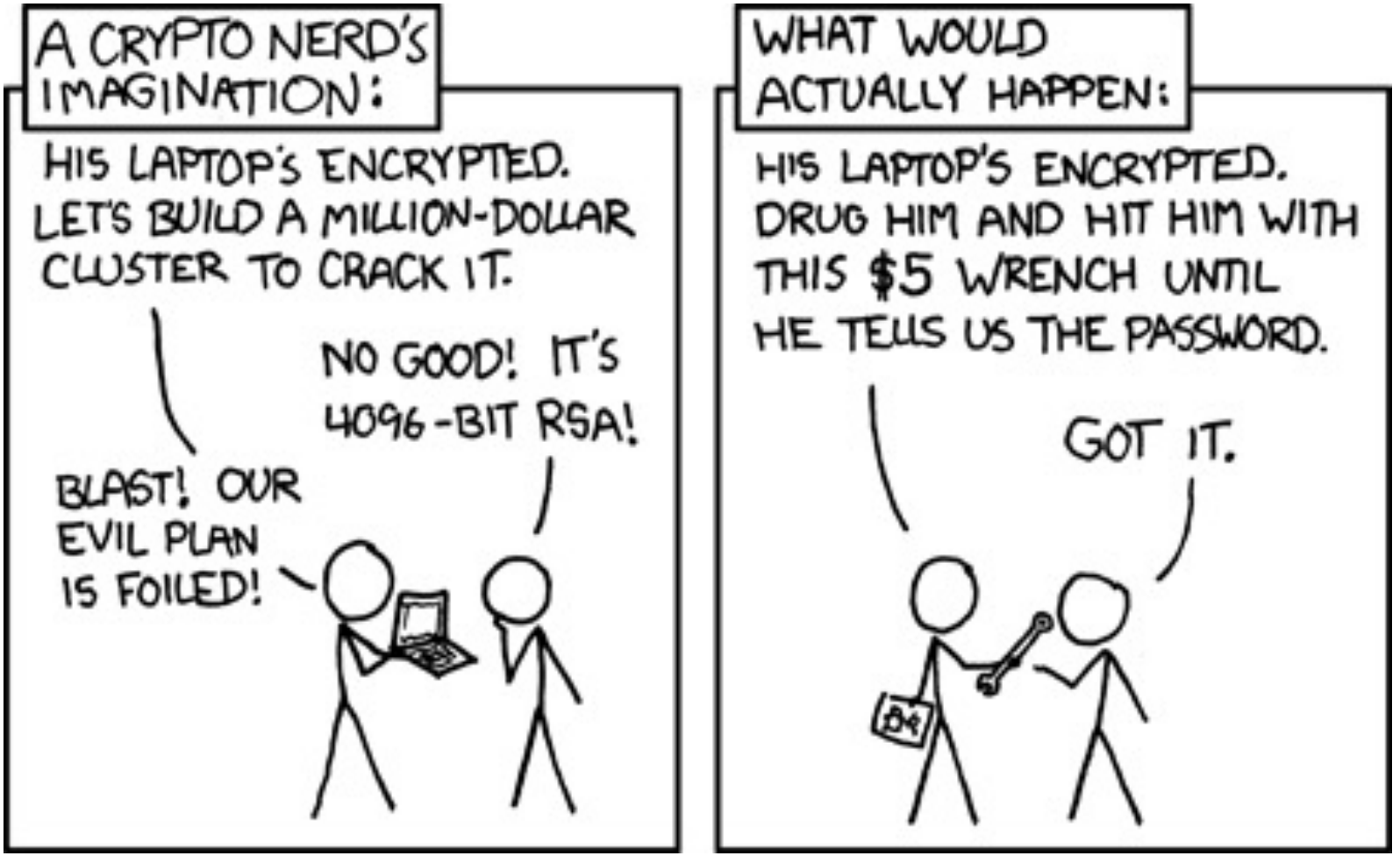
CERTIFICATION AUTHORITY

Česká pošta



Possible ways to obtain Anonymity

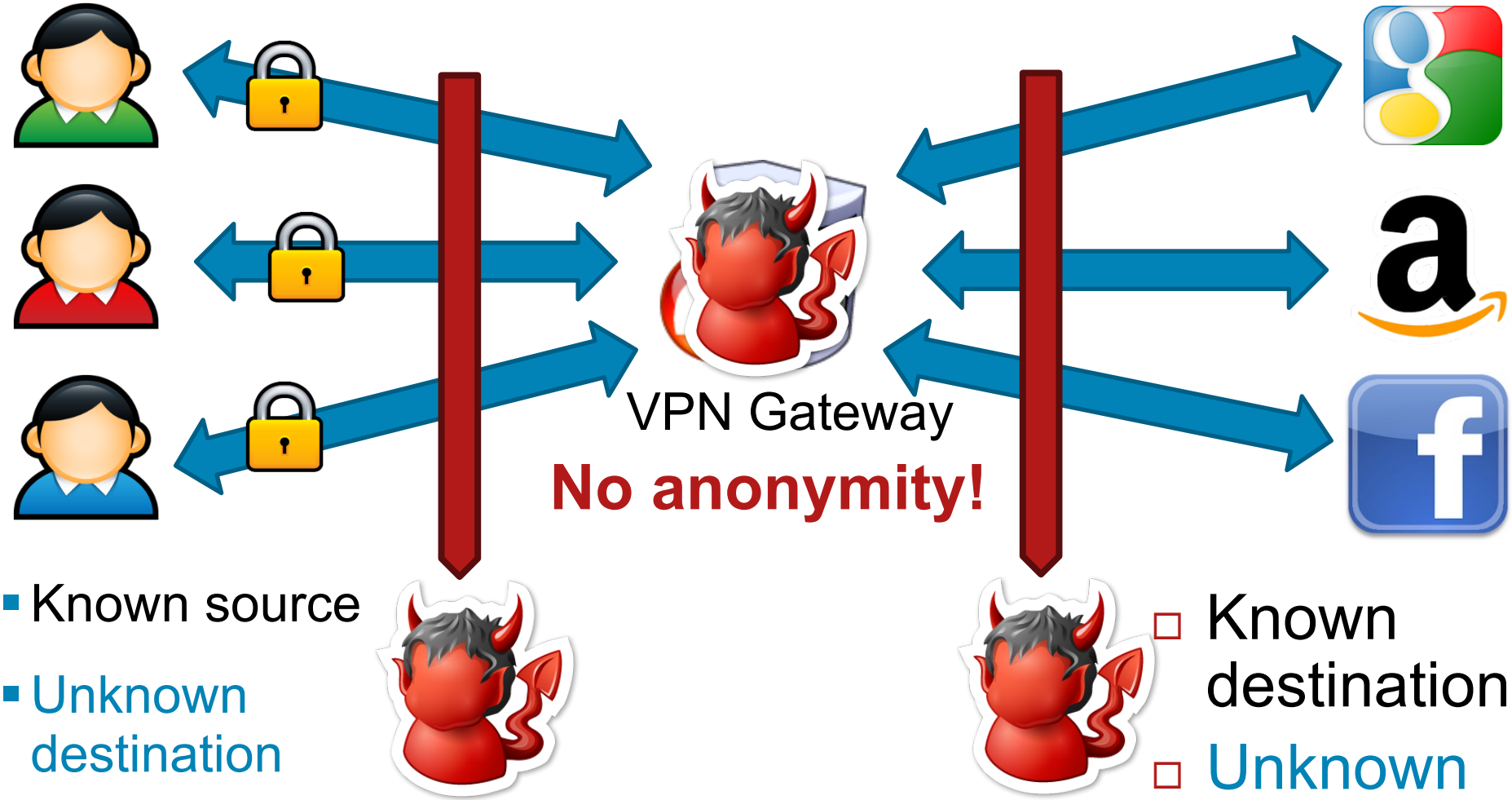
- VPN
- Proxy
- Onion routing
- Garlic routing
- P2P network
- End-to-end encryption



https://xkcd.com/538/

VPN ①

33



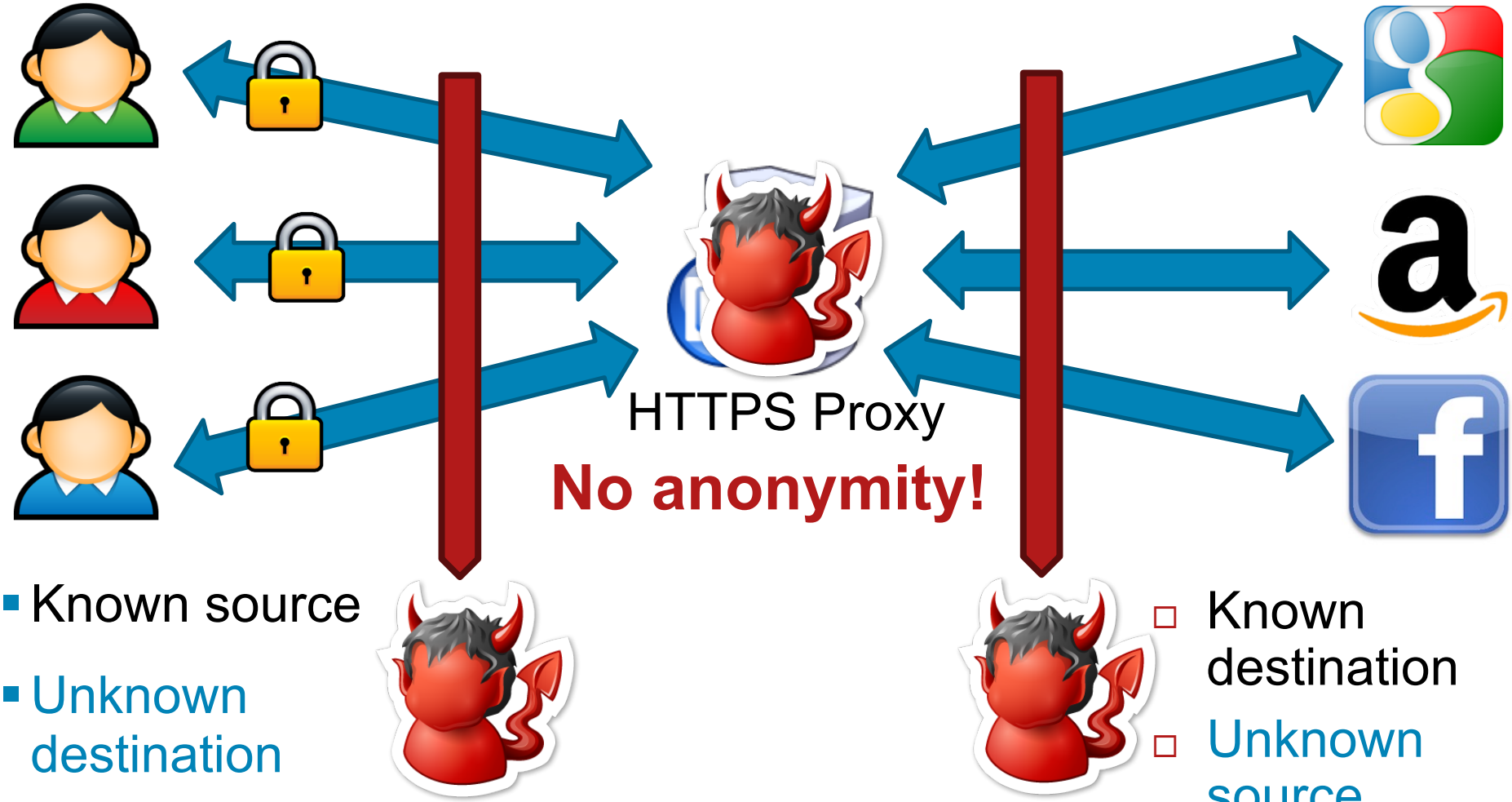
- Known source
- Unknown destination

- Known destination
- Unknown source

VPN ②

- ISP cannot inspect communication
- The user acts as someone else (from IP level)
- Can „unlocking“ some internet services
- VPN provider has information who has joined from what address
- Transparent for all applications
- Payment Bitcoins
- Many providers: ipredator, privateinternetaccess, torguard, btguard…

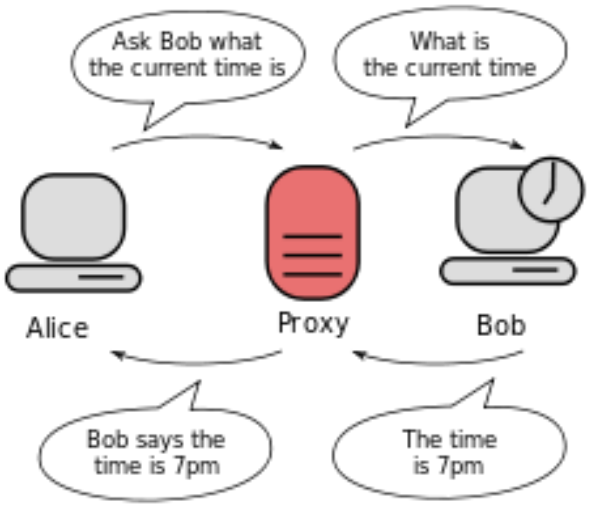
Proxy



- Known source
- Unknown destination

- Known destination
- Unknown source

Proxy

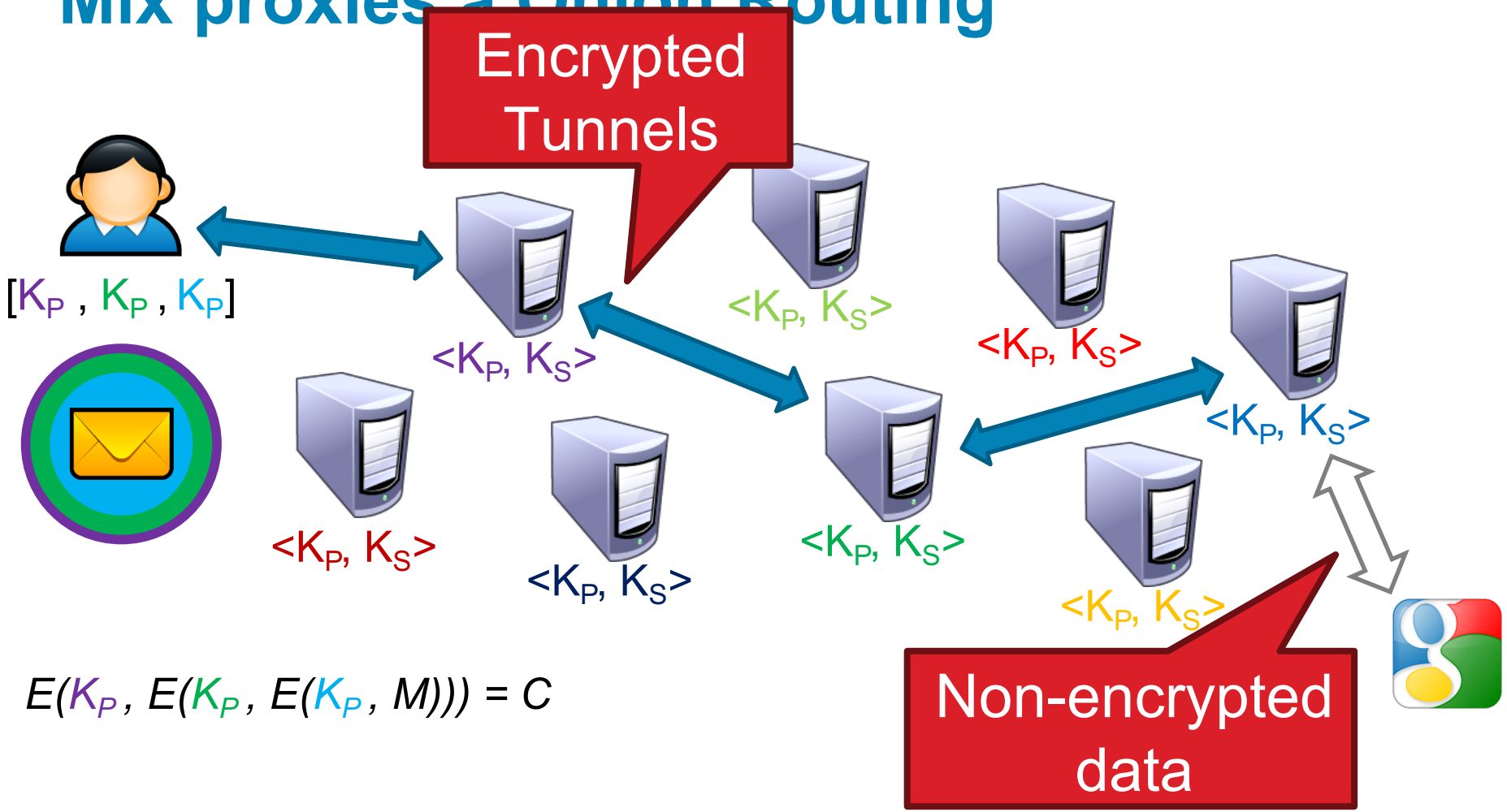


- Similiar to VPN
- Traffic go through a proxy server
- HTTP, SOCK proxy

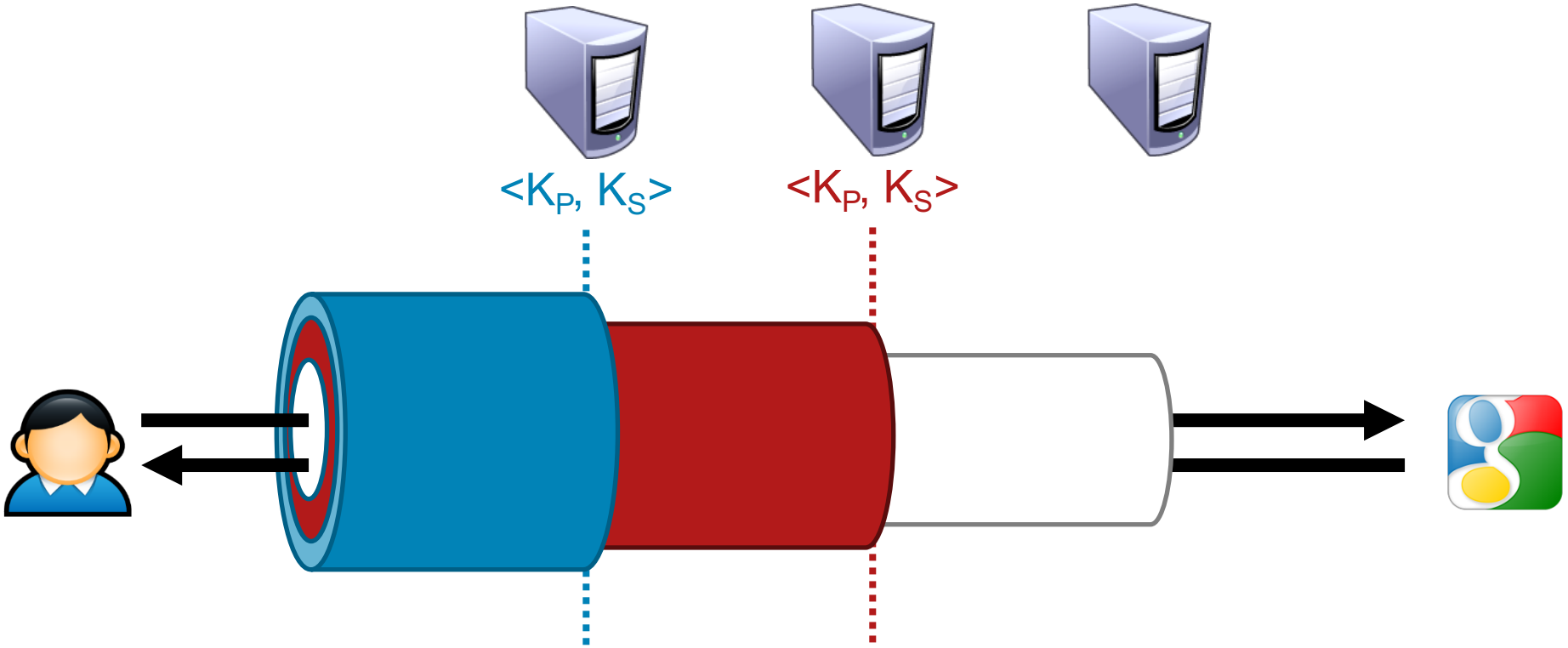
Mix networks, onion routing

- Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* 24.2 (1981): 84-90.
- Ispiration for:
  - Onion routing
  - Traffic mixing
  - Dummy traffic (cover traffic)

Mix proxies a Onion Routing

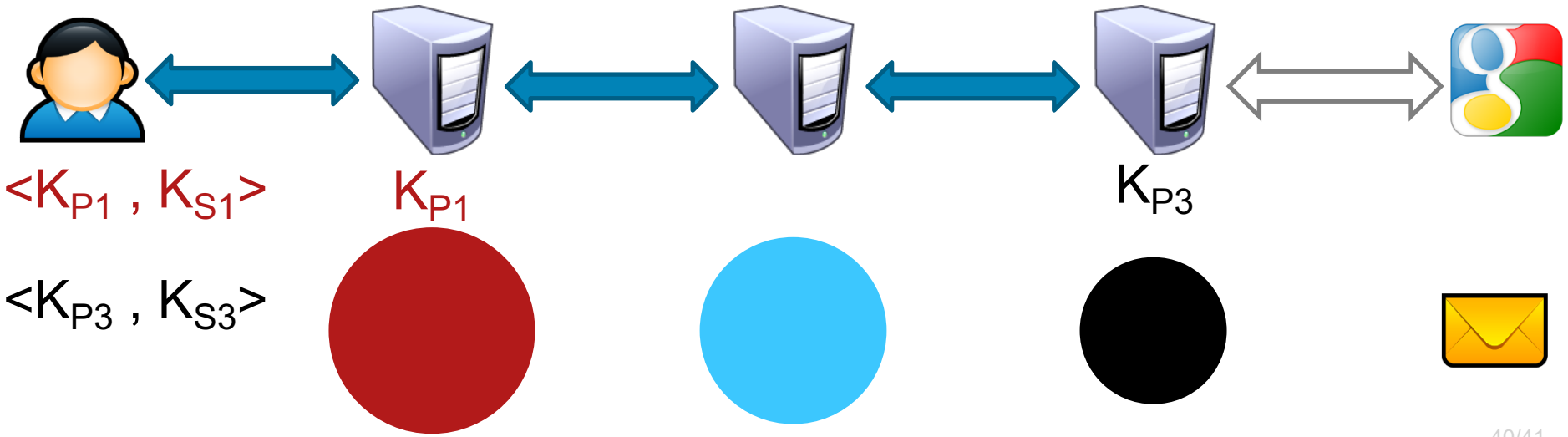


- Cascade of anonymouse proxies/servers
- Traffic is encrypted


<K_P, K_S>
<K_P, K_S>

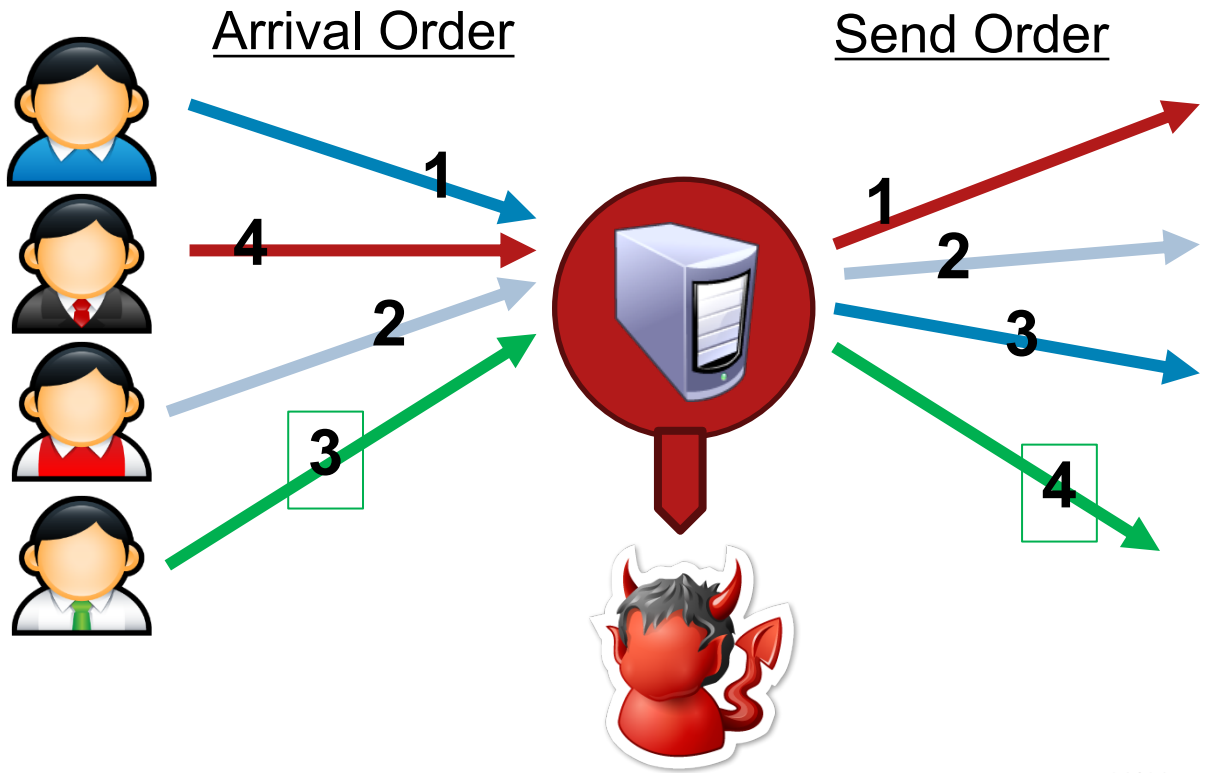
Return Traffic

- What about return traffic?
- Sender can leave keys on the path



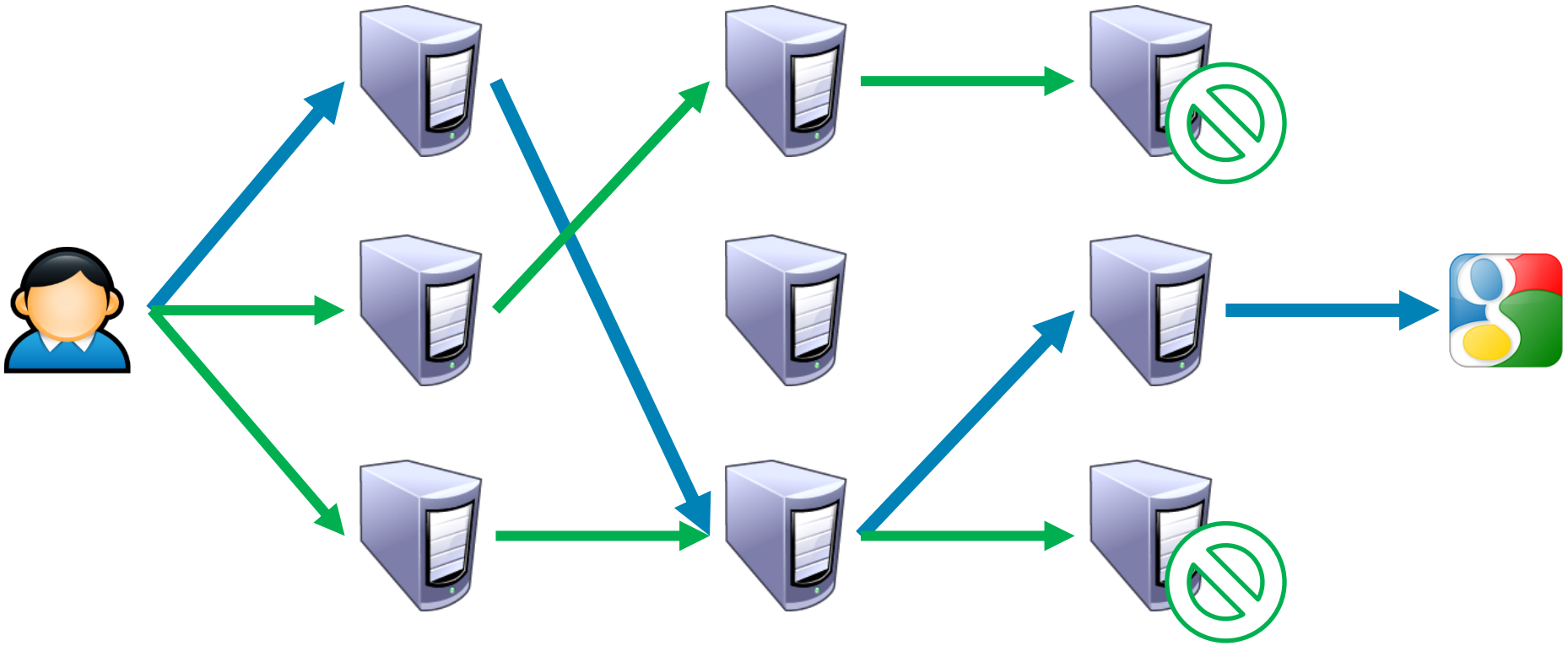
Traffic Mixing

- Protection against timing attacks
- Disadvantages:
  - Needs heavy traffic
  - Add delay/latency



Dummy / Cover Traffic

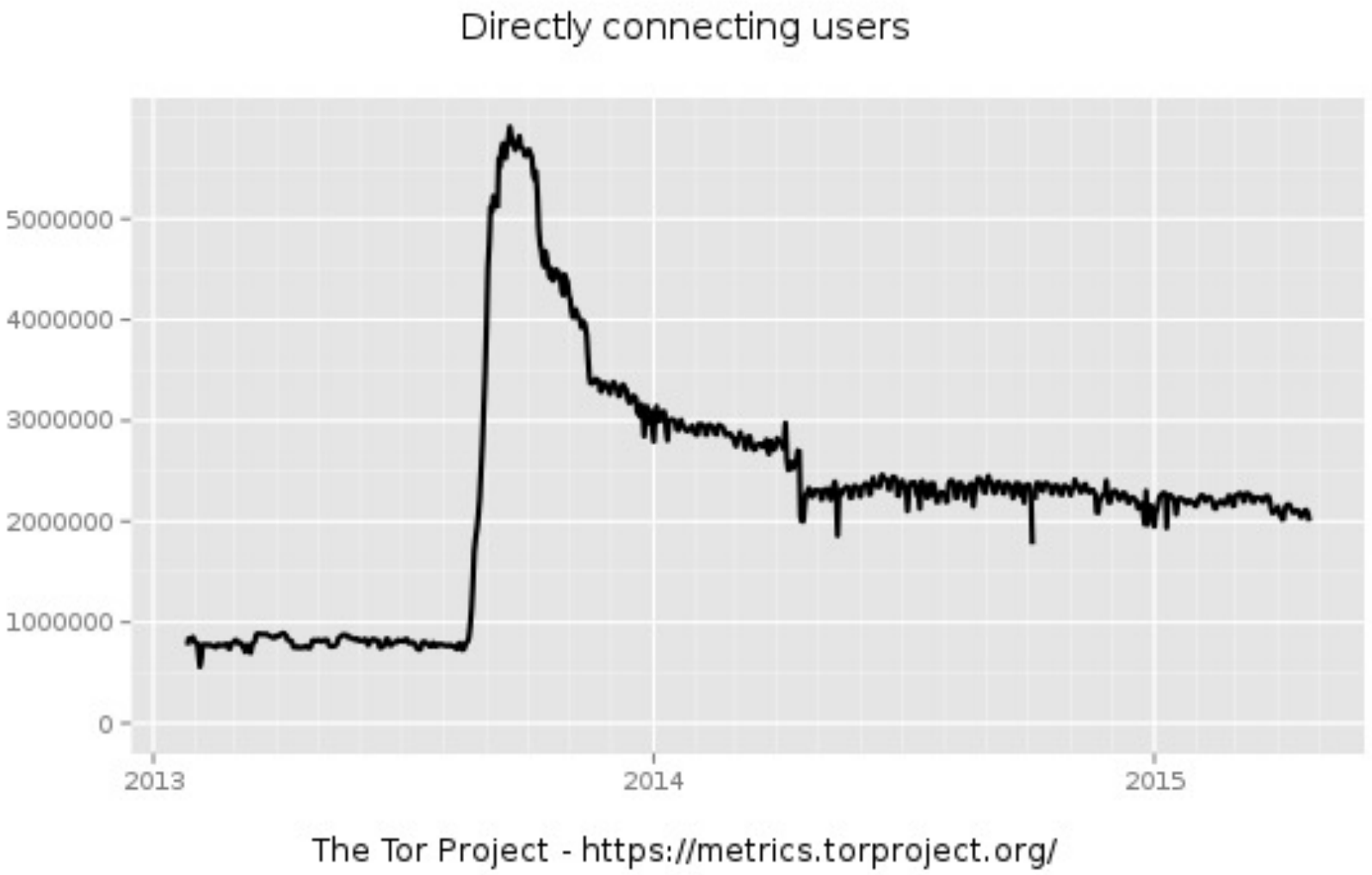
- Sending cover traffic that is discarded in the network



Torproject.org

- Advanced mix network:
  - Guards: enhance source anonymity
  - Relays: mix proxy
  - Hidden services: servers accesible only through Tor (darknet)
- ~5000 Tor relays
  - Run by volunteers, universities, organisations
  - It‘s expected that some run by „intelligence agencies“
- 1 – 2 mil. users

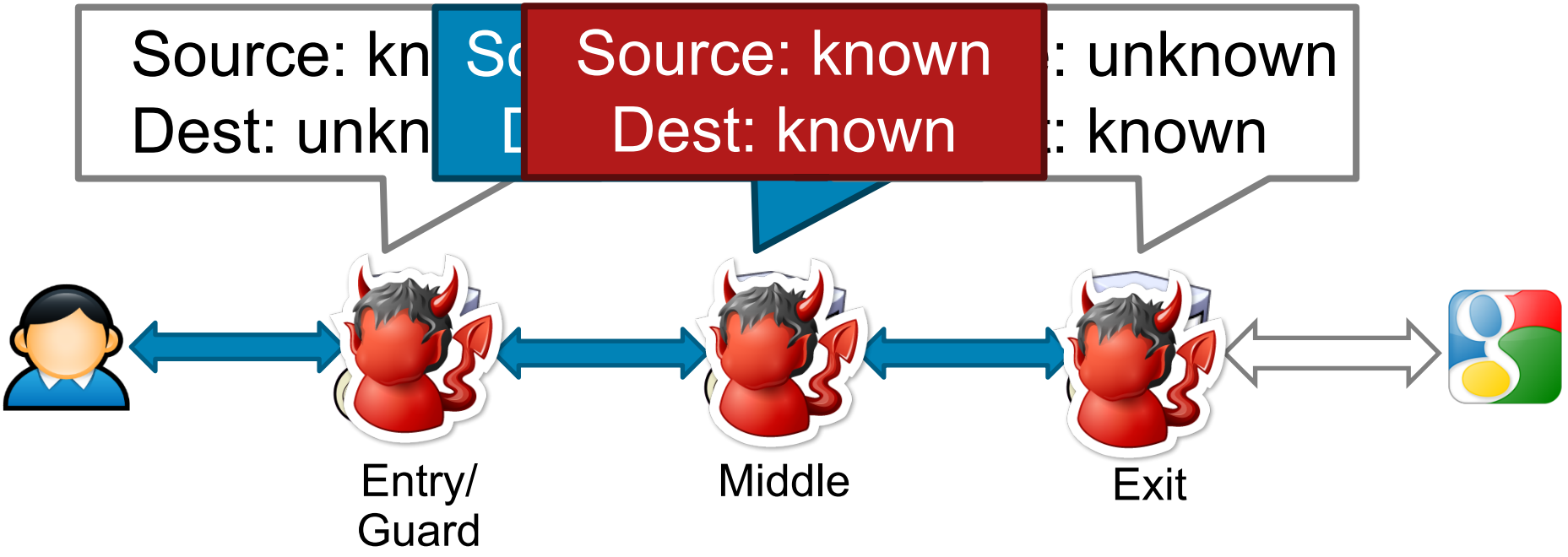
Torproject.org



Torproject.org

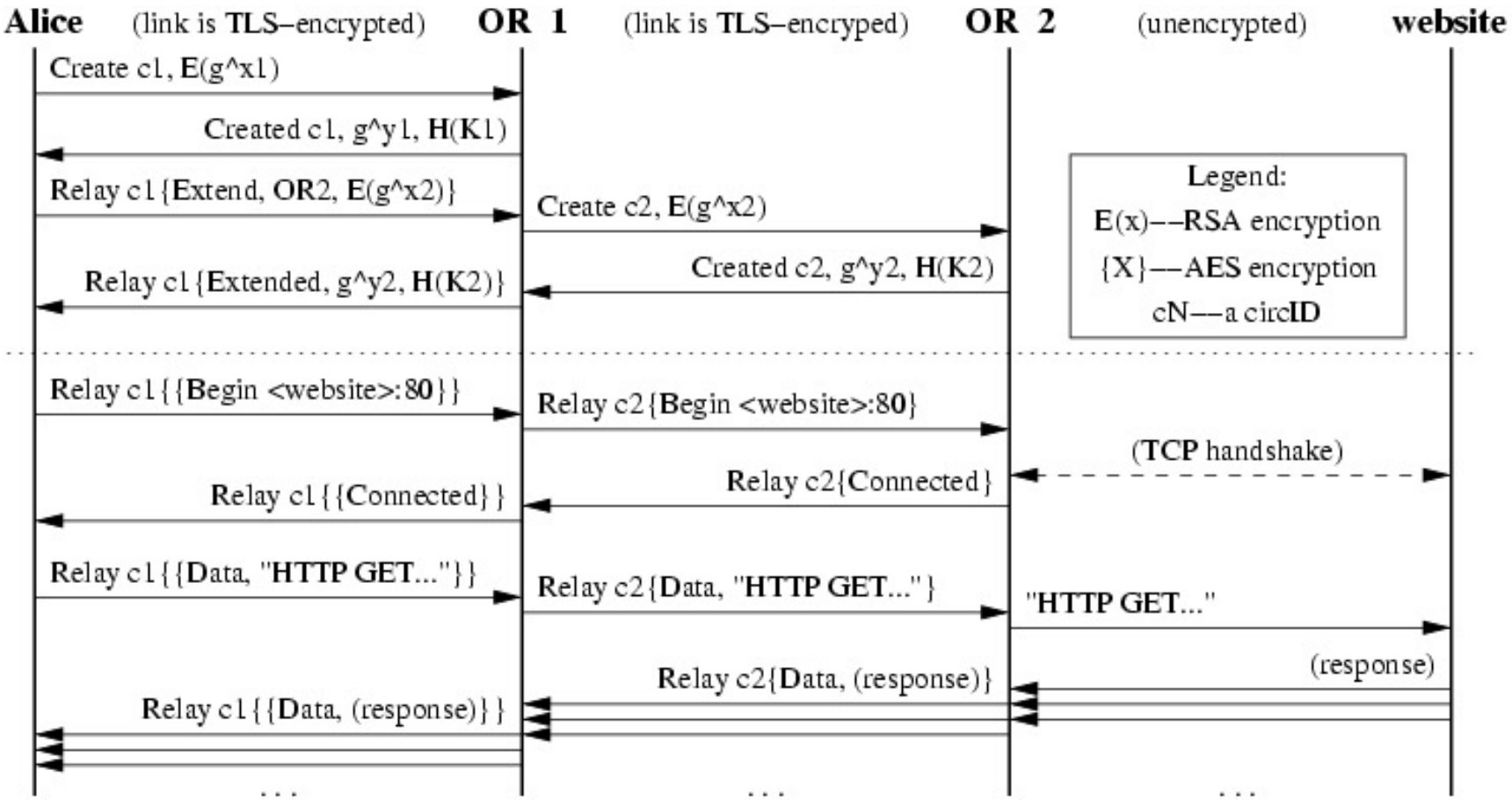
- Tor client acts as a SOCKS proxy
  - Creates and manages circuits
- Support for all application that can connect via SOCKS proxy
- How to find a Tor relay?
  - Tor Consensus File
    - Hosted by directory servers
    - IP addresses of all known relays
      - IP address, uptime, measured bandwidth, etc.
- Packets are divided to cells 512 bajtů
  - Decrease speed, increase anonymity
- https://gitweb.torproject.org/torspec.git/blob/HEAD:/tor-spec.txt

Tor Circuits



- Number of relays can be selected
  - Implicitně 3

Communication example



Guard Relays

- Guard relays protect agains attacker that acts as a entry relay
  - Tor picks 3 guard relays and use them for some time
  - The latest Tor version choose only one guard relay. Why?
- Guard relay:
  - Large uptime
  - Bandwith

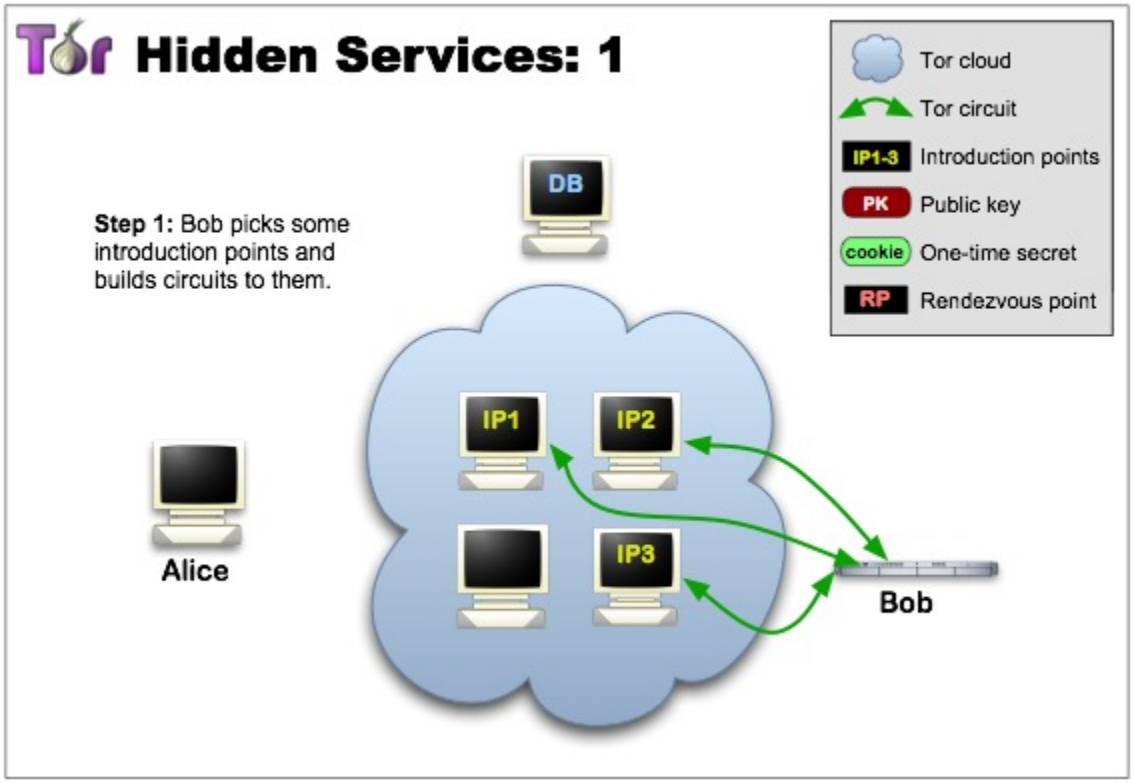
Guard relays attack

- Assumption:
  - *N* : number of relays
  - *M* : number of relays controlled by an attacker
- Attacker‘s goal – control entry and exit relay
  - ~ M/N probability for entry relay
  - ~ (M-1)/(N-1) probability for exit relay
  - ~ $(M/N)^2$ probability for one circuit
- Client creates new circuits
  - Attacker chance increase during long time period

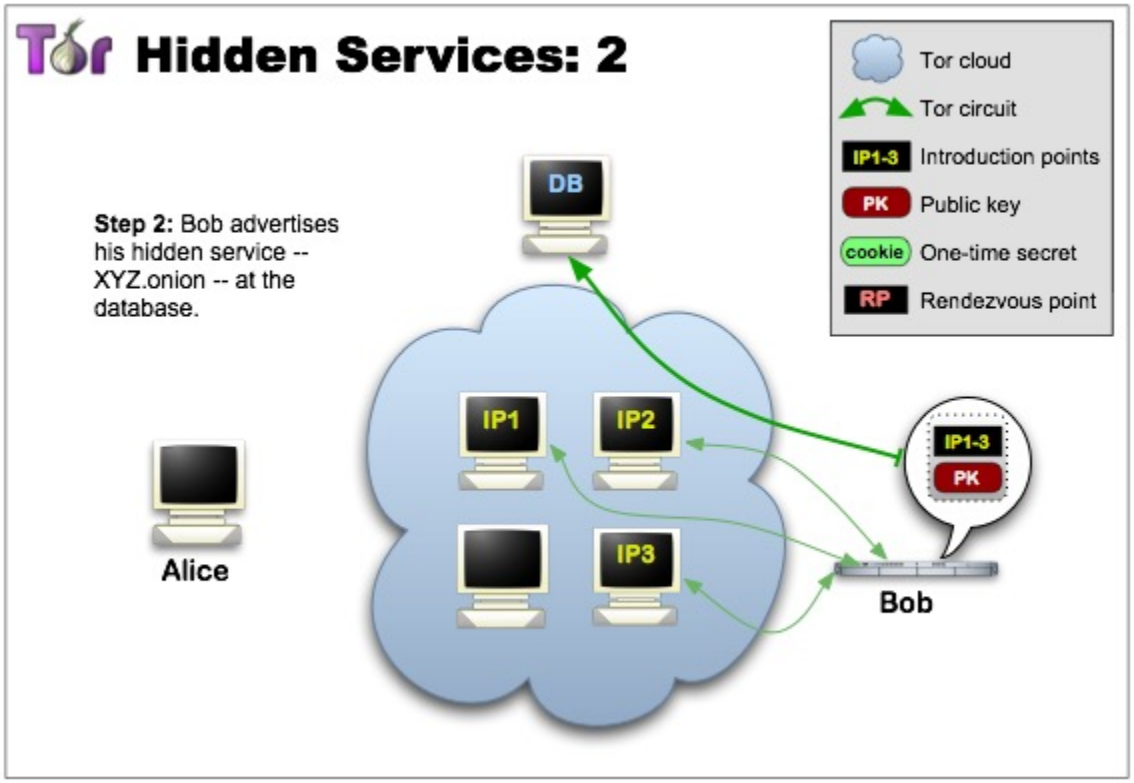
Hidden services

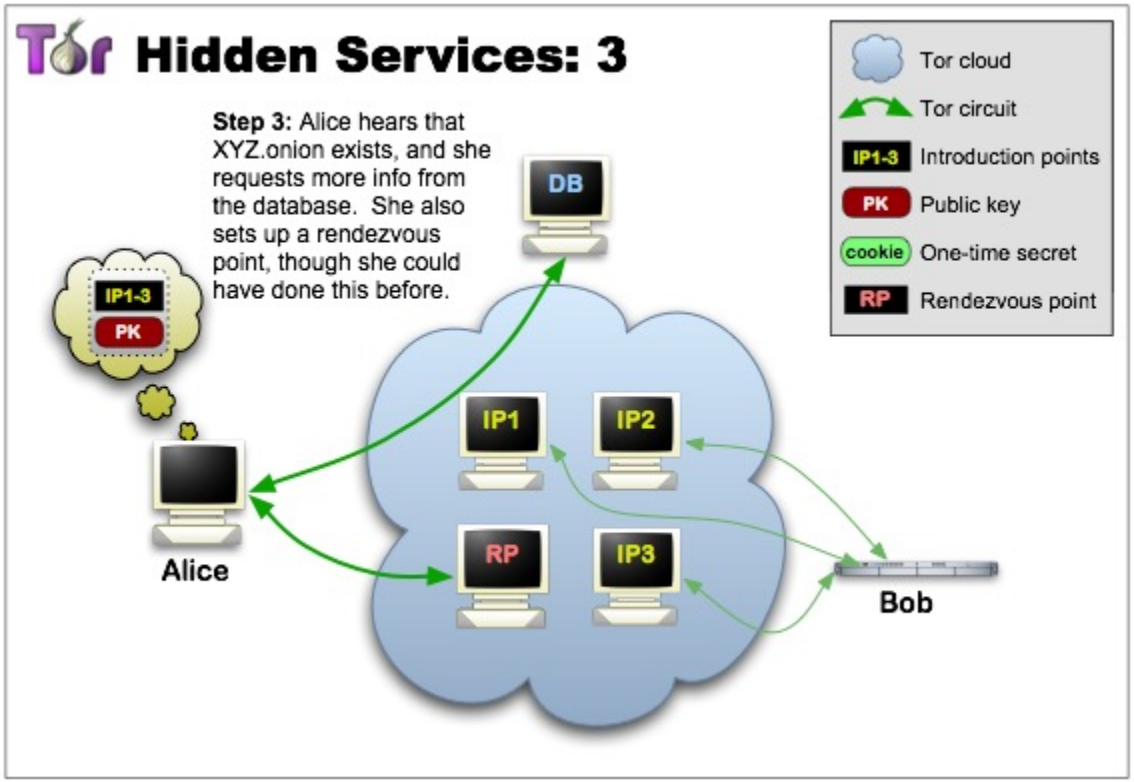
- Web services can be easily monitored
- Tor Hidden Services
  - Allows run an anonymous server without exposing its IP address or DNS name
- Services
  - Tor Mail, Tor Char
  - DuckDuckGo
  - Wikileaks
  - The Pirate Bay, Silk Road …

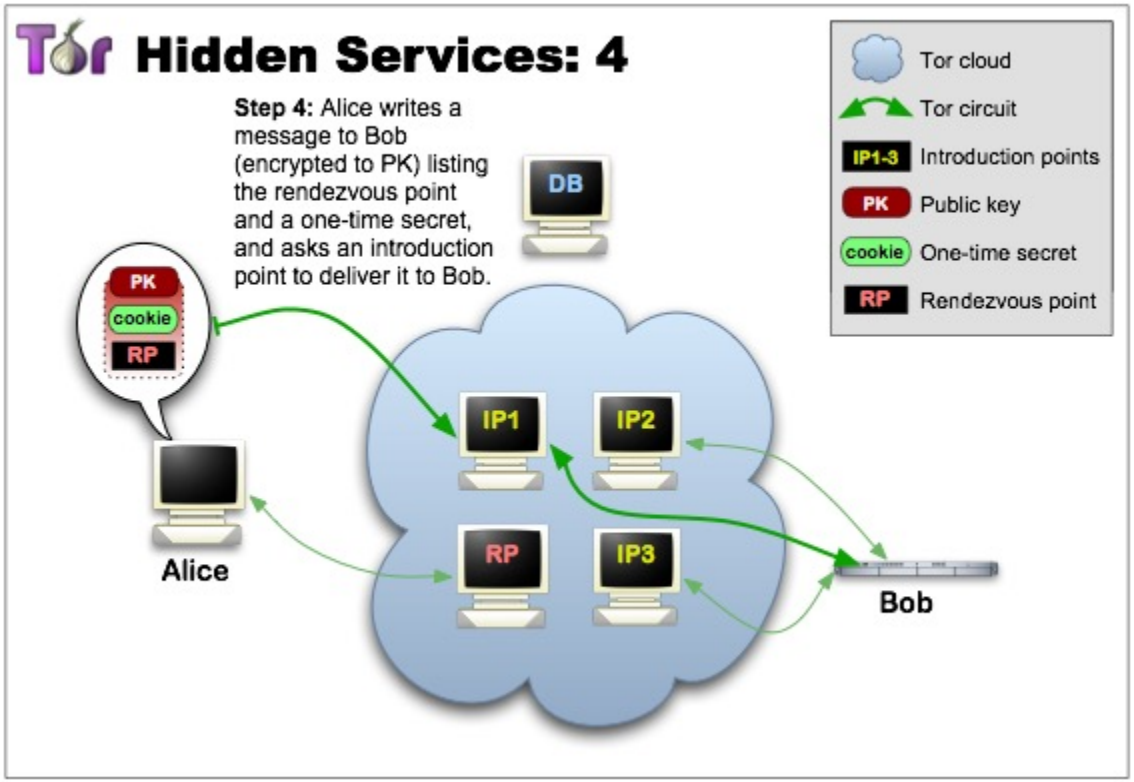
Hidden Services: 1

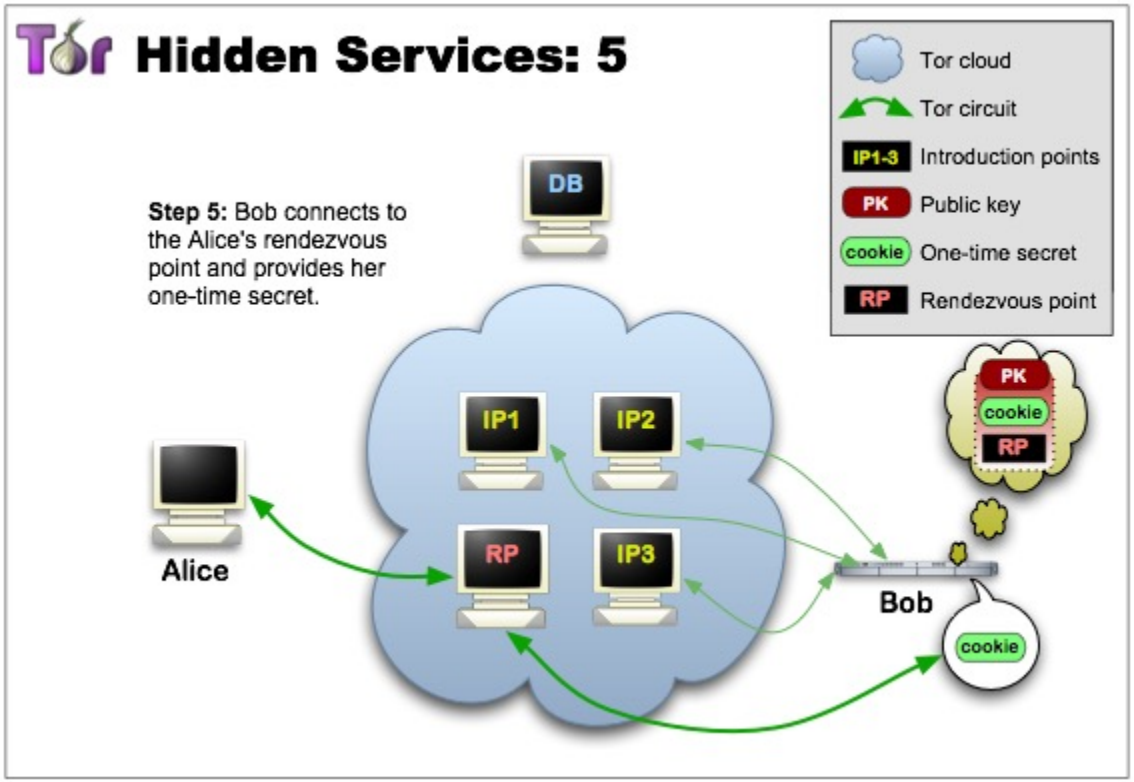


Hidden Services: 2

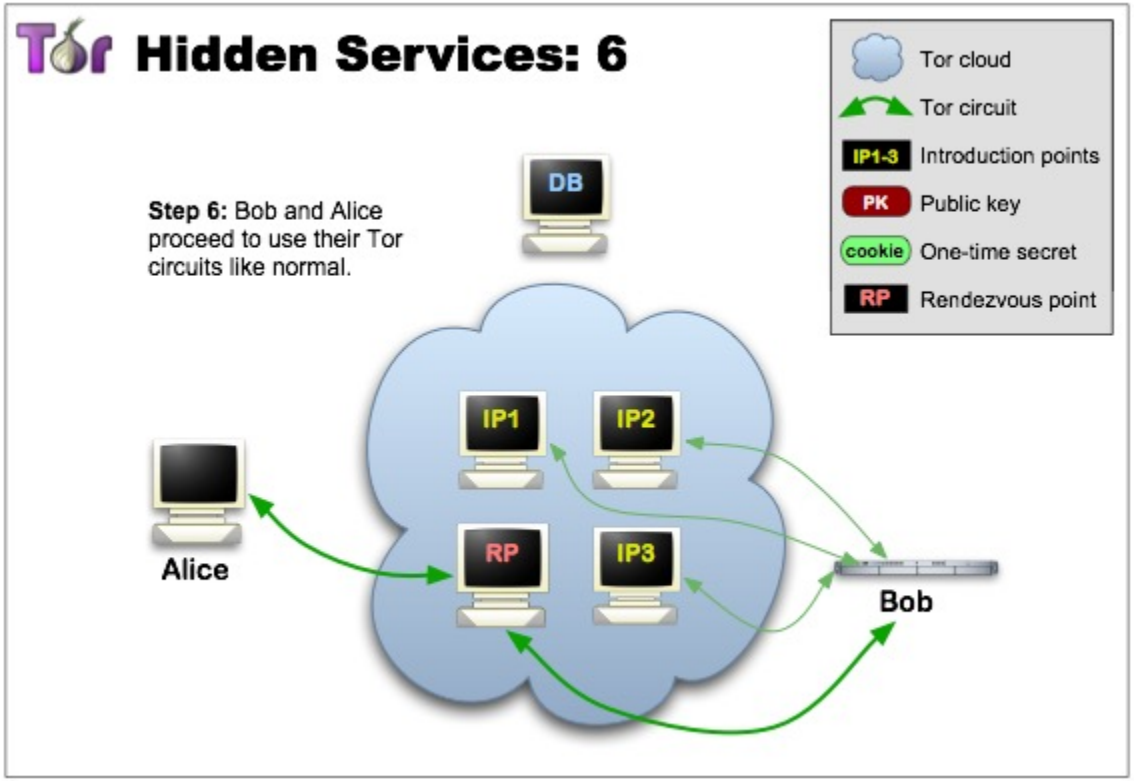



Hidden Services: 3
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.
Tor cloud
Tor circuit
IP1-3 Introduction points
PK Public key
cookie One-time secret
RP Rendezvous point
DB
IP1-3
PK
IP1
IP2
RP
IP3
Alice
Bob


Hidden Services: 4
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.
DB
PK
cookie
RP
Alice
IP1
IP2
RP
IP3
Bob
Tor cloud
Tor circuit
IP1-3
Introduction points
PK
Public key
cookie
One-time secret
RP
Rendezvous point


Hidden Services: 5
Tor cloud
Tor circuit
IP1-3 Introduction points
PK Public key
cookie One-time secret
RP Rendezvous point
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.
DB
IP1
IP2
RP
IP3
Alice
Bob
PK
cookie
RP
cookie

Hidden Services: 6

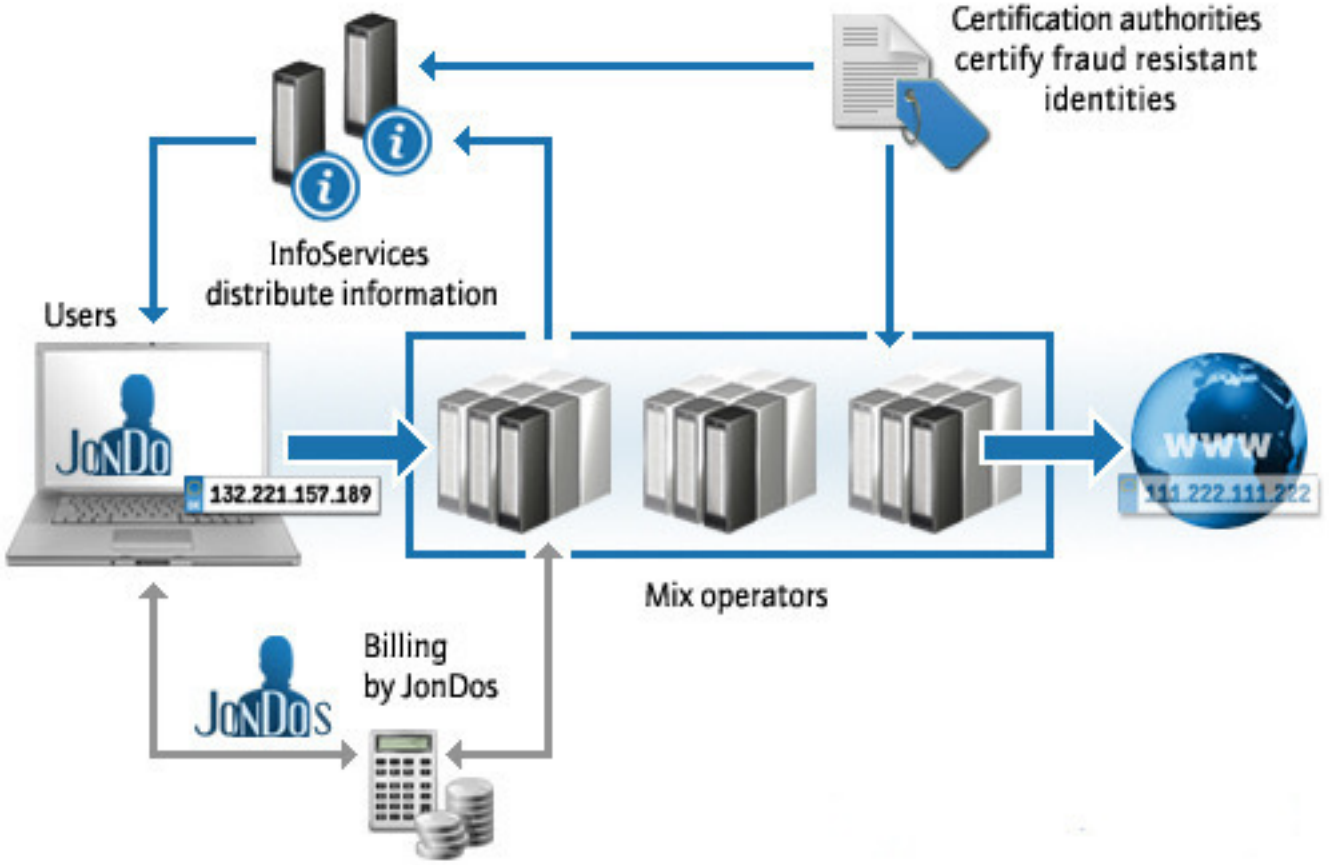


Tor Bridges

- Tor relays is publicly accessible
- Some countries block these IPs
  - DoS vůči Tor
- Tor Bridges
  - Tor proxy, that is not included in the directory

- Tor packets can be detected using the DPI (fix cells)
  - Traffic obfuscating – traffic acts as HTTP, Bittorrent …

JohnDonym


Certification authorities
certify fraud resistant
identities
InfoServices
distribute information
Users
JoNDo
132.221.157.189
Mix operators
WWW
111.222.111.222
Billing
by JonDos
JoNDoS

Other projects

- Snapchat – message can be destroyd after some time
  - http://ridgewood.patch.com/groups/police-and-fire/p/nude-photos-of-ridgewood-high-girls-prompt-police-investigation
- Cjdns – P2P anonymous network using IPv6
- Secret.ly – social network
- Telegram, Whisper, Wickr, Confide
- Reddit
- Vuvuzela
- freehaven.net/anonbib/