

Anonymita

Matěj Grégr

igregr@fit.vutbr.cz

Obsah

- Anonymita
- Adresy
- Onion, garlic routing
- Zajímavé projekty

Anonymita?

- IP adresa může být svázaná přímo s uživatelem
 - ISP si ukládá informace o komunikaci
 - Uloženy typicky po určitou dobu (Data Retention)
 - Law enforcement agency
- Browser fingerprinting
 - Cookies, Flash cookies, E-Tags, HTML5 Storage
 - Browser fingerprinting
- User fingerprinting
 - Aktivita uživatele – které aplikace používá, na které weby přistupuje

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*

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

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

CentOS 6

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

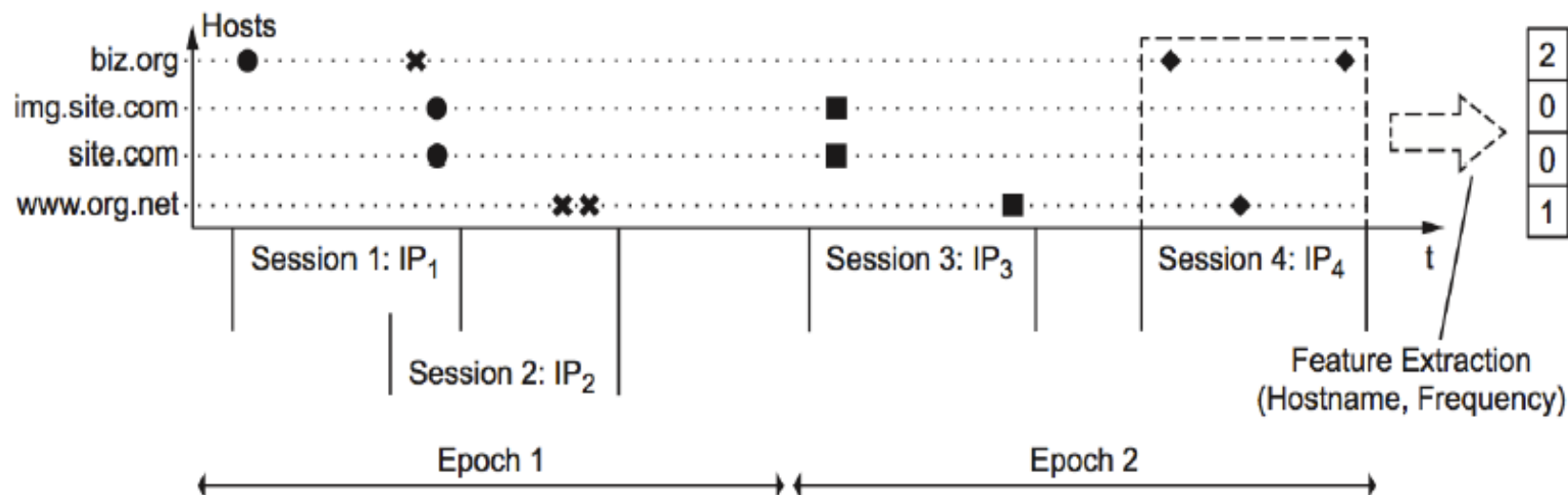
*apis.google.com clients.l.google.com clients1.google.com
safebrowsing-cache.google.com
safebrowsing.clients.google.com ssl.gstatic.com
www.google.com www.google.de www.gstatic.com*

Safari

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

Internet Explorer

Fingerprinting – user behavior



Dominik Herrmann, Christian Banse, Hannes Federrath:
Behavior-based tracking: Exploiting characteristic patterns in DNS traffic

Kdo využívá anonymní přístup?

- “Pokud neděláte nic špatného, nemáte co skrývat.”
 - Anonymní chtějí být pouze kriminálníci?
 - Novináři
 - Law enforcement
 - Podpora lidských práv
- Vyhnutí se postihu
 - Ne každá země povoluje právo na svobodu projevu
- Vyhnutí se „chilling-effects“
 - Kontroverzní, nepopulární myšlenky

Definice?

- Unlinkability

- Neschopnost spojit dvě události
 - Např. pakety, přístupy na web, lidi, akce
- Tři části:
 - Sender anonymity (Kdo to poslal?)
 - Receiver anonymity (Kdo je příjemce?)
 - Relationship anonymity (Jsou A a B v nějakém spojení?)

- Unobservability

- Nelze rozlišit monitorované události od jiných

IP adresa


- IP – globálně unikátní identifikátor
- Vstupní bod do sítě

Your IP address is:

147.229.192.6

ISP: Brno University of Technology


Hostname: kn.vutbr.cz


Country:  Czech Republic


State: Jihomoravsky Kraj

Hub City: Brno
(Routed Internet Connection)

Timezone: Europe/Prague

Browser:  Mozilla Firefox 26.0

OS:  Linux x86

Screen Res.:  1920x1200

Referrer: google.com

IP adresa – přidělení IANA to RIR ①

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



IP adresa – přidělení RIR to LIR to ISP ②

- Provider independent / aggregatable adresy
- Kdo je ISP dané adresy – země, město

```
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: FS6810-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
country: CZ
admin-c: VS47
tech-c: VZ36-RIPE
status: ASSIGNED PI
mnt-by: VUIBR-MNT
mnt-routes: VUIBR-MNT
remarks: Please report network abuse -> abuse@vutbr.cz
source: RIPE # Filtered
```

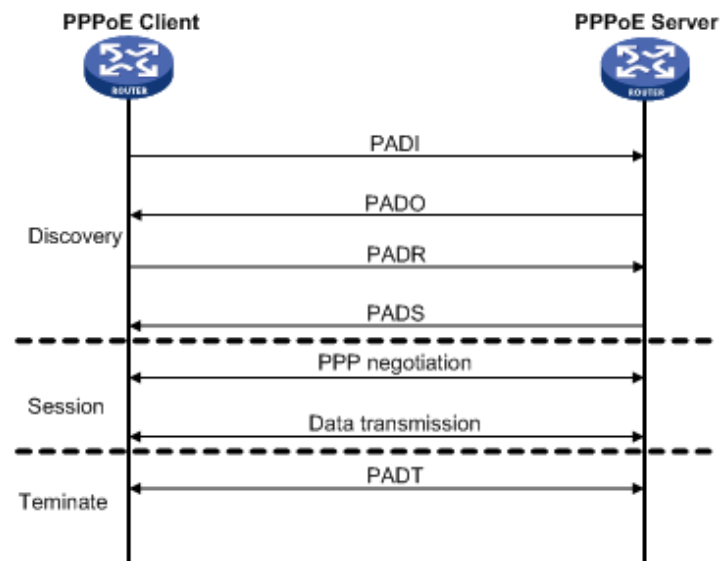
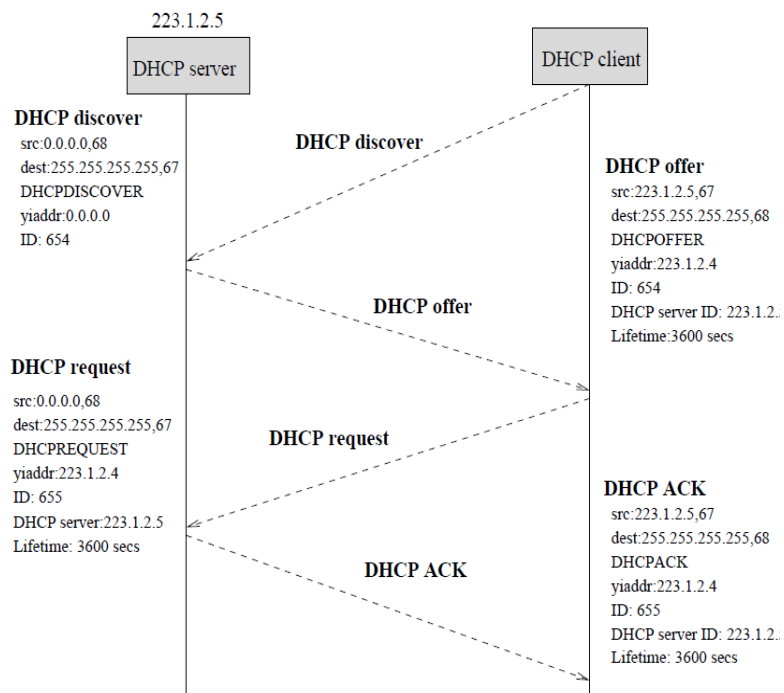
```
person: Vit Slama
address: Brno University of Technology
address: Center of Computing and Information Services
address: Antoninska 1
address: Brno
address: 601 90
address: The Czech Republic
phone: +420 541145630
fax-no: +420 541145419
nic-hdl: VS47
mnt-by: DKT-MNT
source: RIPE # Filtered
```

```
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: VUIBR-MNT
source: RIPE # Filtered
```

IPv4 adresa – přidělení uživateli

- DHCP, PPPoE
- ISP si uloží informaci kdo žádal (MAC, DHCP82, username) a jaká adresa byla přidělena



IPv6 adresa – přidělení uživateli

Router Advertisement

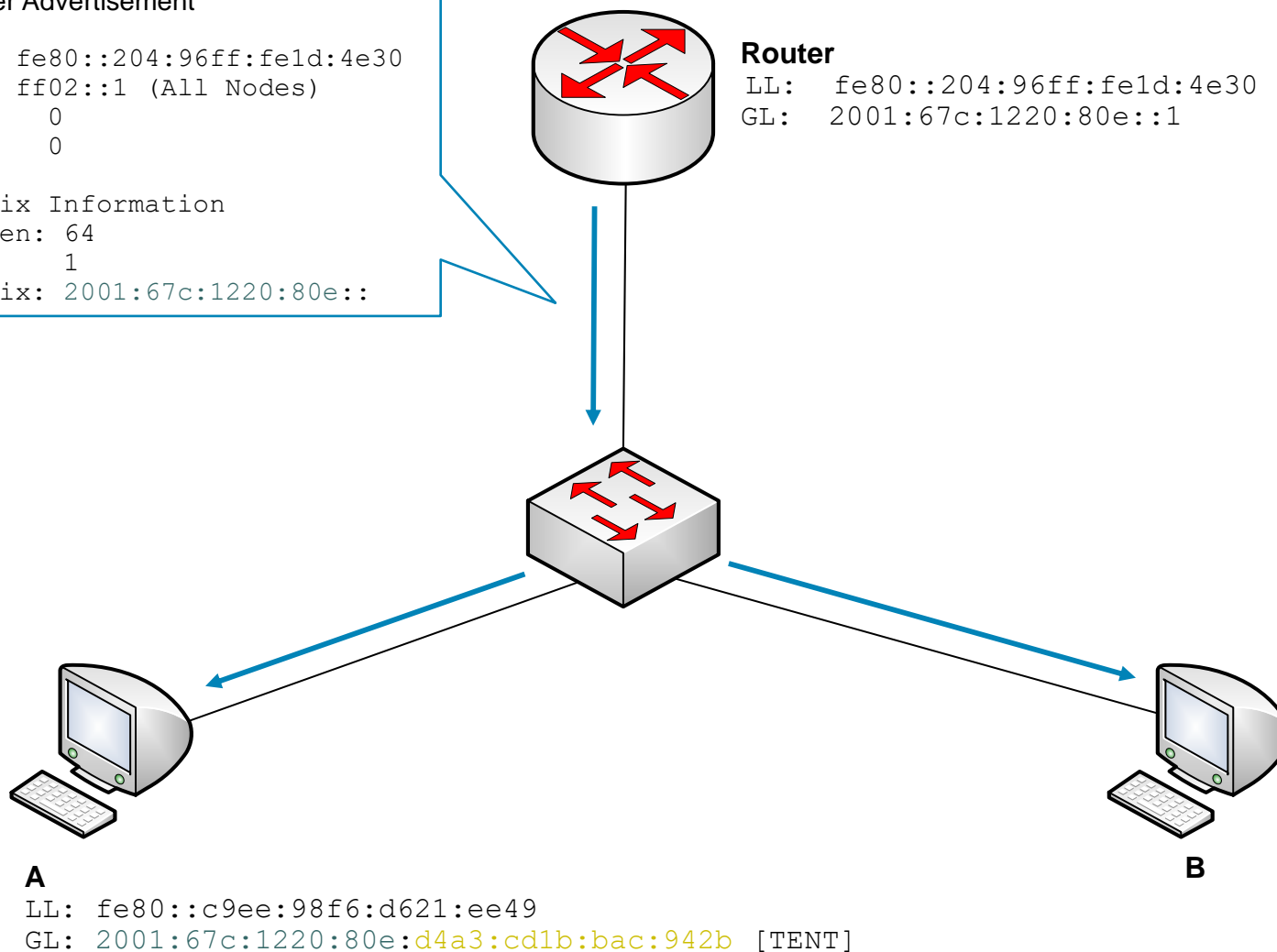
```
src: fe80::204:96ff:fe1d:4e30  
dst: ff02::1 (All Nodes)  
M: 0  
O: 0
```

Prefix Information

```
PrfLen: 64  
A: 1  
Prefix: 2001:67c:1220:80e::
```

Router

```
LL: fe80::204:96ff:fe1d:4e30  
GL: 2001:67c:1220:80e::1
```



IP adresa

- IPv4

- ISP má typicky vždy informaci, který uživatel má přidělenou kterou IPv4 adresu

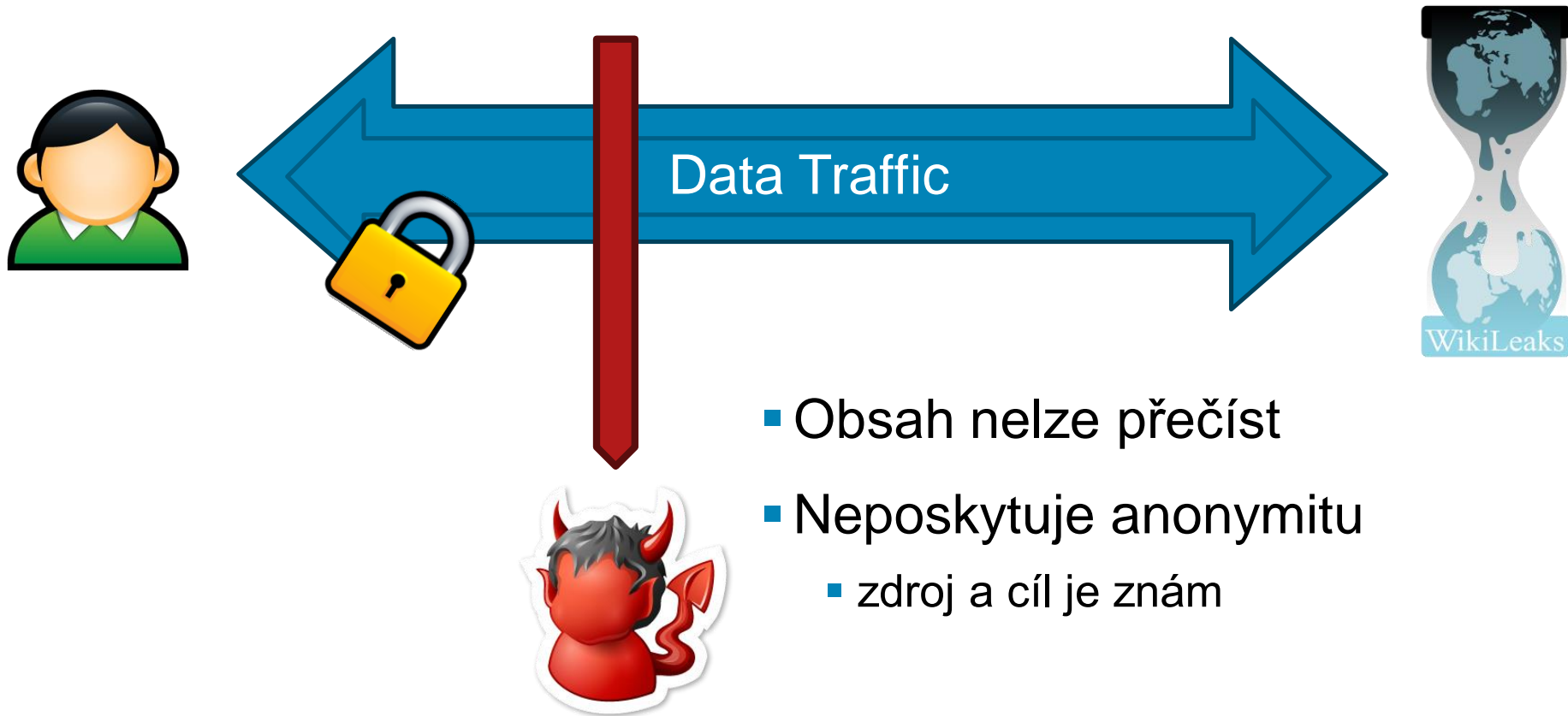
- IPv6

- Přidělení prefixu – podobná situace jako u IPv4
 - Přidělení adresy (metro Ethernet) – problematičtější získání informací

- ISP tyto informace uchovává téměř vždy i bez DR

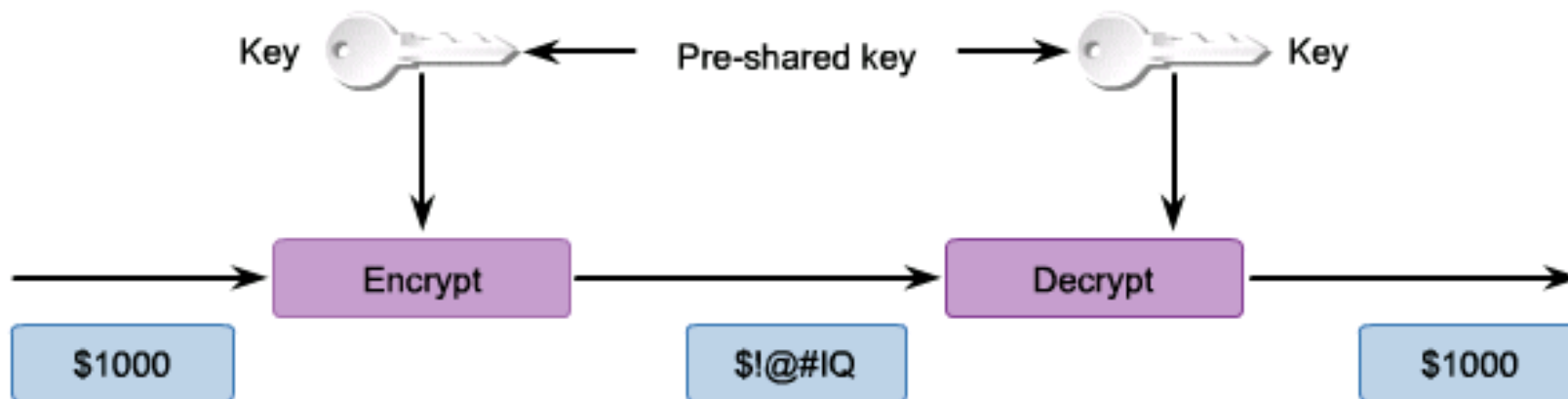
- Dohledávání problémů, účtování ...

Šifrování?



Symetrické kryptografie

- Algoritmy se sdíleným klíčem, který se používá jak pro šifrování, tak pro dešifrování
- Stejný klíč znají obě strany, bezpečnost spočívá v ochraně klíče



Symetrická kryptografie

- Plaintext message M
 - E – symetrický šifrovací algoritmus
 - K - klíč

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

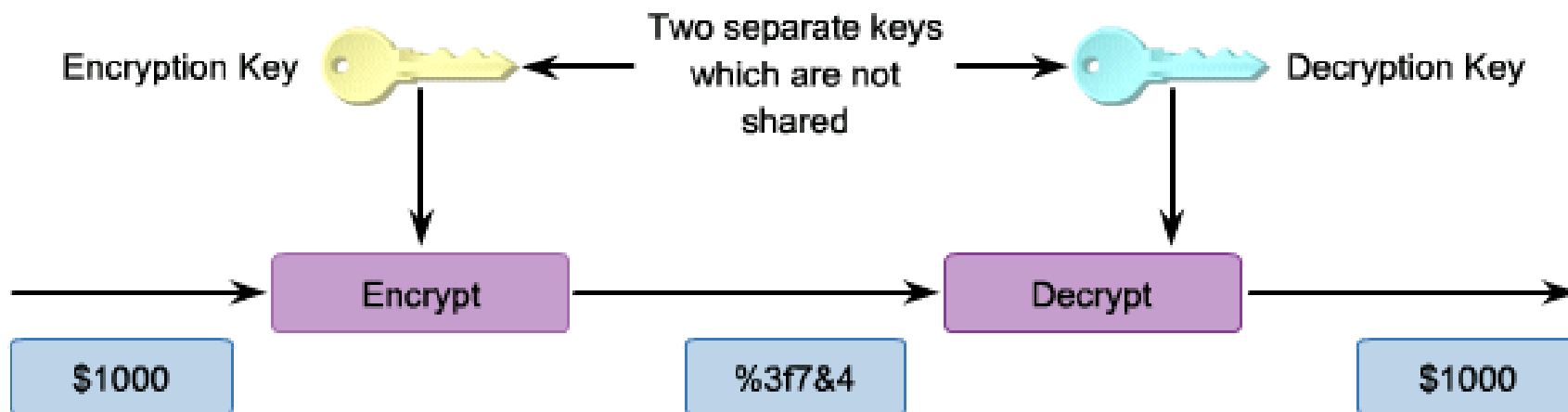
- Výhody
 - Rychlost, jednoduchost
- Nevýhody
 - Distribuce klíčů

Symetrické Algoritmy

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.

Asymetrická kryptografie

- Používá se dvojice navzájem svázaných klíčů – veřejného a privátního
- Oproti symetrickým algoritmům je délka klíče mnohem větší k zajištění stejné míry zabezpečení
- Asymetrické algoritmy jsou náročné na výpočetní prostředky (100× až 1000× pomalejší)



Privátní a veřejný klíč

- Privátní klíč zná a vlastní pouze majitel
- Veřejný klíč je k dispozici komukoli
- Oba klíče jsou rozdílné a je výpočetně „nemožné“ odvodit z jednoho klíče druhý
- Každý z klíčů může být použitý jak pro šifrování tak dešifrování
 - privátní šifruje, veřejný dešifruje
 - veřejný šifruje, privátní dešifruje

Asymetrická kryptografie

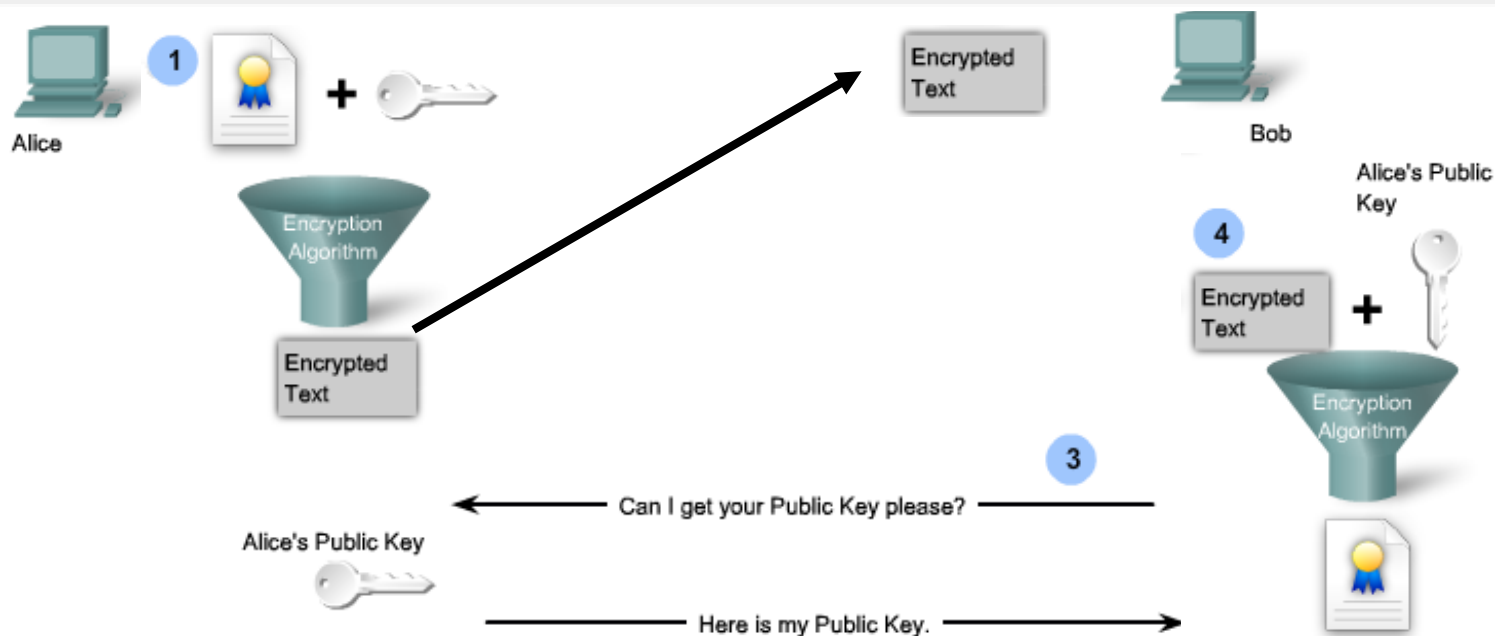
- Plaintext message M
 - F – asymetrický šifrovací algoritmus
 - K_P (veřejný klíč), K_S (privátní klíč)

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

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

Autentifikace, (nepopiratelnost)

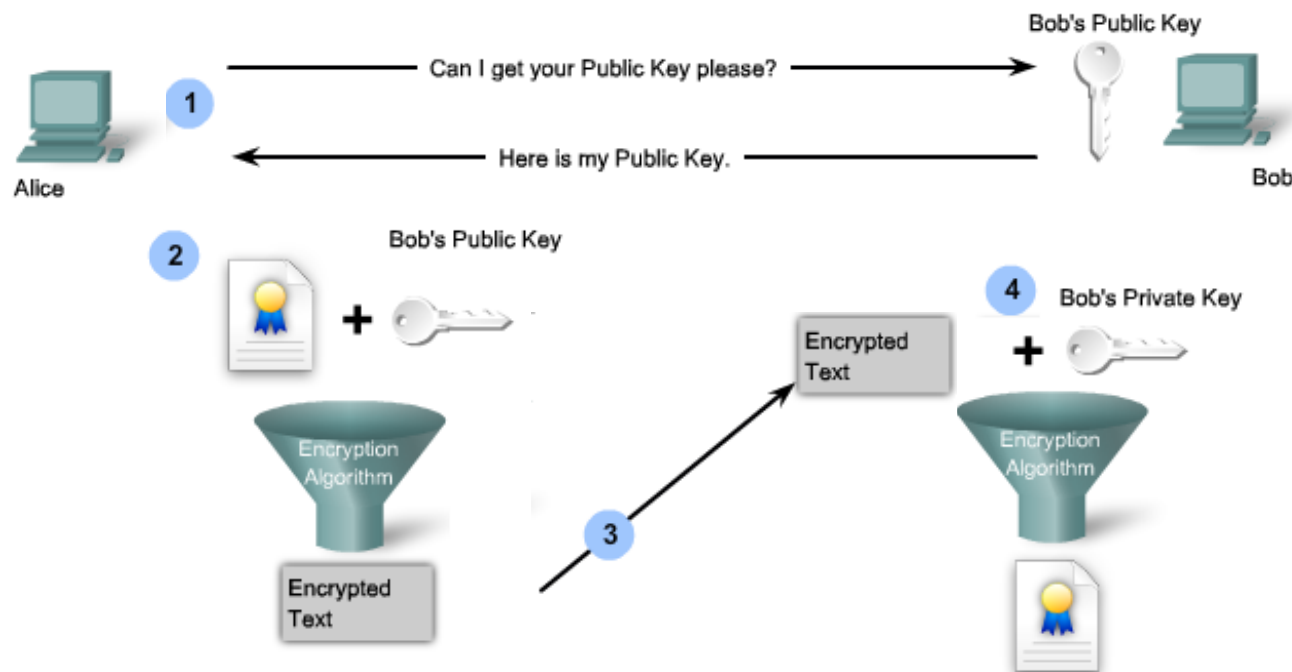
Private Key (Encrypt) + Public Key (Decrypt) = Authentication



1. Alice zašifruje zprávu jejím vlastním privátním klíčem.
2. Alice pošle cipher-text Bobovi.
3. Bob si zažádá o Alicin veřejný klíč k ověření pravosti zprávy.
4. Aby Bob ověřil, že zpráva pochází od Alice, použije na její dešifrování Alicin veřejný klíč. Pokud je zpráva čitelná, je nepopíratelná, že Alice zprávu poslala.

Důvěrnost

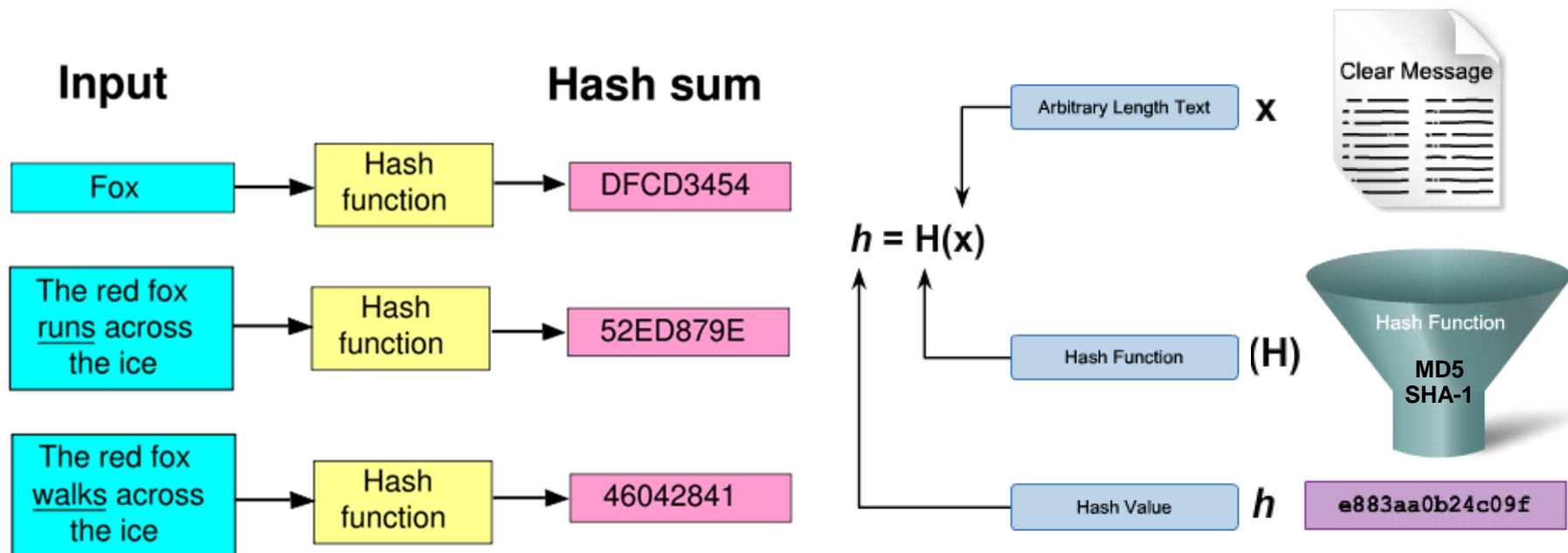
Public Key (Encrypt) + Private Key (Decrypt) = Confidentiality



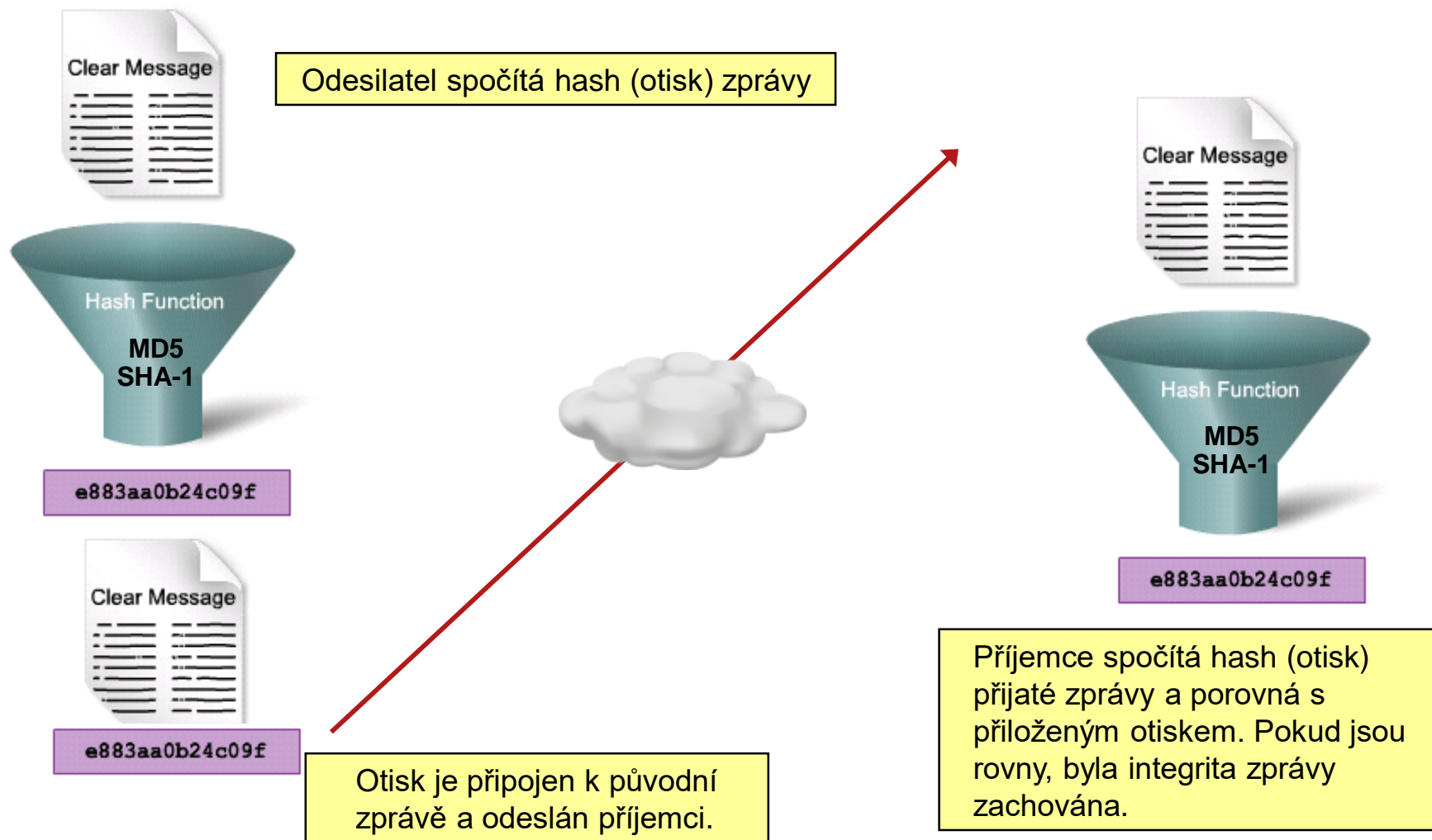
1. Alice požádá Boba o jeho veřejný klíč.
2. Alice použije Bobův veřejný klíč k zašifrování zprávy.
3. Alice pošle Bobovi cipher-text.
4. Bob použije svůj privátní klíč k dešifrování zprávy.

Hash

- Jednocestná matematická hash funkce bere na svém vstupu binární data libovolné délky a produkuje výstup fixní délky zvaný hash
- Hash se používá k zajištění integrity
- Hash funkce by mělo být co nejvíce odolná kolizím

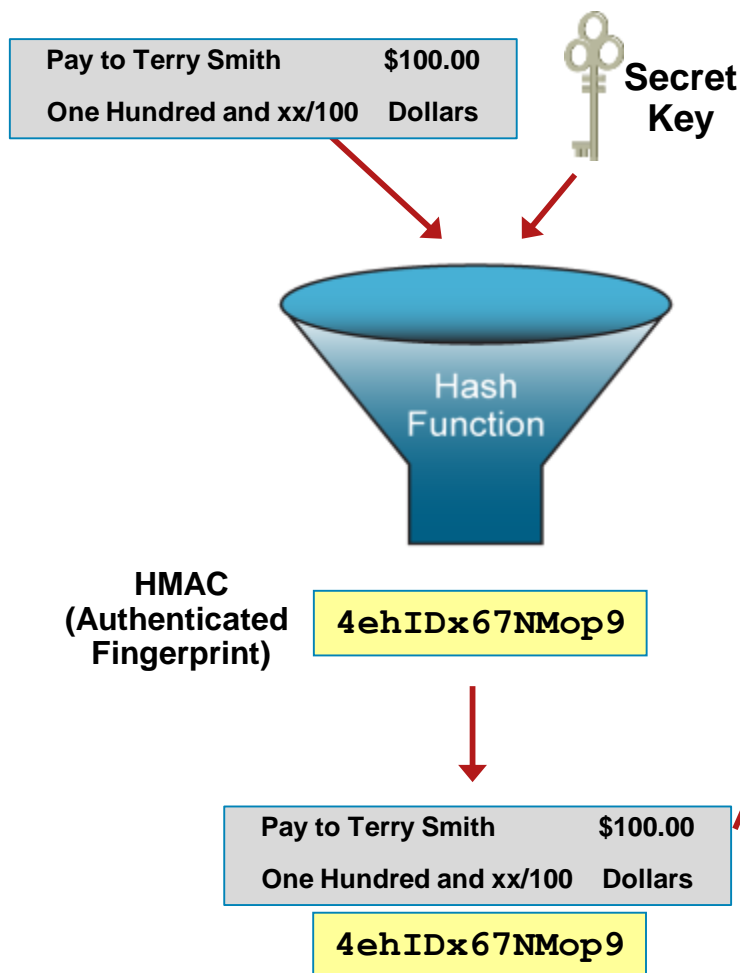


Integrita

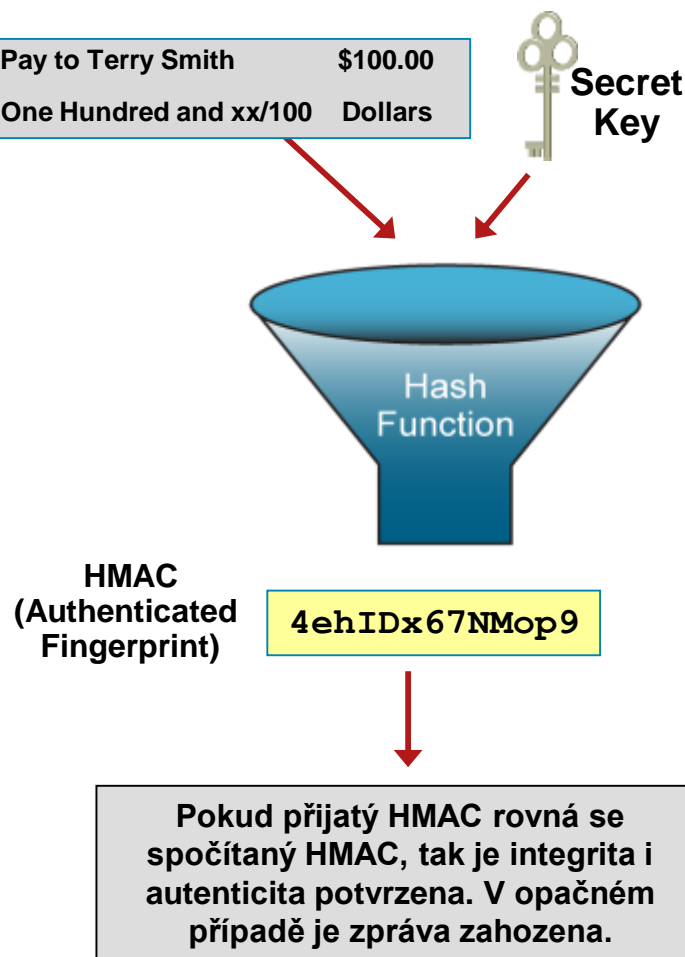


Hash-based message authentication code

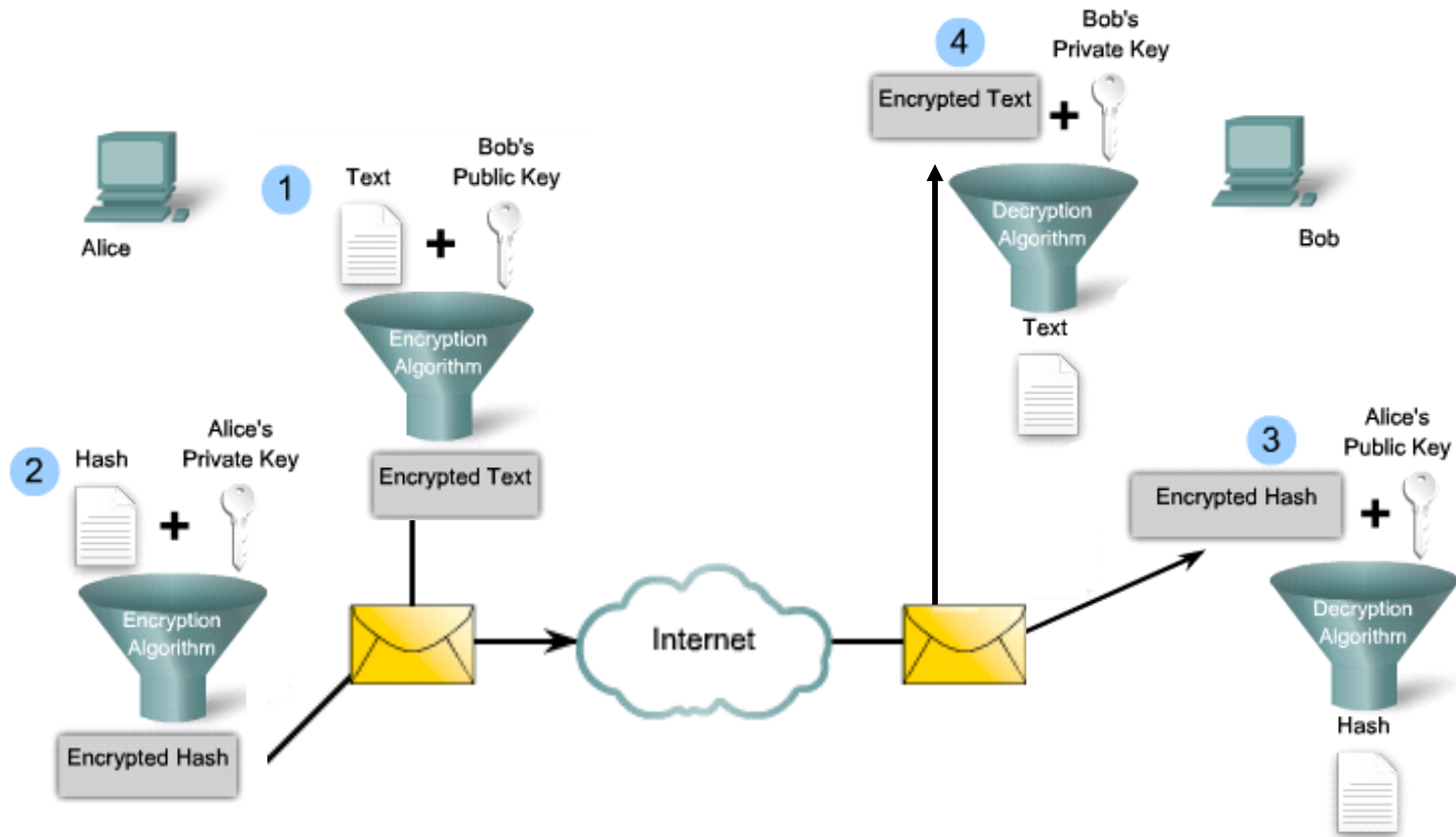
Data



Přijatá Data



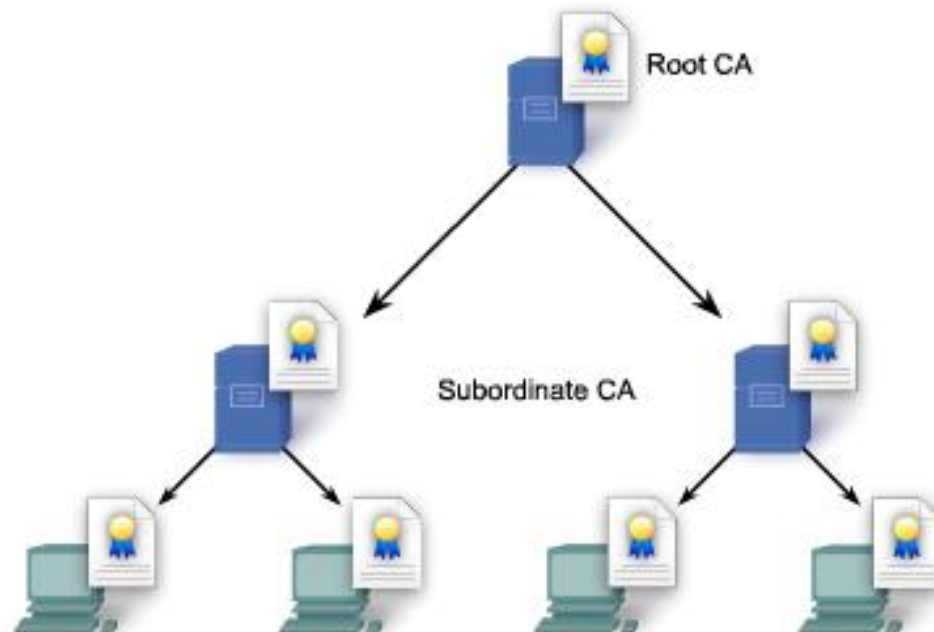
Asymetrická kryptografie + HMAC



1. Alice zašifruje zprávu za použití Bobova veřejného klíče.
2. Alice zašifruje HMAC svým vlastním privátním klíčem.
3. Bob použije Aliciin veřejný klíč k ověření HMAC zprávy.
4. Bob použije svůj privátní klíč k dešifrování cipher-textu.

Certifikát a Public Key Infrastructure (PKI)

- Ověření, že klíče vlastní opravdu uživatel = certifikát
- Hierarchie držitelů certifikátu a certifikačních autorit
- **Certifikační autorita** = důvěryhodná organizace, která vystavuje certifikáty a u které lze vydané certifikáty ověřit



Možné způsoby získání anonymity

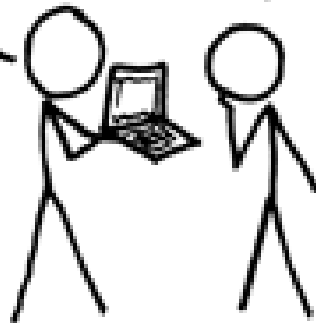
- VPN
- Proxy
- Onion routing
- Garlic routing
- Anonymní P2P síť
- End-to-end šifrování

A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR
CLUSTER TO CRACK IT.

BLAST! OUR
EVIL PLAN
IS FOILED!

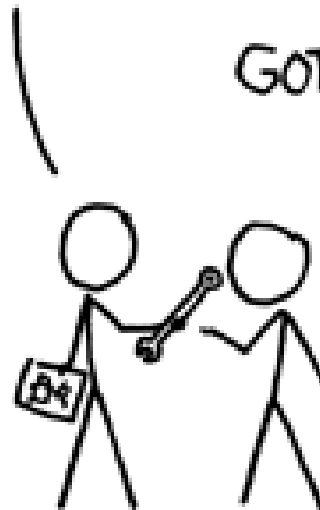
NO GOOD! IT'S
4096-BIT RSA!



WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH
THIS \$5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

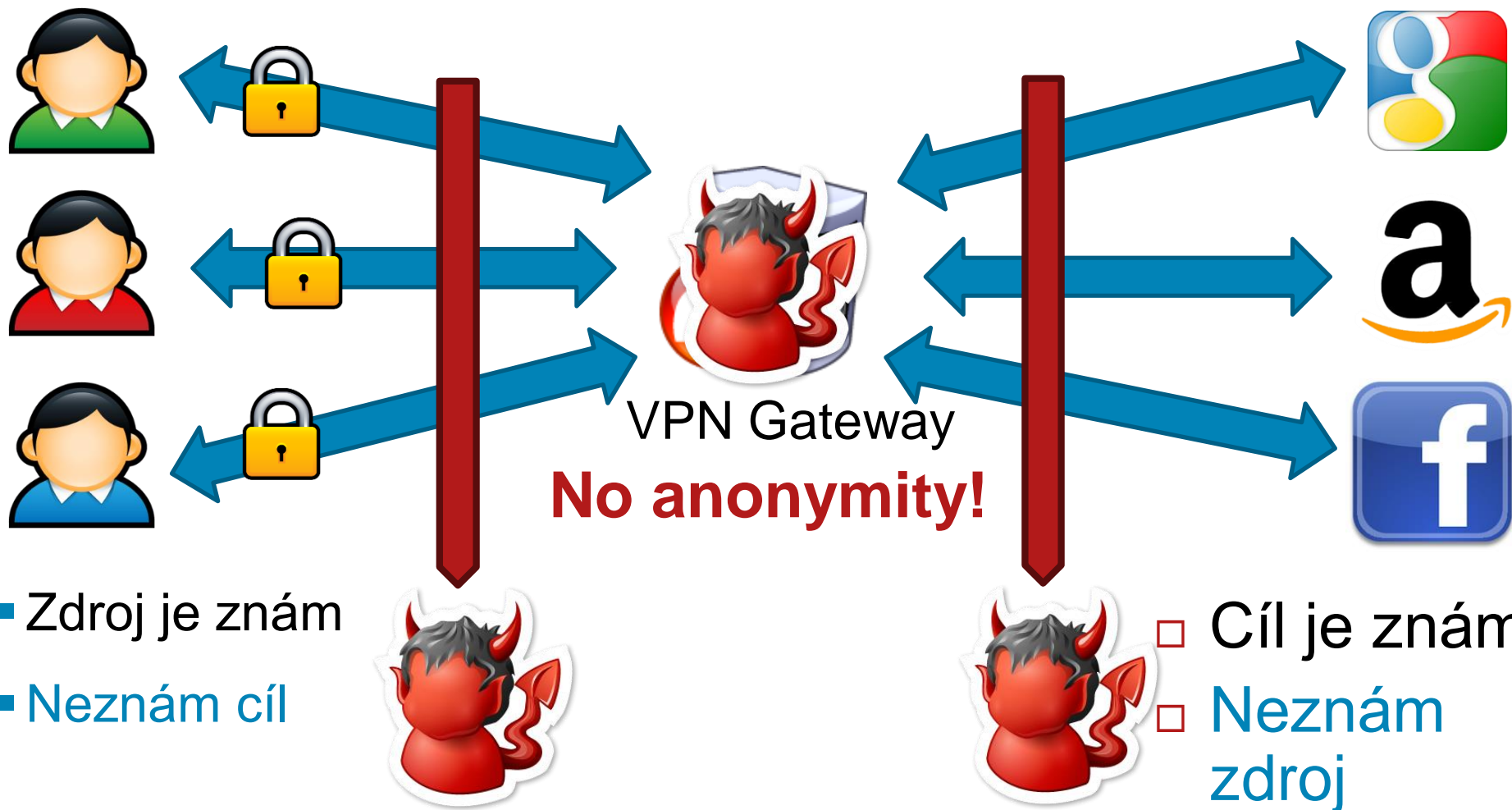
GOT IT.



<https://xkcd.com/538/>

VPN ①

34

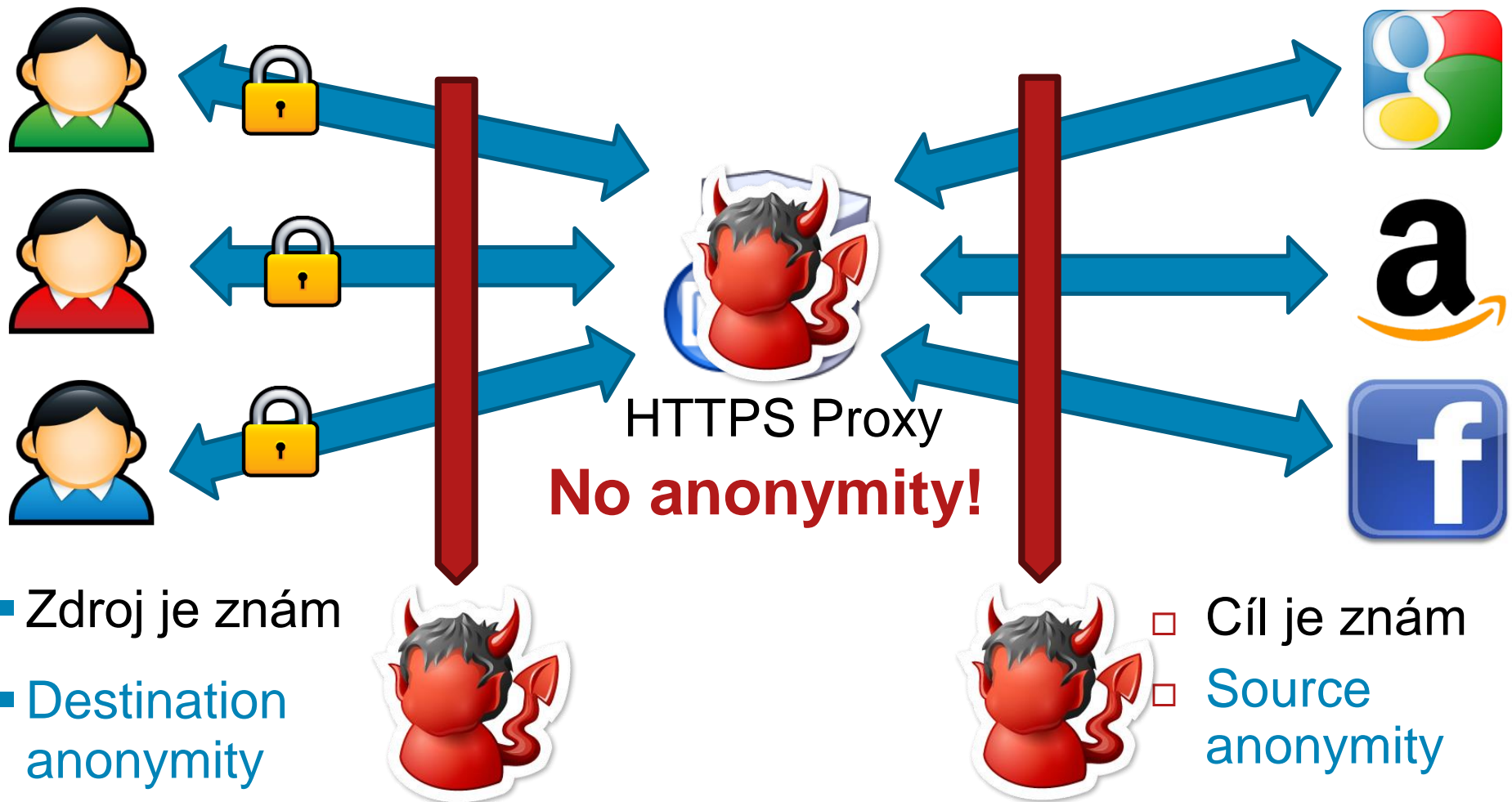


VPN ②

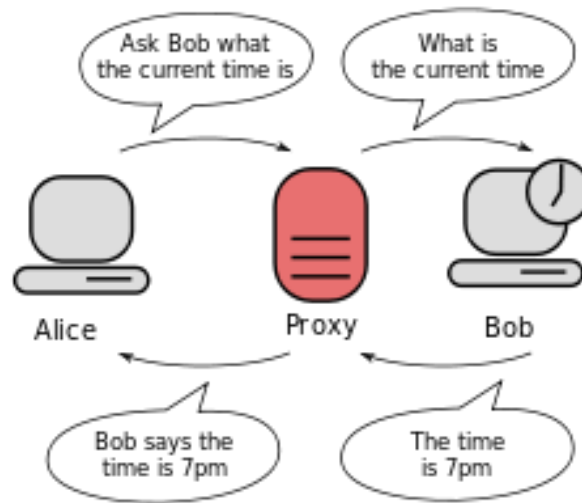


- ISP nevidí do komunikace
- Uživatel se hlásí vůči Internetu jako někdo jiný
 - „anonymizace“, unlocking Internet
- Poskytovatel VPN má informace kdo se připojil z jaké adresy
- Transparentní pro všechny aplikace
- Platba Bitcoin
- Celá řada poskytovatelů: ipredator, privateinternetaccess, torguard, btguard...

Proxy



Proxy



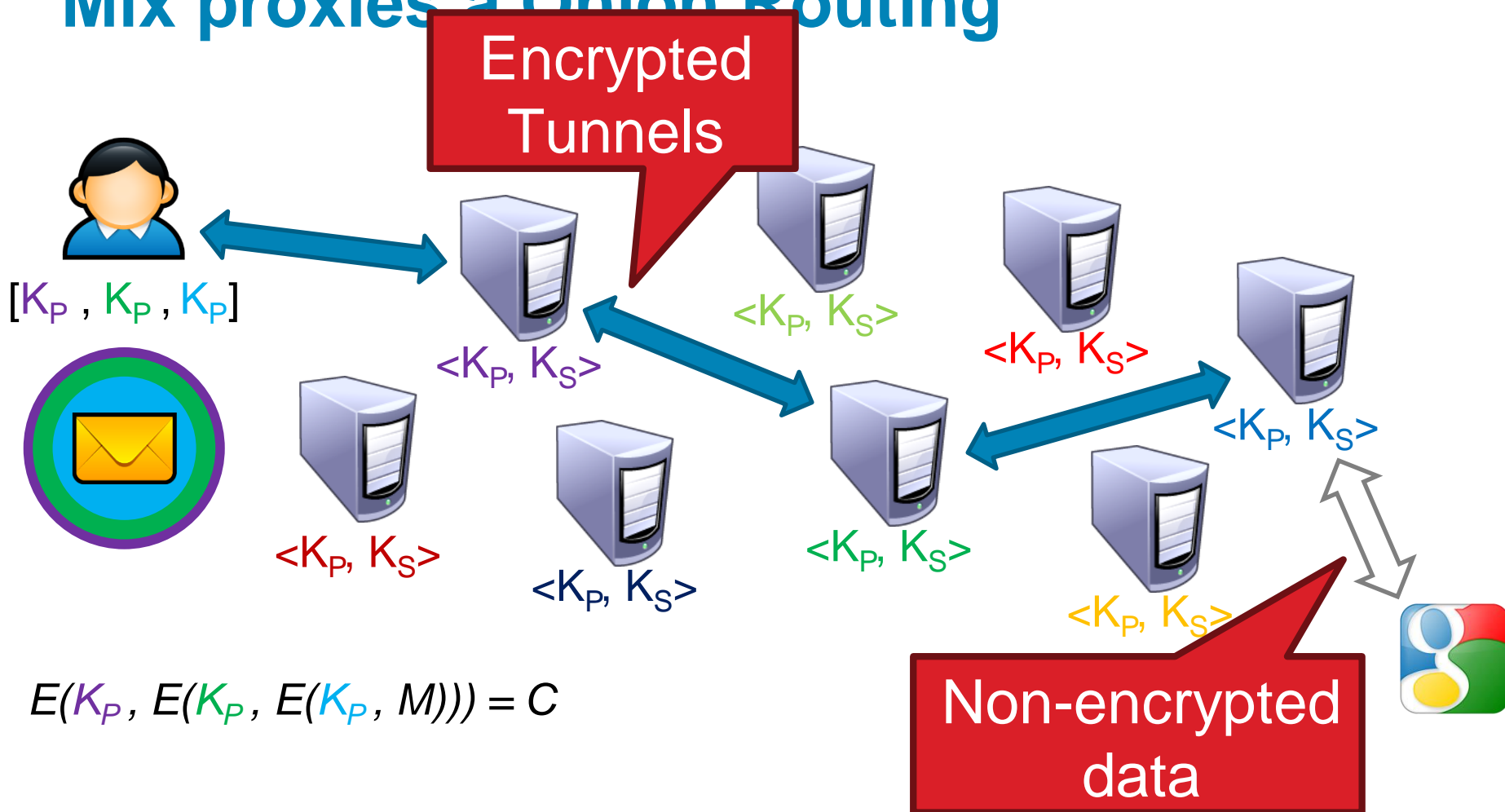
- Podobný princip jako VPN
- Provoz je veden skrz Proxy server
- HTTP, SOCK proxy



Mix networks, onion routing

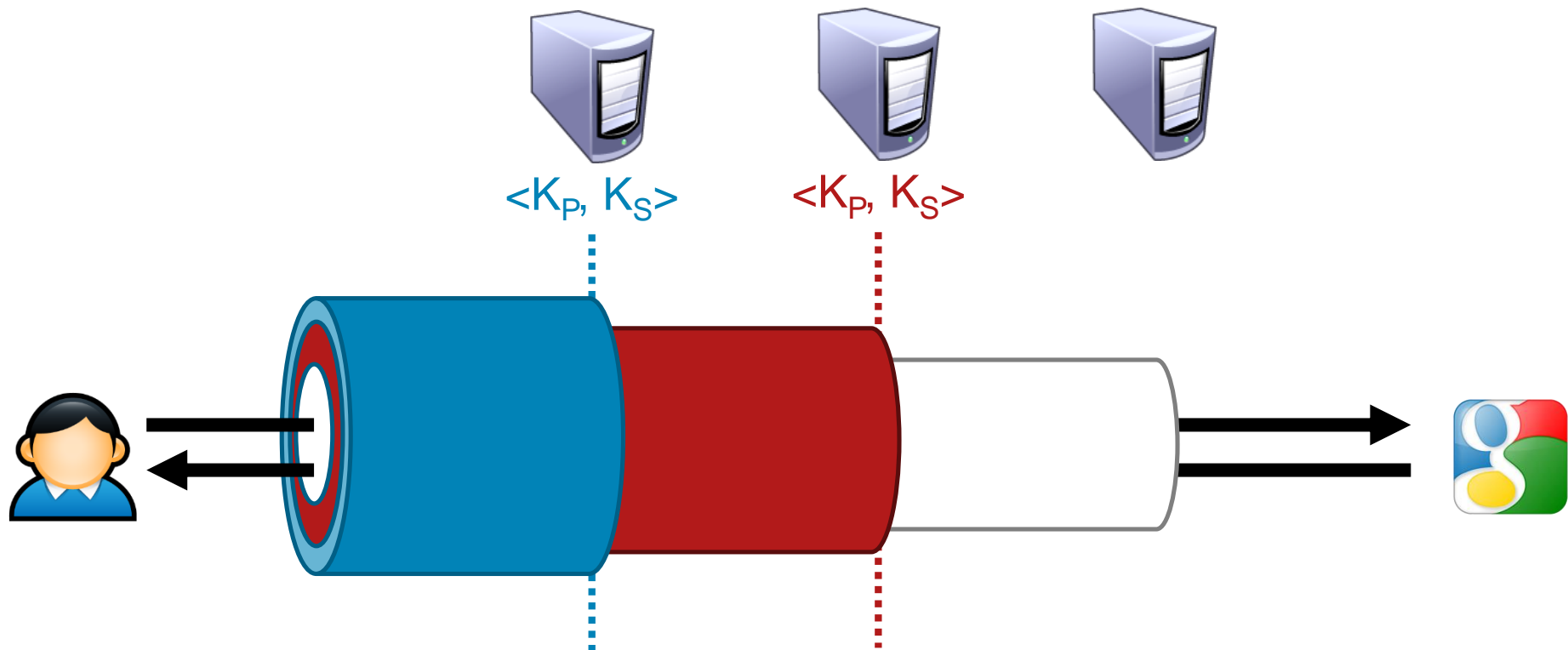
- Chaum, David L. "Untraceable electronic mail, return addresses, and digital pseudonyms." *Communications of the ACM* 24.2 (1981): 84-90.
- Inspirace pro:
 - Onion routing
 - Traffic mixing
 - Dummy traffic (cover traffic)

Mix proxies and Onion Routing



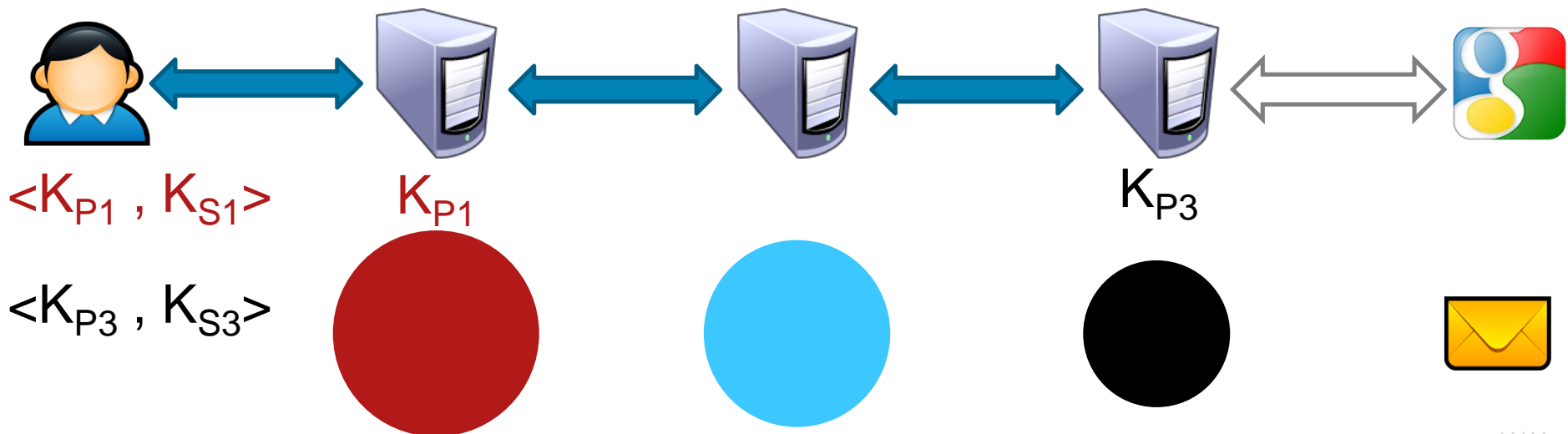
- Kaskáda anonymních proxy/serverů
- Všechn provoz je chráněn šifrováním

Jiný pohled



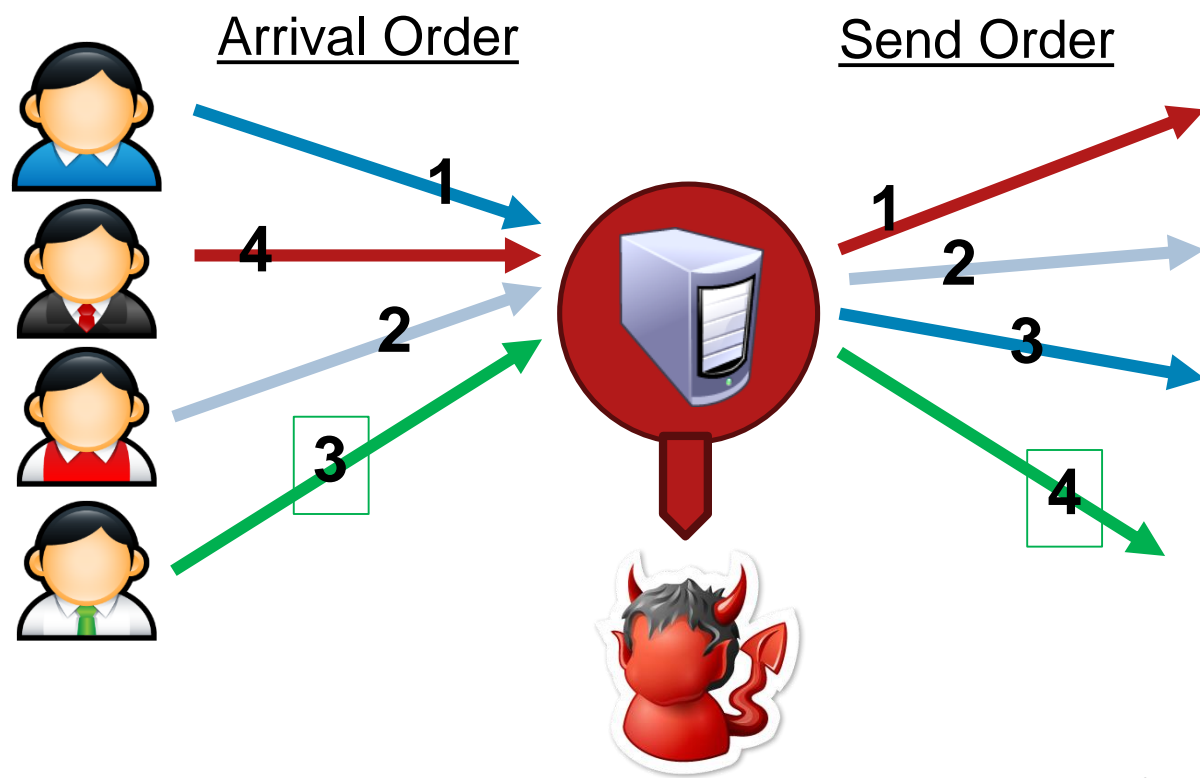
Return Traffic

- Jak se ustanoví cesta zpět?
- Odesílatel nechá klíče po cestě
 - Zpětné zašifrování dat



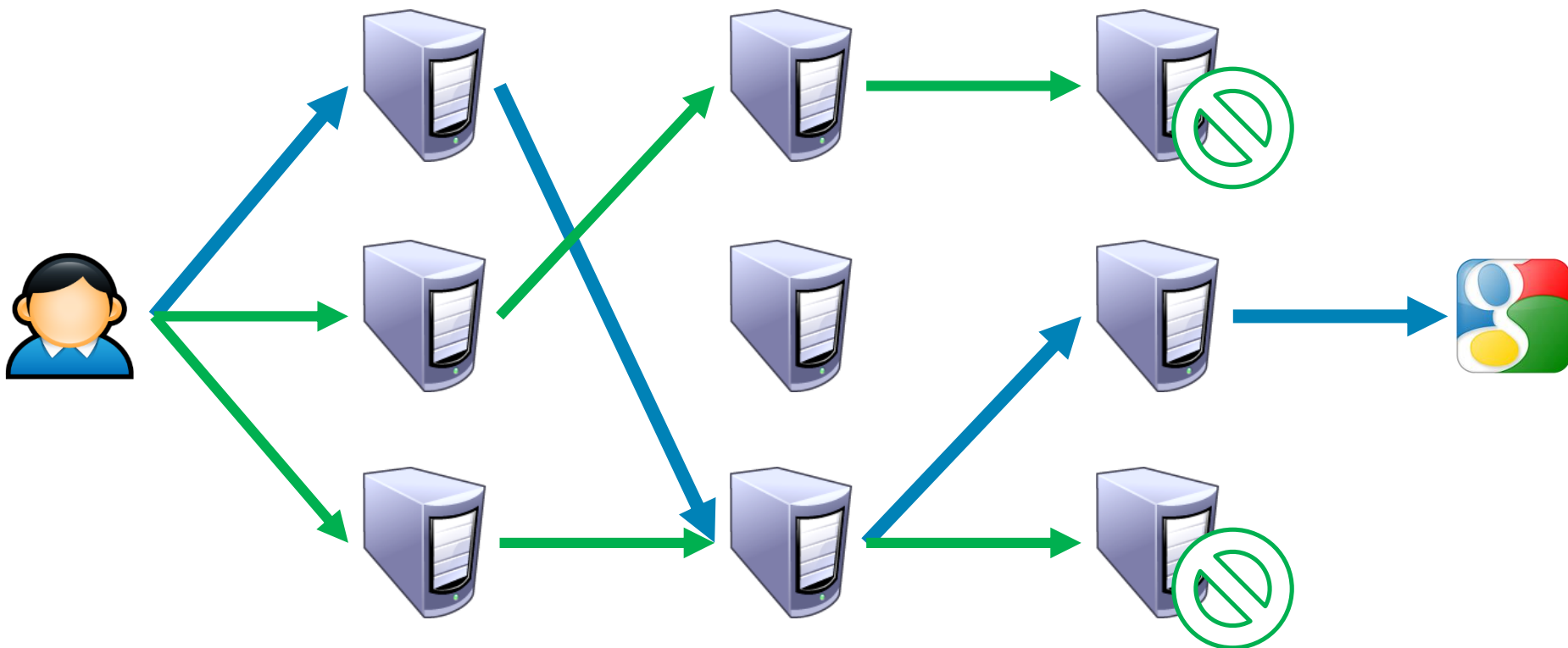
Traffic Mixing

- Ochrana proti timing attacks
 - Zprávy jsou náhodnou dobu pozdrženy
- Problémy:
 - Potřeba velkého množství provozu
 - Přidává zpoždění



Dummy / Cover Traffic

- Odesílání nesmyslného provozu
- Skrytí pomocí různého TTL
 - <http://www.fit.vutbr.cz/~ipolcak/pubs.php?id=10333>

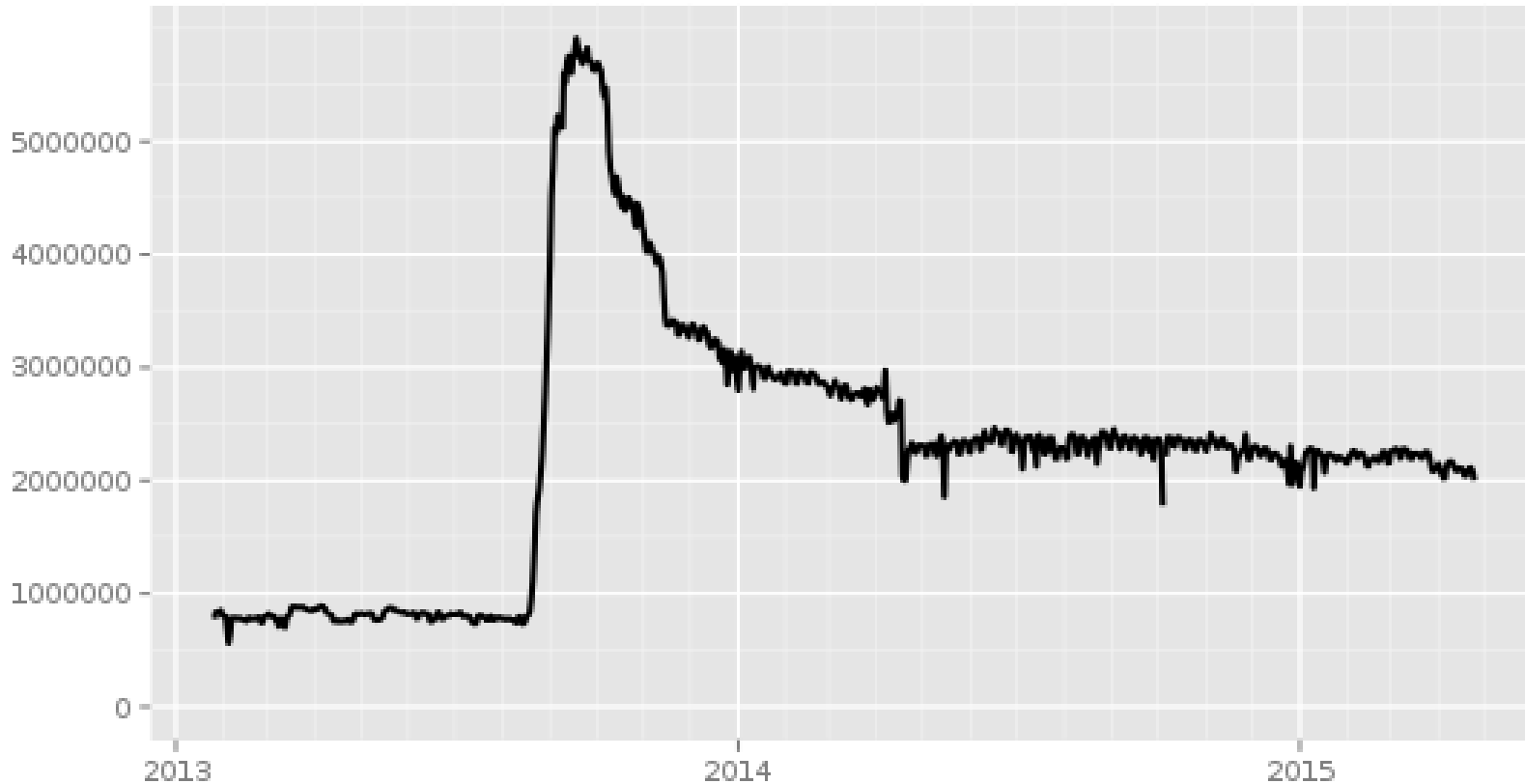


Torproject.org

- Vylepšená mix síť
 - **Guards**: zlepšení source anonymity
 - **Relays**: jiný název pro mix
 - **Hidden services**: servery dostupné pouze skrz Tor (darknet)
- Přibližně ~5000 Tor relays
 - Provozují dobrovolníci
 - Očekává se, že některé provozují „intelligence agencies“
- 1 – 2 mil. uživatelů
 - Nárůst po reportech E. Snowdena

Torproject.org

Directly connecting users

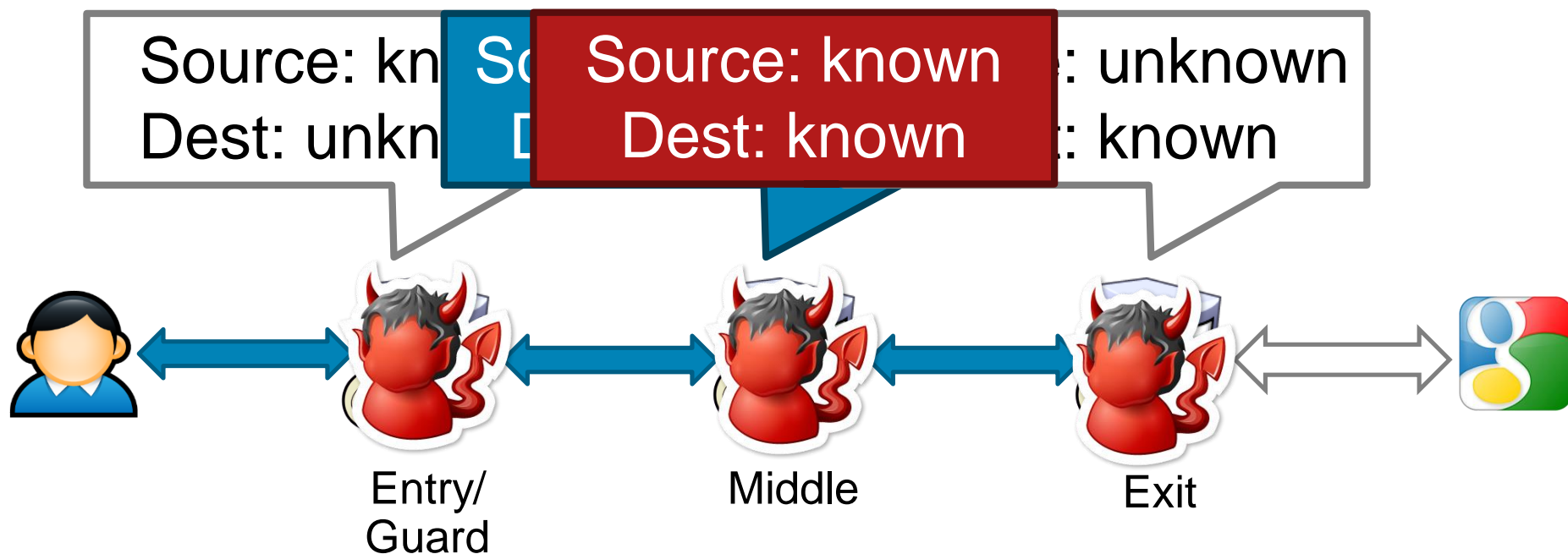


The Tor Project - <https://metrics.torproject.org/>

Torproject.org

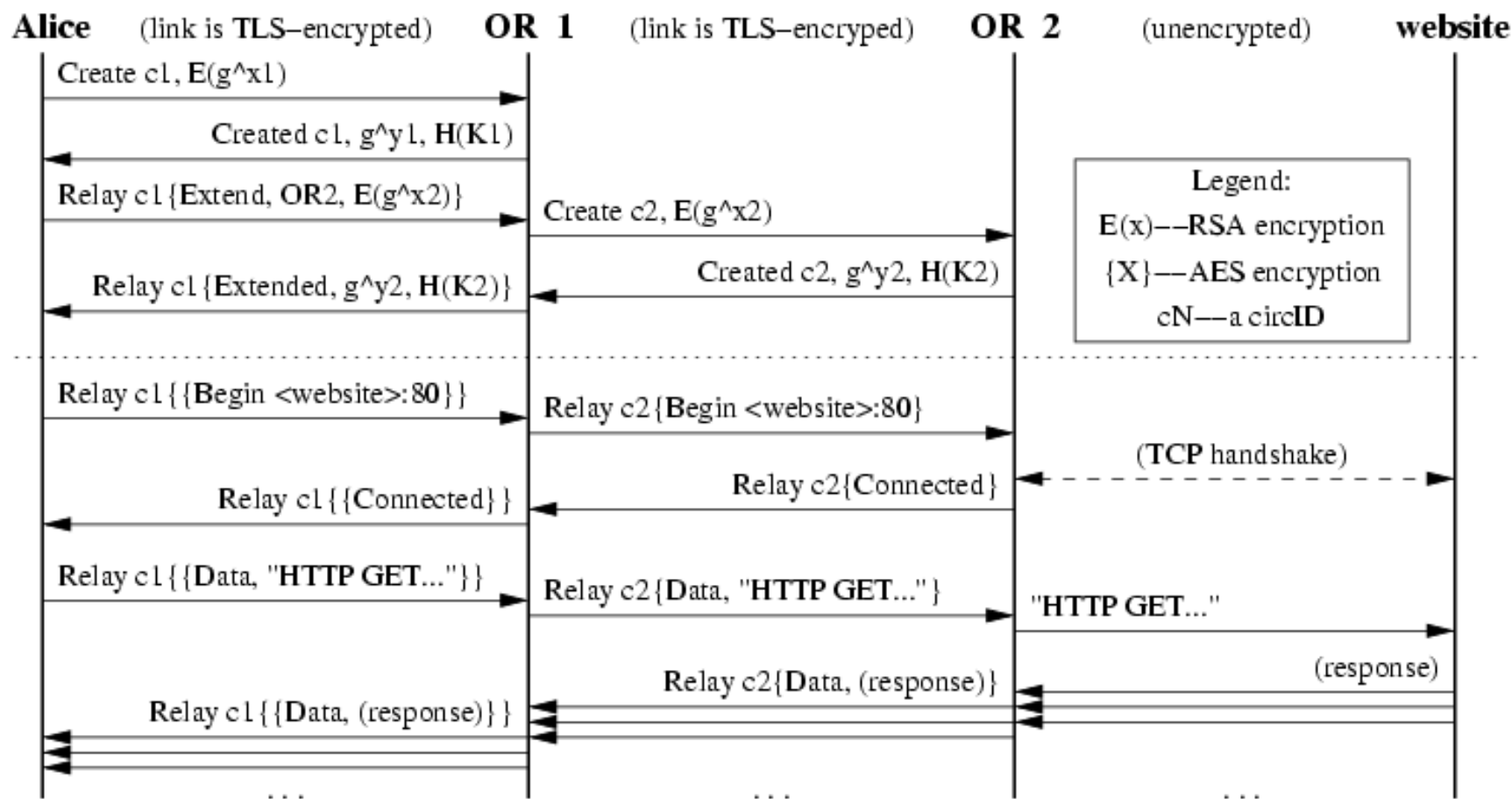
- Tor klient se chová jako SOCKS proxy
 - Vytváří a spravuje okruhy (**circuits**) mezi relays
- Může používat jakákoliv aplikace podporující spojení skrz SOCKS
- Jak se lokalizuje Tor relay?
 - Tor Consensus File
 - Hostován důvěryhodnými **directory** servery
 - Seznam všech známých relay
 - IP address, uptime, measured bandwidth, etc.
- Výběr relay není náhodný
 - Šance pro výběr je proporční šířce pásma
- Pakety rozdělené na buňky (cells) 512 bajtů
 - Snižuje efektivitu přenosu, zvyšuje anonymitu
- <https://gitweb.torproject.org/torspec.git/blob/HEAD:/tor-spec.txt>

Tor Circuits



- Počet relays lze zvolit
 - Implicitně 3

Příklad komunikace



Vstupní body: Guard Relays

- Guard relays pomáhají zabránit útočnickovi stát se vstupní relay
 - Tor vybere 3 guard relays a používá je cca 3 měsíce, pak vybere jiné
- Guard relay lze být pokud mám:
 - Dlouhý uptime
 - Velkou šířku pásma
 - Manuálně zvolen

Jsou vstupní body bezpečné?

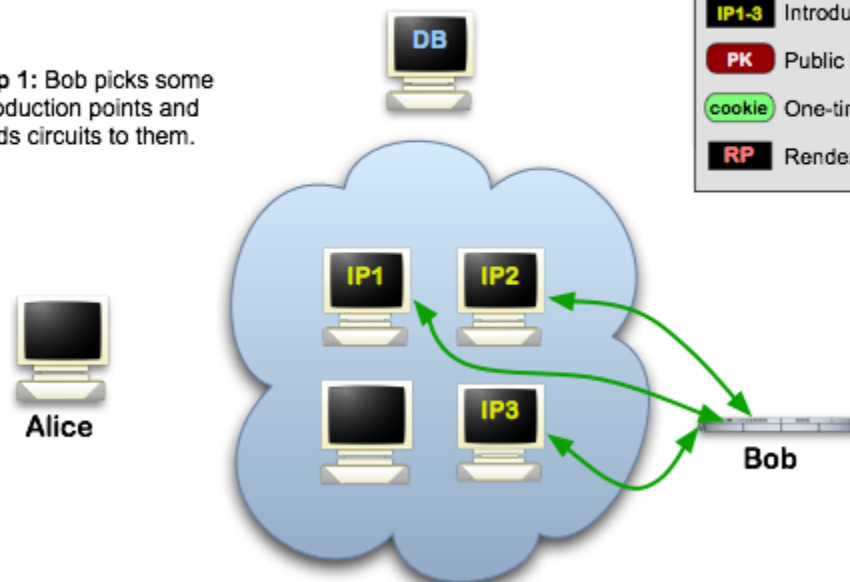
- Předpoklad:
 - N celkový počet relays
 - M počet relays kontrolovaný útočníkem
- Útočníkův cíl – kontrolovat první a poslední relay
 - M/N šance pro vstupní
 - $(M-1)/(N-1)$ šance pro poslední relay
 - $(M/N)^2$ celková šance pro jeden okruh
- Klient tvoří nové okruhy periodicky
 - Šance se zvyšují s časem

Hidden services

- Webové stránky jsou dostupné a snadno monitorovatelné
- Lze provozovat anonymní službu?
 - Např. web stránku u které není známá IP adresa?
- Tor Hidden Services
 - Umožňuje provozovat anonymní server bez odhalení jeho IP adresy nebo DNS jména
- Celá řada služeb
 - Tor Mail, Tor Char
 - DuckDuckGo
 - Wikileaks
 - The Pirate Bay, Silk Road a jeho varianty

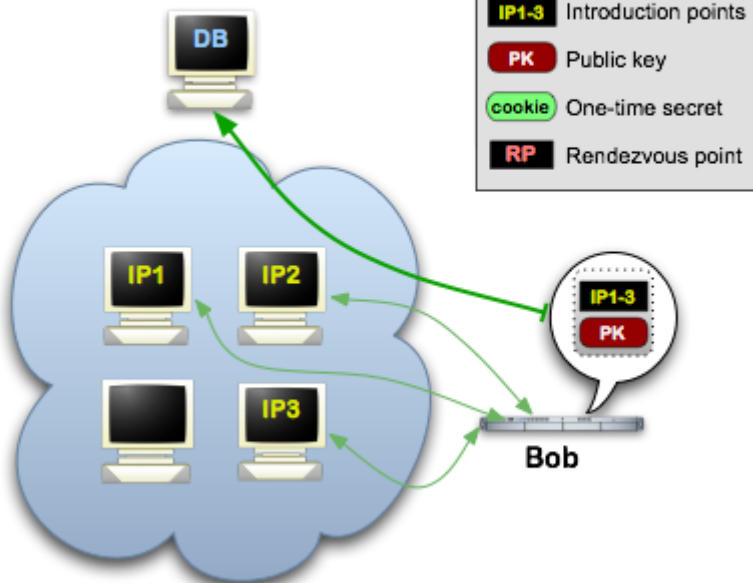
Hidden Services: 1

Step 1: Bob picks some introduction points and builds circuits to them.



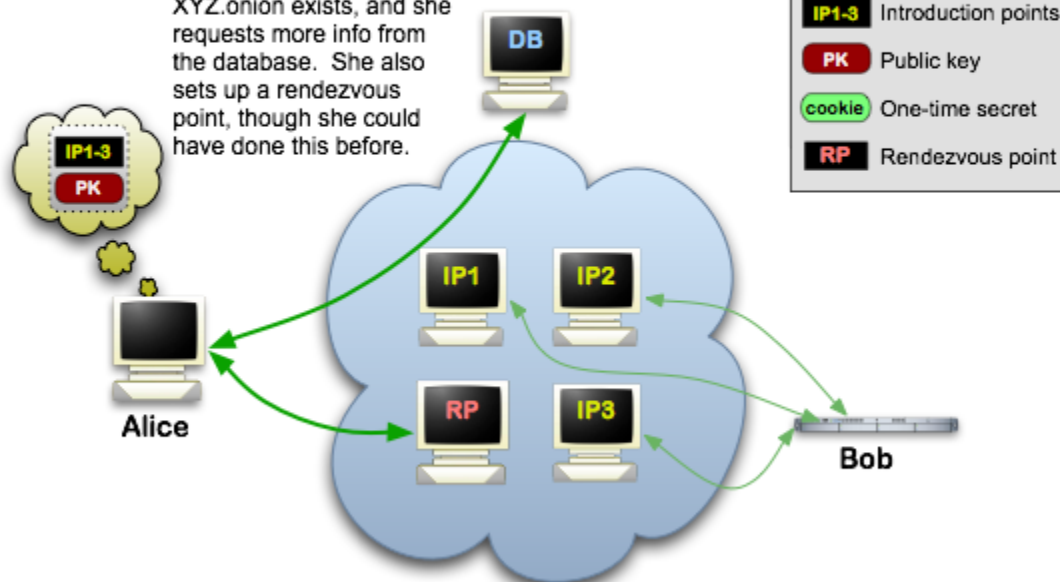
Tor Hidden Services: 2

Step 2: Bob advertises his hidden service -- XYZ.onion -- at the database.



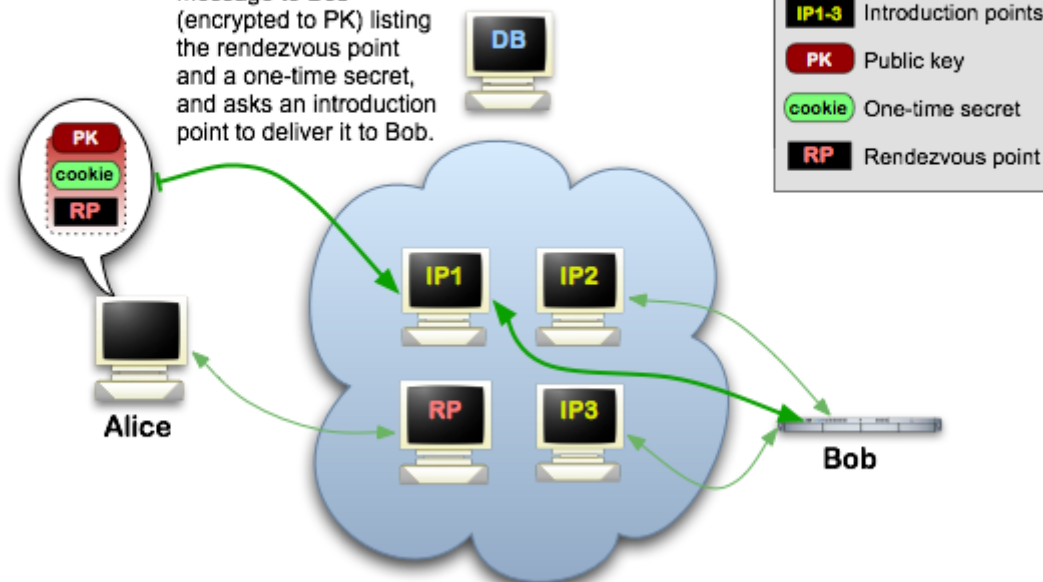
Tor Hidden Services: 3

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.



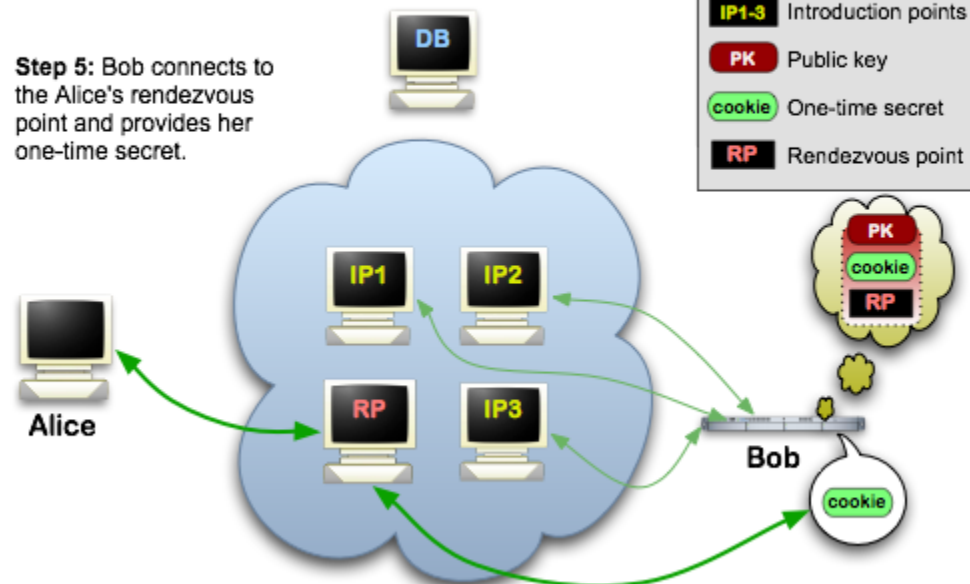
Tor Hidden Services: 4

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.



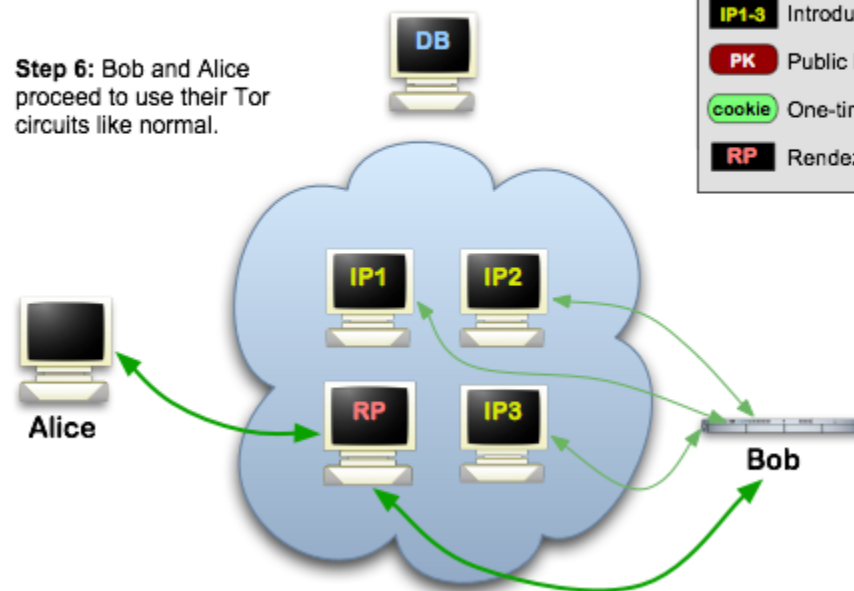
Tor Hidden Services: 5

Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.



Tor Hidden Services: 6

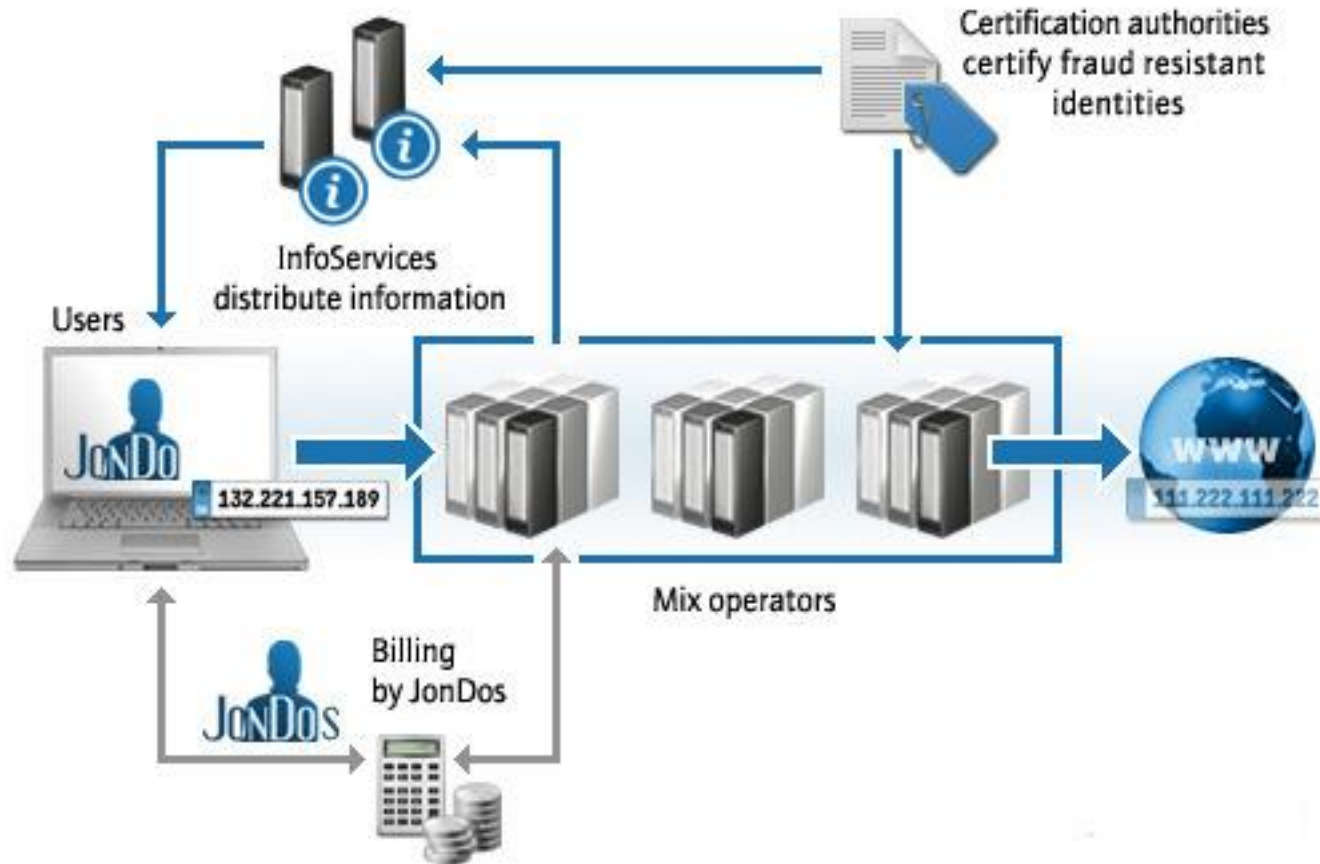
Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Tor Bridges

- Seznam Tor relays je volně dostupý
- Některé země mohou tyto IP blokovat
 - DoS vůči Tor
- Tor Bridges
 - Tor proxy, která není veřejně známa
 - Používaná pro připojení klientů v oblastech s velkou cenzurou
- Lze detekovat Tor pakety pomocí DPI (fixní buňky)
 - Zamlžení (obfuscating) provozu – provoz se tváří jako HTTP, Bittorrent ...

JohnDonym



Další zajímavé projekty

- Snapchat - sdílení obrázků, které se zničí po předem definované době
 - <http://ridgewood.patch.com/groups/police-and-fire/p/nude-photos-of-ridgewood-high-girls-prompt-police-investigation>
- Cjdns – P2P anonymní síť, postavená na IPv6
- Secret.ly – sociální síť, anonymní sdílení tajemství
- Telegram, Whisper, Wickr, Confide
- Reddit
- Vuvuzela
- freehaven.net/anonbib/