

# Lecture 24 – Anonymity and Privacy

Stephen Checkoway

University of Illinois at Chicago

CS 487 – Fall 2017

Slides based on Miller and Bailey's ECE 422

# a·non·y·mous

## Origin



late 16th century: via late Latin from Greek *anōnumos* 'nameless' (from *an-* 'without' + *onoma* 'name') + **-ous**.

# Anonymity

- Anonymity: Concealing your identity
- In the context of the Internet, we may want anonymous communications
  - Communications where the identity of the source and/or destination are concealed
- Not the same as secrecy/confidentiality
  - Confidentiality is about message contents,
    - (what was said)
- Anonymity is about identities
  - (who said it and to whom)

# Nymity Spectrum

- Verinymity
  - credit card #s, driver's license, address
- Pseudonymity
  - pen names, many blogs
- Linkable anonymity
  - loyalty cards, prepaid mobile phone
- Unlinkable anonymity
  - paying in cash, Tor

# Why do we need anonymity?

- Necessary to ensure civil liberties:
  - Free speech, free association, autonomy, freedom from censorship and constant surveillance
- Privacy is a human right
  - Dignity
  - Not explicit in US constitution, but relevant to 1st 4th 5th 9th amendments in bill of rights
- Surveillance is exploited for profit
  - Targeted marketing campaigns
  - Discrimination (insurance, employment)

# Arguments against Privacy?

- The "Nothing to Hide" Argument
  - Dangers of constructing a Kafkaesque world
  - Optional reading: 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy, Daniel J. Solove
  - Typically spoken from a view of privilege
- No one expects privacy anymore anyway
  - Kids today share their entire lives on Facebook
- Benefits from sharing (better search results?)
- Private communications abused by bad guys

# How to get Anonymity

- Internet anonymity is hard\*
  - Difficult if not impossible to achieve on your own
  - Right there in every packet is the source and destination IP address
  - \* But it's easy for bad guys. Why?
- How do we do it?
- State of the art technique: Ask someone else to send it for you
  - Ok, it's a bit more sophisticated than that...

# Proxies

- Proxy: Intermediary that relays our traffic
- Trusted 3rd party, e.g. ... [hidemyass.com](https://hidemyass.com)
  - You set up an encrypted VPN to their site
  - All of your traffic goes through them
- Why easy for bad guys? Compromised machines as proxies.



# Alice wants to send a message M to Bob ...

- Bob doesn't know M is from Alice, and
- Eve can't determine that Alice is indeed communicating with Bob.



- HMA accepts messages encrypted for it. Extracts destination and forwards.

# Anonymity motivation



Surveillance under:

- The Patriot Act
  - Section 215
  - National Security Letters (NSLs)
- FISA Amendment Act

# SURVEILLANCE UNDER THE PATRIOT ACT

## Hastily passed 45 days after 9/11 in the name of national security...

The Patriot Act was the first of many changes to surveillance laws that made it easier for the government to spy on ordinary Americans by expanding the authority to monitor phone and email communications, collect bank and credit

reporting records, and track the activity of innocent Americans on the Internet. While most Americans think it was created to catch terrorists, the Patriot Act actually turns regular citizens into suspects.

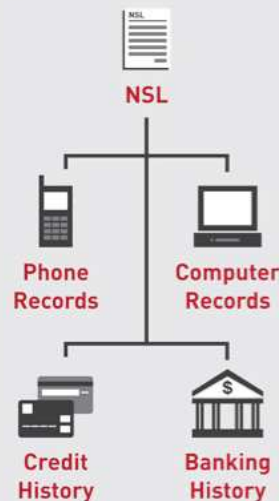
**National Security Letters (NSLs)** are issued by FBI agents, without a judge's approval, to obtain personal information...

*"I want to deliver a warning... when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."*

Senator Ron Wyden (D-OR),  
May 26, 2011

SOURCE: 1

**National Security Letters (NSLs)** are issued by FBI agents, without a judge's approval, to obtain personal information...



*"I want to deliver a warning... when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."*

Senator Ron Wyden (D-OR),  
May 26, 2011

SOURCE: 1



SOURCE: 2

The conviction would have occurred even without the Patriot Act.

SOURCE: 3

Image credit: ACLU

# Google Transparency Report

## National Security Letters (NSLs)

Reporting Period	National Security Letters	Users/Accounts
January to June 2016	0–499	500–999
July to December 2015	1–499	500–999
January to June 2015	0–499	500–999
July to December 2014	0–499	500–999
January to June 2014	500–999	500–999
July to December 2013	500–999	1000–1499
January to June 2013	0–499	500–999
July to December 2012	0–499	500–999
January to June 2012	500–999	1000–1499
July to December 2011	0–499	500–999
January to June 2011	0–499	500–999
July to December 2010	0–499	1000–1499
January to June 2010	500–999	1500–1999
July to December 2009	0–499	500–999
January to June 2009	0–499	500–999

# Metadata

- Everything except the contents of your communications:
  - If
  - When
  - How much
  - Who
- What (this is actually the data)

“... analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content.”

— Prof. Edward W. Felten, Computer Science and Public Affairs, Princeton;  
(former) Chief Technologist of FTC

# *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*

---

By CHARLIE SAVAGE and JONATHAN WEISMAN MAY 7, 2015




In a [97-page ruling](#), a three-judge panel for the United States Court of Appeals for the Second Circuit held that a provision of the U.S.A. [Patriot Act](#), known as Section 215, cannot be legitimately interpreted to allow the bulk collection of domestic calling records.

# XKEYSCORE

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

## What Can Be Stored?



- Anything you wish to extract
  - Choose your metadata
  - Customizable storage times
  - Ex: HTTP Parser

```
GET /search?hl=en&q=islamabad&meta= HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-
application/msword, application/x-shockwave-flash, */*
Referer: http://www.google.com.pk/
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: www.google.com.pk
```

Connection: keep-alive

TOP SECRET//COMINT//R

**No username/strong selector**

**"I, sitting at my desk, certainly had the authorities to wiretap anyone, from you or your accountant, to a federal judge or even the President, if I had a personal e-mail,"**



# Technology as a defense





“Whether we are surveilled by our government, by criminals, or by our neighbors, it is fair to say that never has our ability to shield our affairs from prying eyes been at such a low ebb. The availability and use of secure encryption may offer an opportunity to reclaim some portion of the privacy we have lost.”

— 9th Circuit court opinion, Bernstein v US DOJ 1999

“Crypto wars”

# Encryption Tools: PGP

- GnuPG, free software
  - Pretty Good Privacy (PGP), Phil Zimmerman (1991)
  - GnuPG (GPG) is a free software recreation
  - Lets you hide email content via encryption
- Basic idea:
  - Hybrid encryption to conceal messages
  - Digital signatures on messages (hash-then-sign)

## PGP cont'd

- Each user has:
  - A public encryption key, paired with a private decryption key
  - A private signature key, paired with a public verification key
- How does sending/receiving work?
- How do you find out someone's public key?

# Sending and receiving

- To send a message:
  - Sign with your signature key
  - Encrypt message and signature with recipient's public encryption key
- To receive a message:
  - Decrypt with your private key to get message and signature
  - Use sender's public verification key to check sig

Secret location (2)

Get Messages

Write

Chat

Address Book

Tag

Decrypt

Reply

Reply All

Forward

Archive

Junk

Delete

More

From Me <jrandomhacker@example.org> ★

Subject Secret location (2)

To Me <ludwig@enigmail.net> ★

Bcc Me <ludwig@hammernoch.net> ★

Enigmail

Decrypted message; UNTRUSTED Good signature from John Random Hacker <jrandom  
Key ID: 0x41BD7F8B / Signed on: 12.02.15 04:56

Details

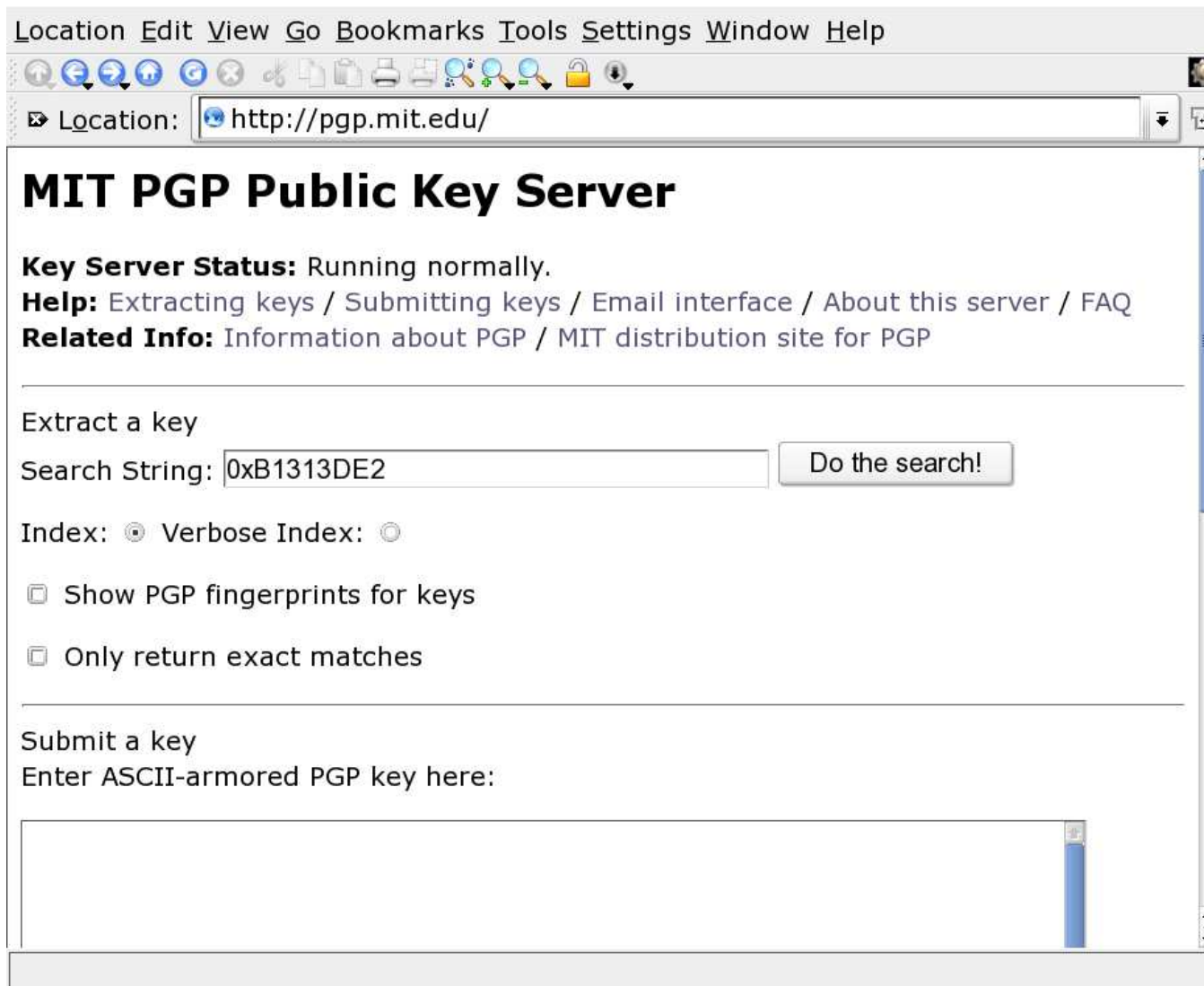
Skeleton Island E.S.E. and by E.  
Ten feet.

—  
John

1 message downloaded

# Fingerprints

- How do you obtain Bob's public key?
  - Get it from Bob's website? ( ☹ )
  - Get it from Bob's website, verify using out-of-band communication
    - Keys are unwieldy → fingerprints
    - A fingerprint is a cryptographic hash of a key
  - Key servers: store public keys, look up by name/email address, verify with fingerprint
- What if you don't personally know Bob?
  - Web of Trust (WoT), “friend of a friend”
  - Bob introduces Alice to Caro by signing Alice's key

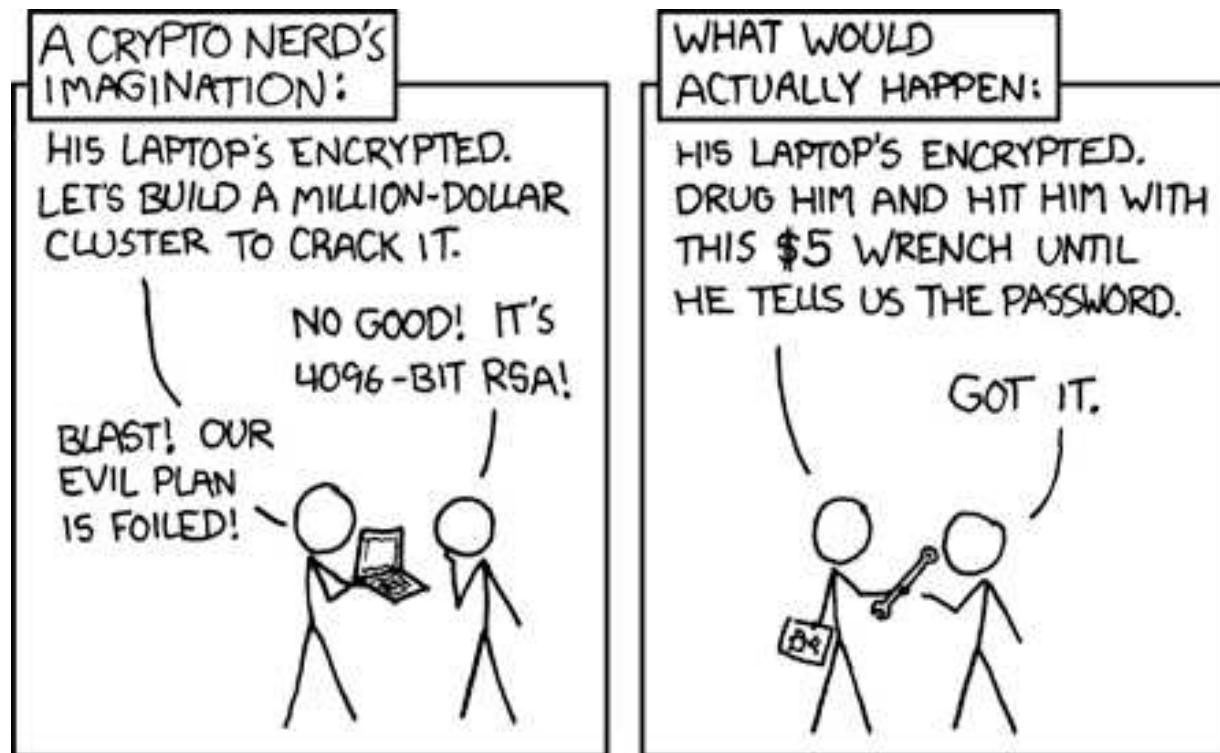


# Drawbacks of (Just) Encryption I

- What if Bob's machine compromised?
  - His key material becomes known
  - Past messages can be decrypted and read
  - You also have sender's signature on messages sent, so you can prove identity of sender
- The software created lots of incriminating records
  - Key material that decrypts data sent over the public Internet
  - Signatures with proofs of who said what
- Alice better watch what she says
  - Her privacy depends on Bob's actions



## Drawbacks of (Just) Encryption II



# Casual Conversations

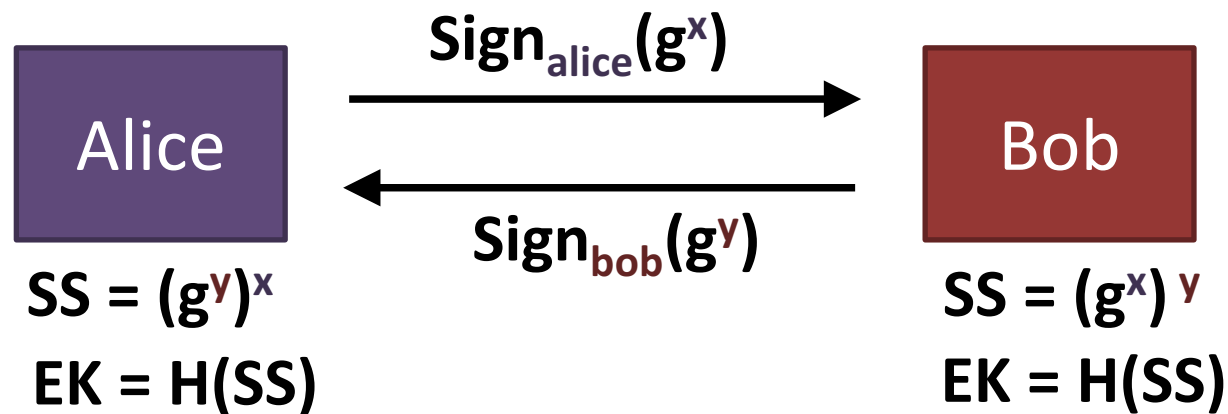
- Alice and Bob talk in a room
- No one else can hear
  - Unless being recorded
- No one else knows what they say
  - Unless Alice or Bob tell them
- No one can prove what was said
  - Not even Alice or Bob
- These conversations are “off-the-record”

# Desirable communication properties

- Forward secrecy:
  - Even if your key material is compromised, past messages should be safe
- Deniability: be able to plausibly deny having sent a message
- Mimic casual, off-the-record conversations
  - Deniable authentication: be confident of who you are talking to, but unable to prove to a third party what was said

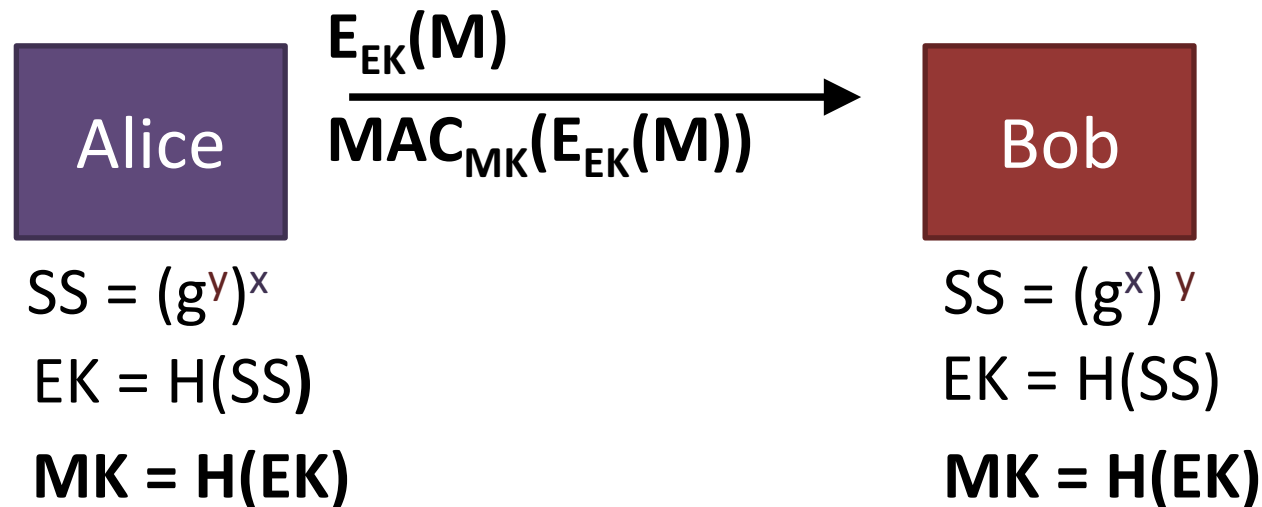
# Off-the-Record (OTR) Messaging

1. Use Authenticated Diffie-Hellman to establish a (short-lived) session key EK



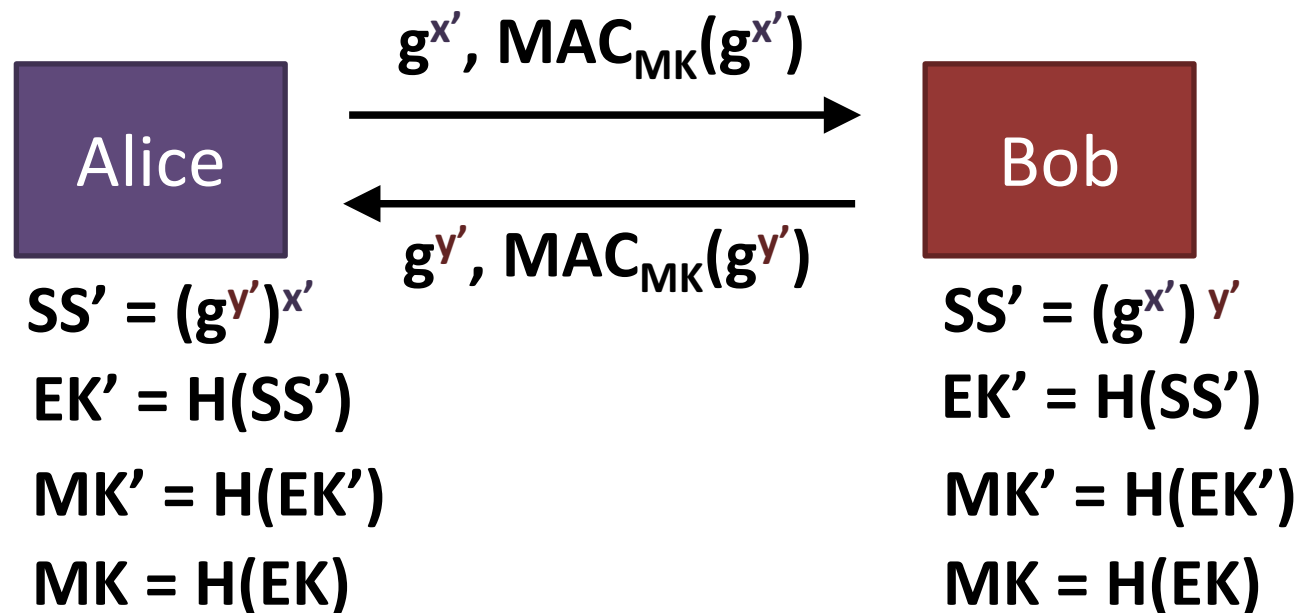
## OTR II

2. Then use secret-key encryption on message M  
... And authenticate using a MAC



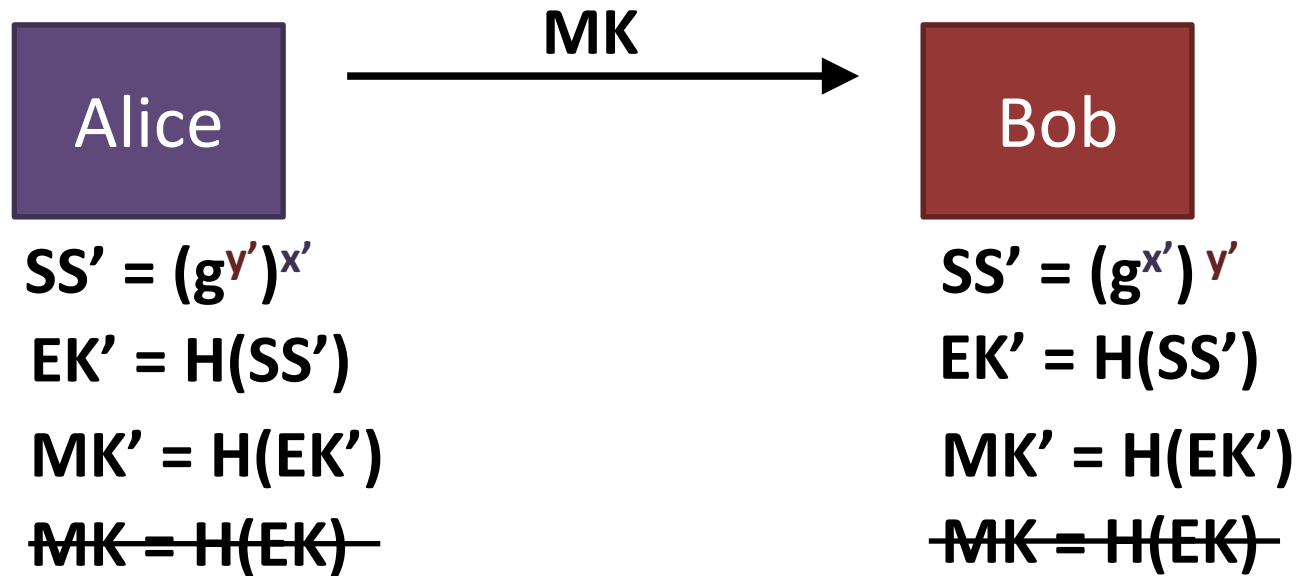
# Off-the-Record

## 3. Re-key using Diffie-Hellman



# Off-the-Record

## 4. Publish old MK



# Off-the-record Messaging (OTR)

- Note this is suited to interactive communication, not so much email
- But, OTR provides
  - message confidentiality
  - authentication
  - perfect forward secrecy
  - deniability
    - Caveat: we do not have examples of “deniability” serving its purpose in practice



# Using OTR

- Built in to Adium and Pidgin
- But beware defaults
  - Logging enabled by default
  - Etiquette dictates you should disable this, so does history (e.g., Chelsea Manning)
- Very different from Google Hangout's "off the record" feature which merely doesn't log the conversation

# Signal and the “Double Ratchet”

*The protocol behind Signal app (iphone, android)*

*Trevor Perin and Moxie Marlinspike*

- **Forward secrecy**

Today's messages are secret, even if key compromised tomorrow

- **Future secrecy**

Tomorrow's messages are secret, even if key compromised today

- **Deniability**

No permanent/transferable evidence of what was said

- **Usability**      Tolerates out-of-order message delivery

<https://whispersystems.org/docs/specifications/doublerratchet/>



# Plausibly Deniable Storage

Goal: Encrypt data stored on your hard drive

Problem: Can be compelled to decrypt it!

Idea: have a “decoy” volume with benign information on it

Example: VeraCrypt

[Does this solve the problem? Caveats?]

# Recap Privacy/Anonymity

- Metadata: Everything except the contents of your communications:

- If
- When
- How much
- Who

- What (this is actually the data)



Signal and OTR

# Anonymity for browsing?

You

Server

## Naive approach .... VPNs



# VPNs



## Lulzsec fiasco

Posted on [September 23, 2011](#)

We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group 'lulzsec'. Lulzsec have been ALLEGEDLY been responsible for a number of high profile cases such as:

- The hacking of the Sony Playstation network which compromised the names, passwords, e-mail addresses, home addresses and dates of birth of thousands of people.
- The DDOS attack which knocked the British governments SOCA (Serious Organised Crime Agency) and other government websites offline.
- The release of various sensitive and confidential information from companies such as AT&T, Viacom, Disney, EMI, NBC Universal, and AOL.
- Gaining access to NATO servers and releasing documents regarding the communication and information services (CIS) in Kosovo.
- The defacement of British newspaper websites The Sun & The Times.
- The hacking of 77 law enforcement sheriff websites.

# VPNs



## Lulzsec fiasco

Posted on September 22, 2014

We have received concerns by users that our VPN service was utilized by a member or members of the hacktivist group Lulzsec. Lulzsec have been ALLEGEDLY been responsible for a number of high profile users such as:

- The hacking of home addresses
- The OGCIS and other government
- The release of Disney CEO's
- Gaining access to services (CIS)
- The defacement
- The hacking of

“...received a **court order** asking for information relating to an account associated with some or all of the above cases. As stated in our terms of service and **privacy policy** our service is not to be used for illegal activity, and as a legitimate company ***we will cooperate with law enforcement if we receive a court order***”



## Better approach: Tor

- Low-latency anonymous communication system
- Hide metadata
  - who is communicating with whom?
  - e.g., just sending an encrypted message to The Intercept may get you in trouble
- Hide existence of communication
  - any encrypted message may get you in trouble

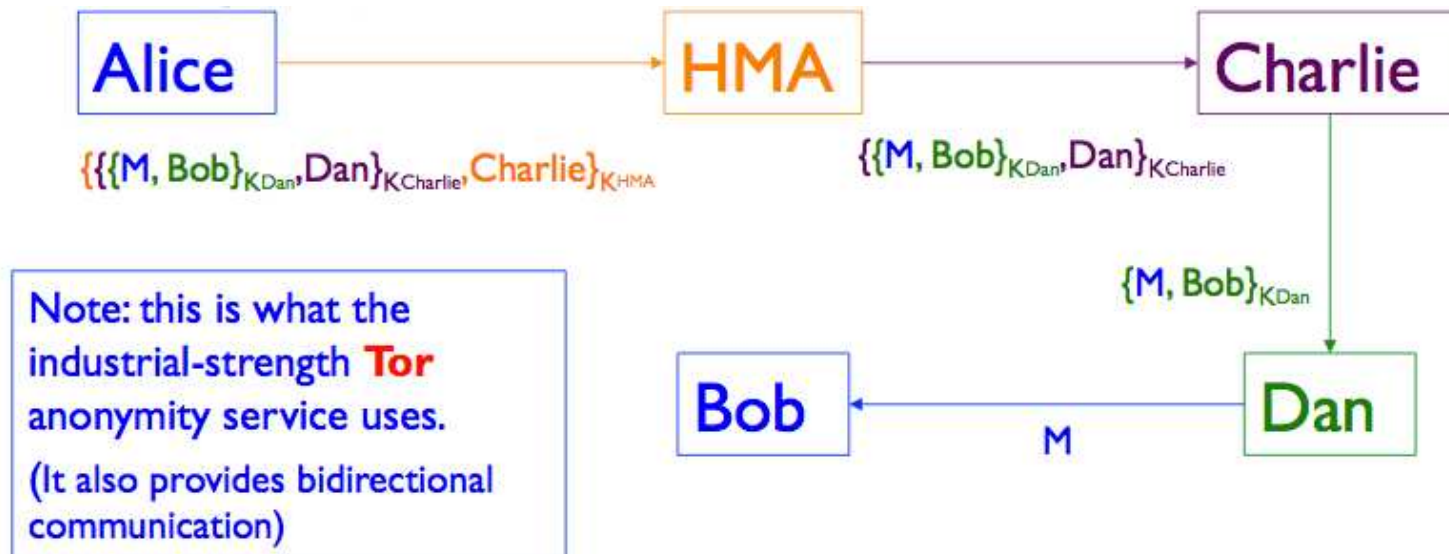
# Tor overview

- Works at the transport layer
- Allows you to make TCP connections without revealing your IP address
- Popular for web connections
- Tor network made up of volunteer-run nodes, or onion routers, located all over the world
- Basic idea: Alice wants to connect to a web server without revealing her IP address

# Onion Routing

- This approach generalizes to an arbitrary number of intermediaries (“mixes”)
- Alice ultimately wants to talk to Bob, with the help of HMA, Dan, and Charlie
- As long as any of the mixes is honest, no one can link Alice with Bob

# Onion Routing



**Key concept: No one relay knows both you and the destination!**

# Tor

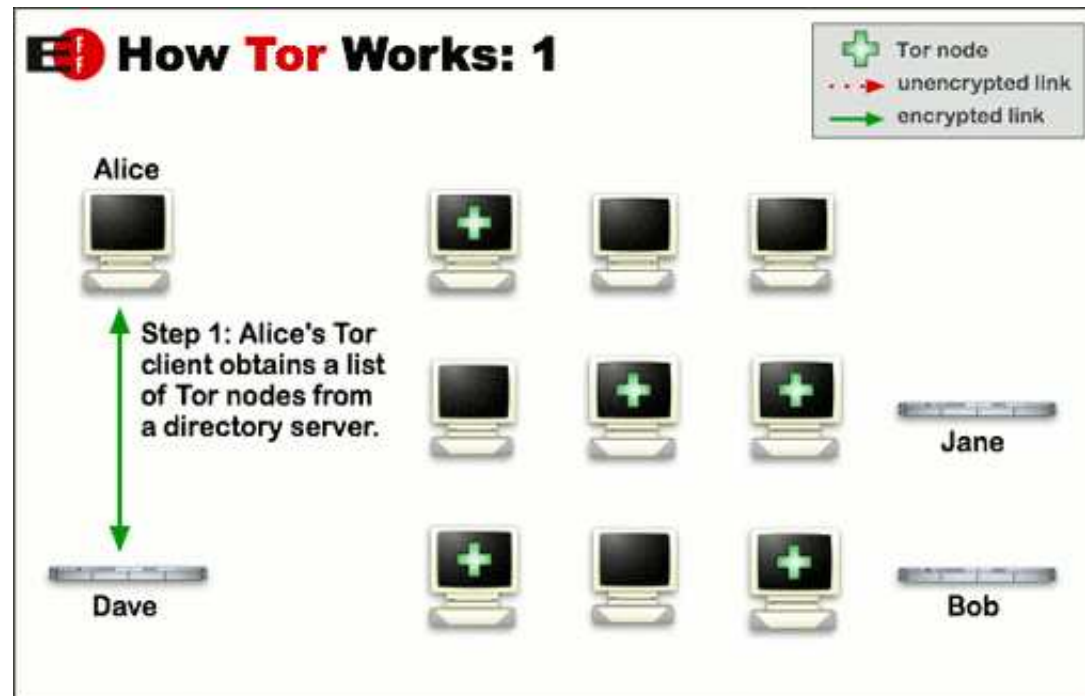


Image credit:  
Tor Project

# Tor

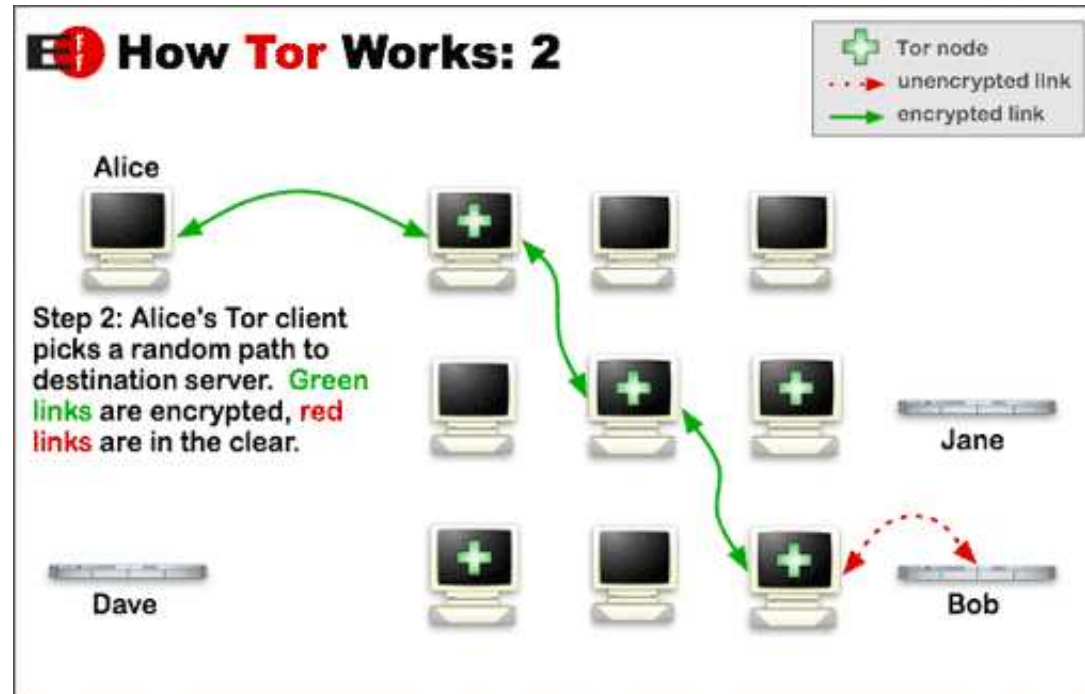


Image credit:  
Tor Project

# Tor

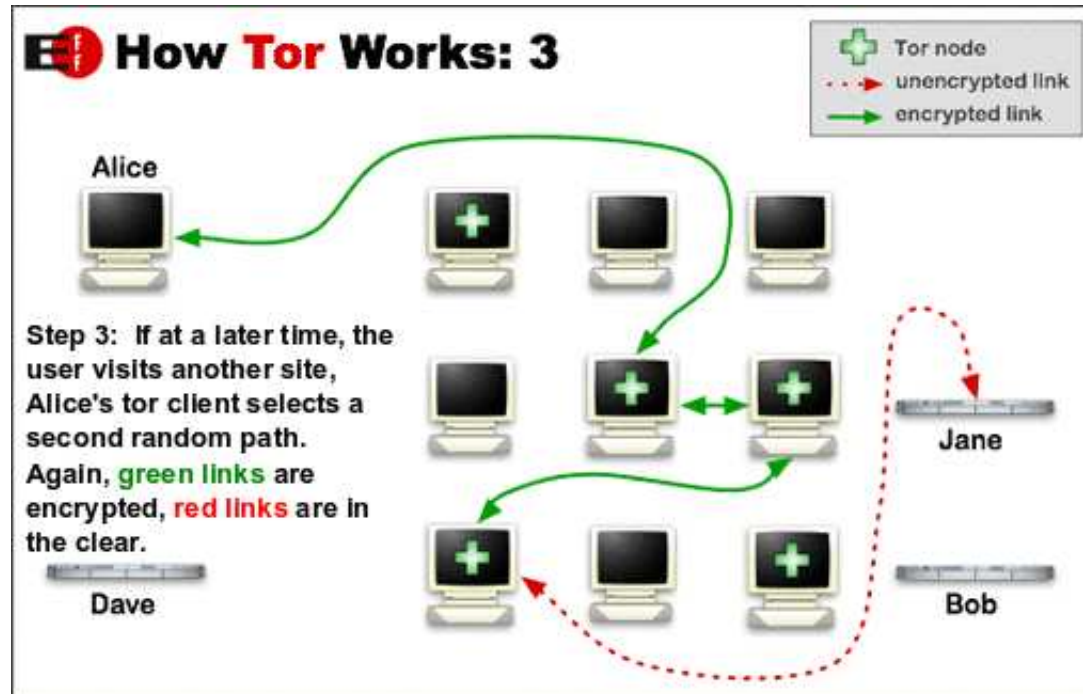


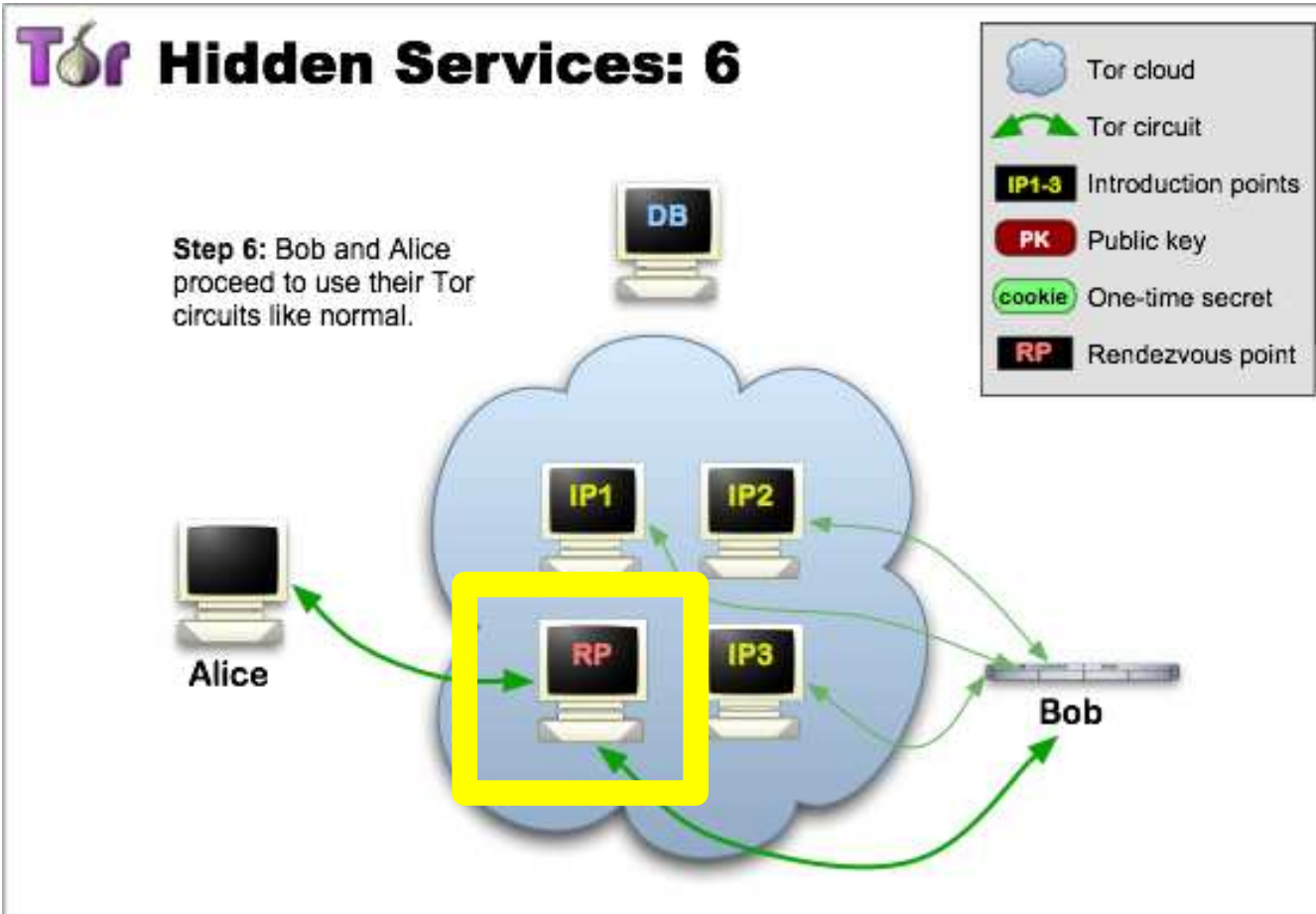
Image credit:  
Tor Project

# Trust in Tor

- Entry node: knows Alice is using Tor, and identity of middle node, but not destination
- Exit node: knows some Tor user is connecting to destination, but doesn't know which user
- Destination: knows a Tor user is connecting to it via the exit node
- Important to note that Tor does not provide encryption between exit and destination! (e.g., use HTTPS)



# Tor Hidden Services



# How to get Tor

- Tor Browser bundle available (built on modified version of firefox)
- ☺ optional exercise: download and use it!
- <https://www.torproject.org/>
- ...or volunteer to be a part of the Tor network.

# Onion Routing Issues/Attacks?

- Performance: message bounces around a lot
- Attack: rubber-hose cryptanalysis of mix operators
  - Defense: use mix servers in different countries
- Attack: adversary operates all of the mixes
  - Defense: have lots of mix servers (Tor today: ~6,500) <https://metrics.torproject.org/networksize.html>
- Attack: adversary observes when Alice sends and when Bob receives, links the two together
- A side channel attack – exploits timing information
  - Defenses: pad messages, introduce significant delays
    - Tor does the former, but notes that it's not enough for defense

## Onion Routing Issues, cont.

- Issue: traffic leakage
- Suppose all of your HTTP/HTTPS traffic goes through Tor, but the rest of your traffic doesn't
- How might the operator of sensitive.com
- deanonymize your web session to their server?

# The traffic leakage problem

- Answer: they inspect the logs of their DNS server to see who looked up sensitive.com just before your connection to their web server arrived
- Hard, general problem: anonymity often at risk when adversary can correlate separate sources of information

HACKING

# Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds



JOSEPH COX

Feb 24 2016, 8:05am

**Update 25 Feb:** *In a statement, the Tor Project told Motherboard that "the Tor network is secure and has only rarely been compromised. The Software Engineering Institute ("SEI") of Carnegie Mellon University (CMU) compromised the network in early 2014 by operating relays and tampering with user traffic. That vulnerability, like all other vulnerabilities, was patched as soon as we learned about it. The Tor network remains the best way for users to protect their privacy and security when communicating online."*

# Metadata


- If
- When
- How much
- Who
- What

# Metadata

- If
- When
- How much
- Who
- What      ← TLS/PGP/OTR/Signal



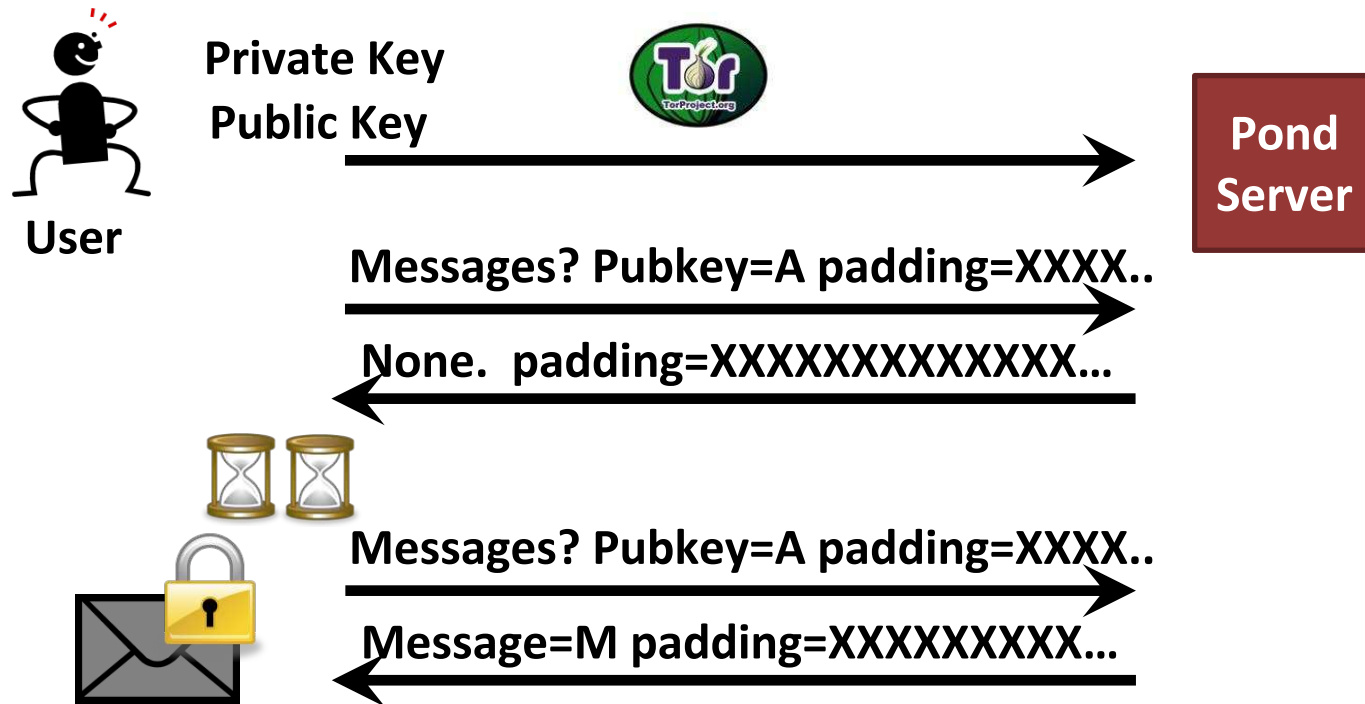
# Metadata

- If
- When
- How much
- Who      ← 
- What      ← TLS/PGP/OTR/Signal

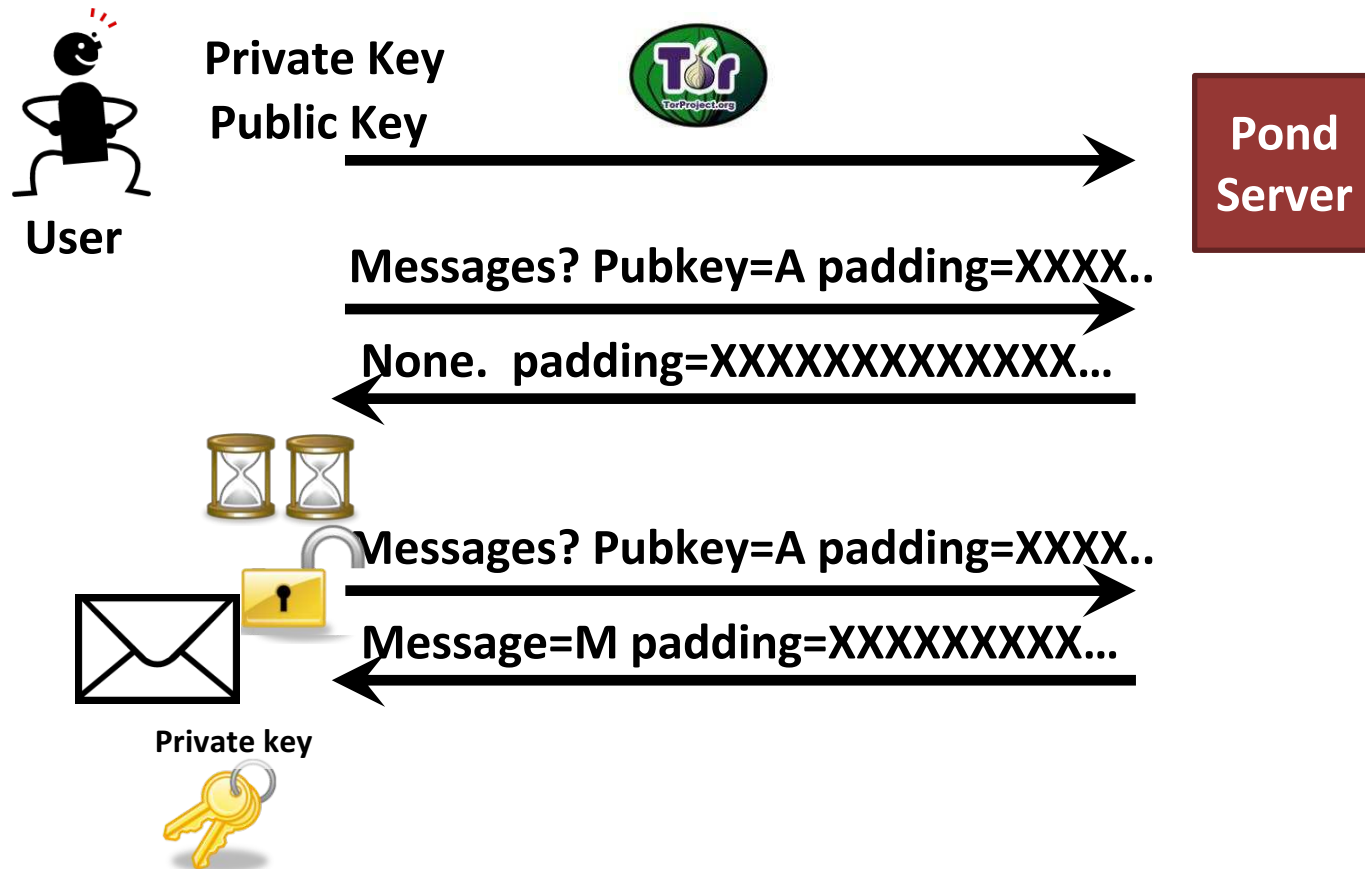
# Pond

- "Pond is not email. Pond is a forward secure, asynchronous messaging system for the discerning"
- Seeks to protect against leaking traffic info against all but a global passive adversary
  - forward secure
  - no spam
  - messages expire automatically after a week




# Pond



# Pond



# Metadata summary

- If
- When ←  Pond
- How much ← 
- Who ←  TorProject.org
- What ← TLS/PGP