CS 203

Privacy & Anonymity

Privacy

•*(Image from geekologie.com)*

- Privacy and society
  - Basic individual right & desire
  - Relevant to corporations & government agencies
  - Increasing public awareness
    - However, public's perception of privacy is both nebulous and fickle
    - Social networking promotes voyeurism and exhibitionism

- Privacy and technology in recent 20+ years
  - >> Information disclosed on the Internet
  - >> Handling and transfer of sensitive information
  - << Privacy and accountability

Privacy on Public Networks

- Internet is designed as a public network
  - Machines on a (wired ot wireless) LAN can see all traffic, network routers see all traffic that passes through them
- Routing information is public
  - IP packet headers identify source and destination
  - Even a passive observer can easily figure out who is talking to whom
- Encryption (e.g., TLS or IPSec) does not hide identities
  - Encryption hides payload, not routing information
  - Even IP-level encryption (tunnel-mode IPsec/ESP) reveals IP addresses of IPsec gateways

Applications of Anonymity (1)

- Privacy
  - Hide online transactions, Web browsing, etc. from intrusive governments, marketers, archival/search entities (e.g., Google) as well as from criminals and snoops.
- Untraceable electronic mail
  - Corporate/government whistle-blowers
  - Political dissidents in oppressive societies
  - Socially sensitive communications (online AA or STD meeting)
  - Confidential business negotiations
- Law enforcement and intelligence
  - Sting operations and honeypots
  - Secret communications on a public network
    - Informers, secret agents, etc.

Applications of Anonymity (2)

- Digital cash & anonymous payments
  - Electronic currency with properties of paper money (online purchases unlinkable to buyer's identity)
- Anonymous electronic voting
- Censorship-resistant publishing

Nefarious Applications of Anonymity

- The usual: porn, pedophilia, libel, etc.
- Dis-/mis-information (fake news) / propaganda
- Sale of illegal substances, weapons and actions, e.g., SilkRoad
- Tax avoidance (via untraceable payments) and various cryptocurrency tricks
- Incitement to criminal activity (e.g., murder, rioting, genocide, terrorism)

What is Anonymity?

- Anonymity: inability to identify someone within a set of subjects (size varies)
  - Different from PRIVACY (right to be left alone)
  - Hide your activities among similar activities by others
  - One cannot be anonymous alone!
    - Big difference between anonymity and confidentiality
- Unlinkability: inability to connect (1) multiple actions or (2) action and identity
  - For example, connecting sender (Alice) to a sent email. Or, connecting two emails to the same (even unknown) sender
- Unobservability: (very hard to achieve)
  - Observer cannot tell whether a certain action took place, e.g.
    - Did someone do a DNS query of: sprout.ics.uci.edu
    - Did someone send a packet to Bob

Attacks on Anonymity

- Passive traffic analysis
  - Infer from network traffic who is talking to whom
  - To hide your own traffic, must carry other people's traffic!
- Active traffic analysis
  - Inject packets or put a timing signature on packet flow
- Compromise of network nodes (routers)
  - Not obvious which nodes have been compromised
    - Attacker may be passively logging traffic
  - It's better not to trust any individual node
    - Assume that most nodes are bad, and a few are good, without knowing which

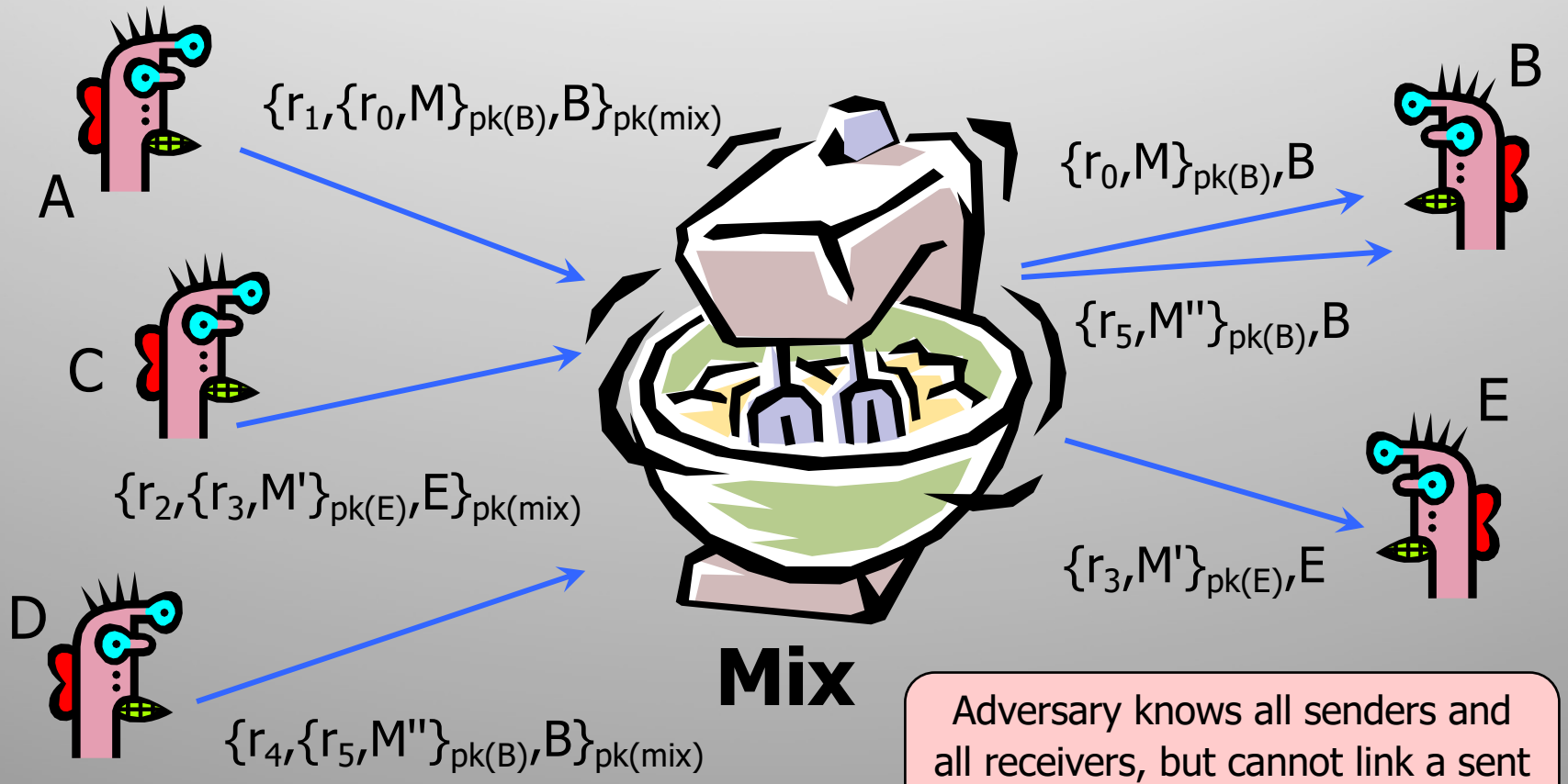
Chaum's Mix

- Earliest proposal for anonymous email (1981!!!)
  - David Chaum. “Untraceable electronic mail, return addresses, and digital pseudonyms”. Communications of the ACM, February 1981.

Before spam, people thought anonymous email was a good idea ☺

- Public key crypto + trusted re-mailer (Mix)
  - Untrusted communication medium
  - Public keys used as persistent pseudonyms
- Modern anonymity systems use Mix as the basic building block

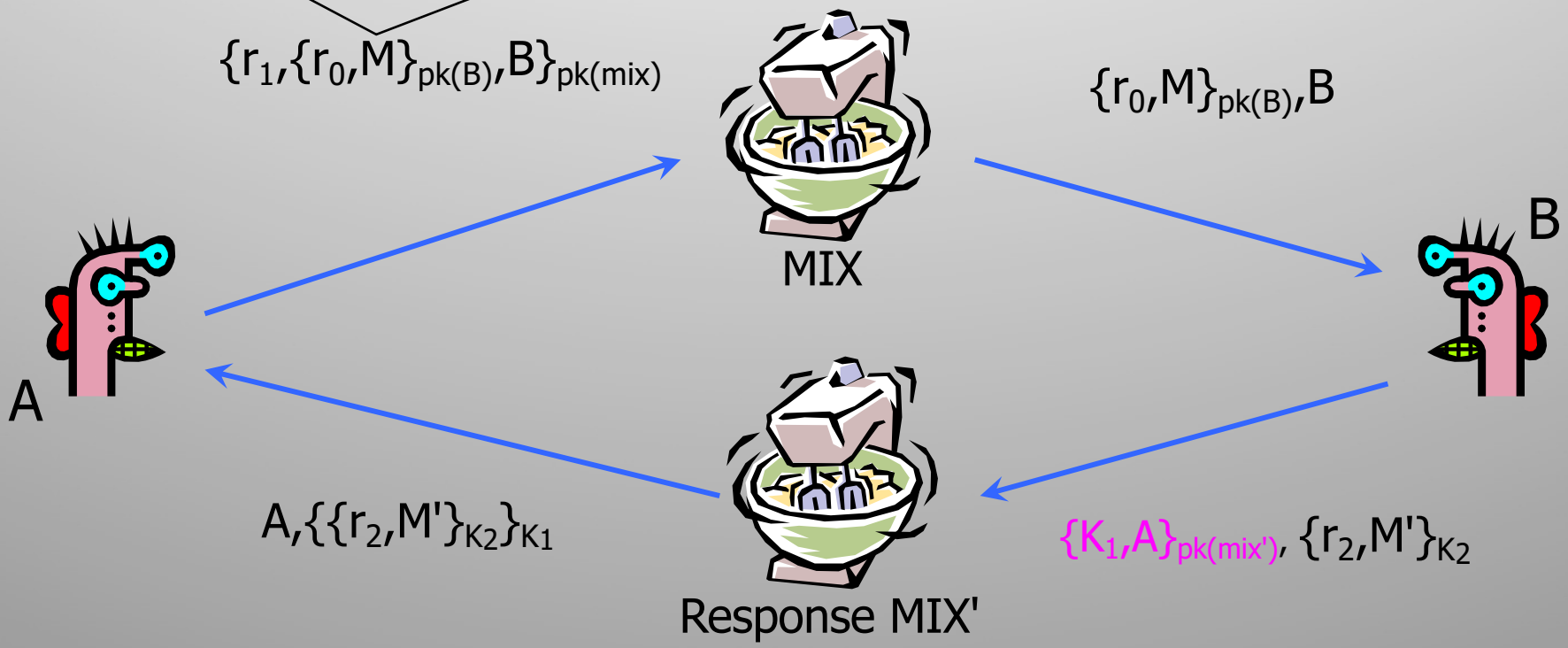
Basic Mix Design



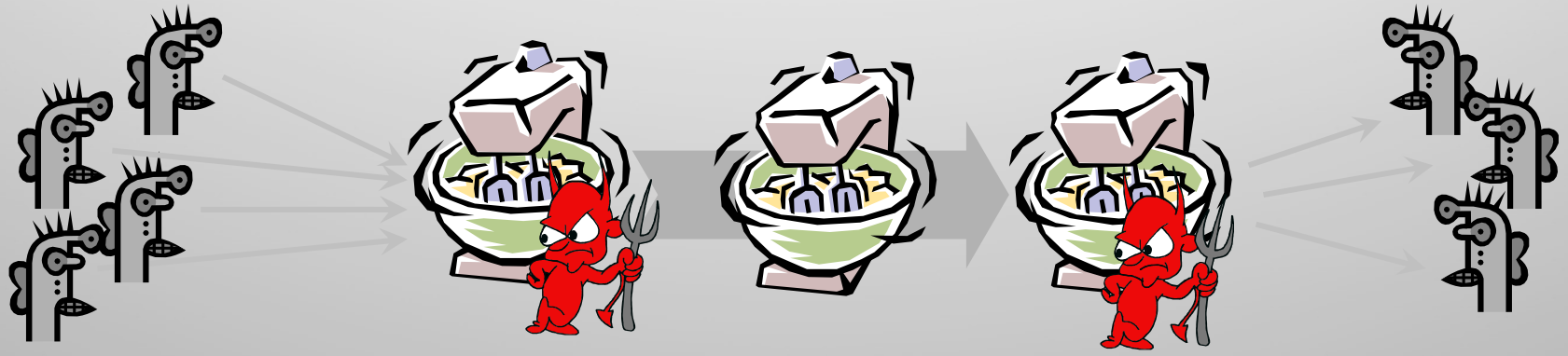
Adversary knows all senders and all receivers, but cannot link a sent message with a received message

Anonymous Return Addresses

M includes $\{K_1,A\}_{pk(mix')}$, K_2 where K_2 is a fresh public key and MIX'is possibly different from MIX



Mix Cascade



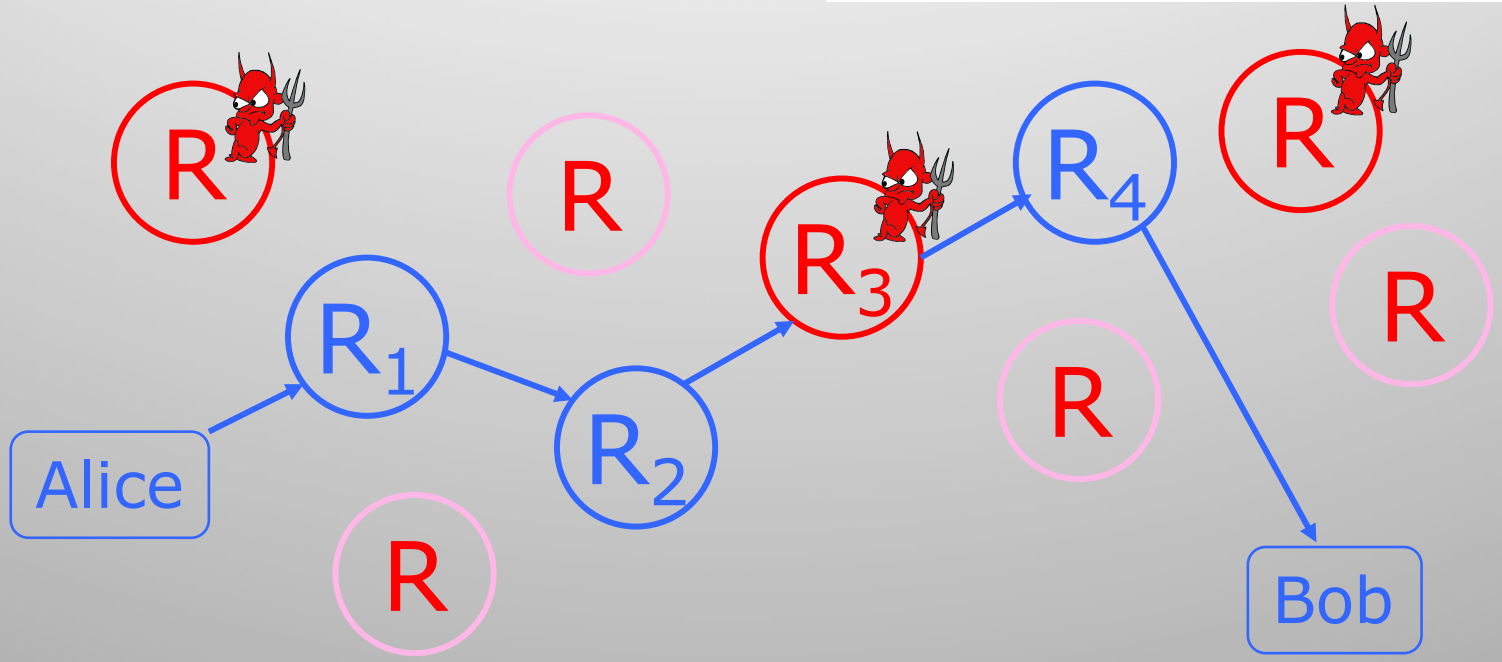
- Messages are sent through a sequence of mixes
  - Can also form an arbitrary network of mixes ("mixnet")
- Some mixes may be controlled by attacker, but even a single good mix guarantees some anonymity
- Pad and buffer traffic to foil correlation attacks

Disadvantages of Basic Mixnets

- Public-key encryption and decryption at each mix are computationally expensive
- Basic mixnets incur high latency
  - Ok for email, but not for anonymous Web browsing or any other low-latency communication
- Challenge: need a low-latency anonymity network
  - Use public-key cryptography to establish a "circuit" with pairwise symmetric keys between hops on the circuit
  - Then use symmetric decryption and re-encryption to move data messages along the established circuits
  - Each node behaves like a real-time mix; anonymity is preserved even if some nodes are compromised

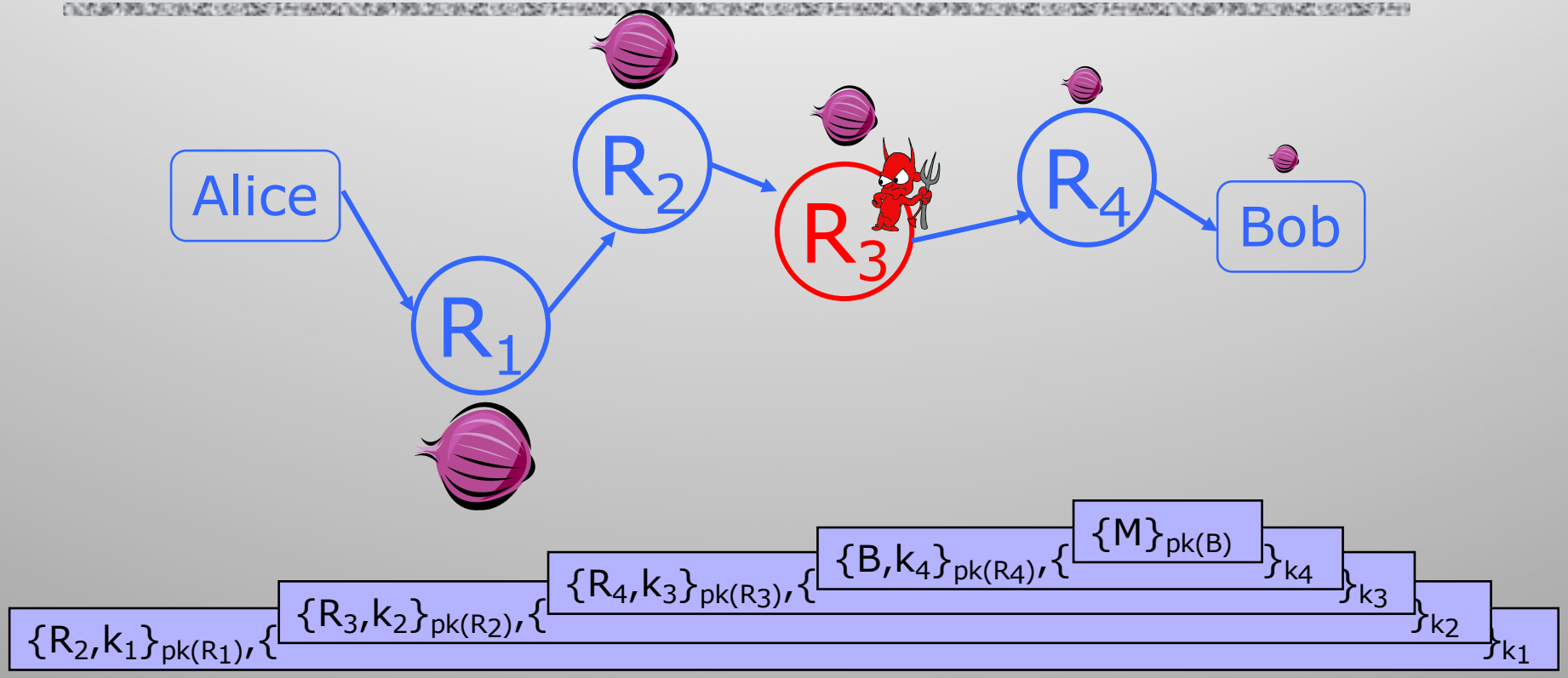
Onion Routing

[Reed, Syverson, Goldschlag 1997]



- Sender chooses a random sequence of routers
  - Some routers are honest, some are not
  - Sender controls path length

Route Establishment



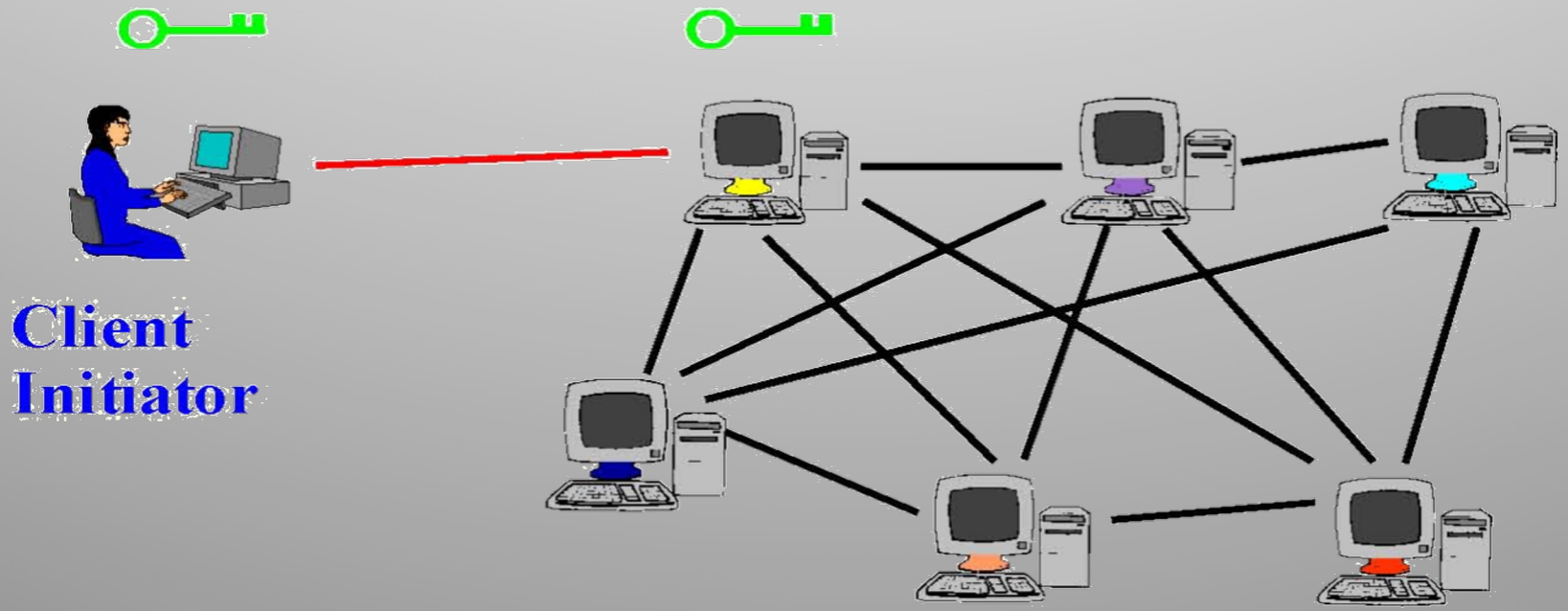
- Routing info for each link encrypted with router's public key
- Each router learns only the identity of the next router

Tor

- Second-generation onion routing network
  - First generation used onion routing
  - This one uses "telescopic" route setup
  - http://tor.eff.org
  - Specifically designed for low-latency anonymous Internet communications (e.g., Web browsing)
  - Running since October 2003
- Thousands of Tor nodes worldwide, 100s on each continent
- About 3-4 Mil users (06/22)
- "Easy-to-use" apps, client proxies and plug-ins
  - Including ToR Browser (slow-ish, but highly recommended!!!)
  - Freely available, excellent for anonymous browsing

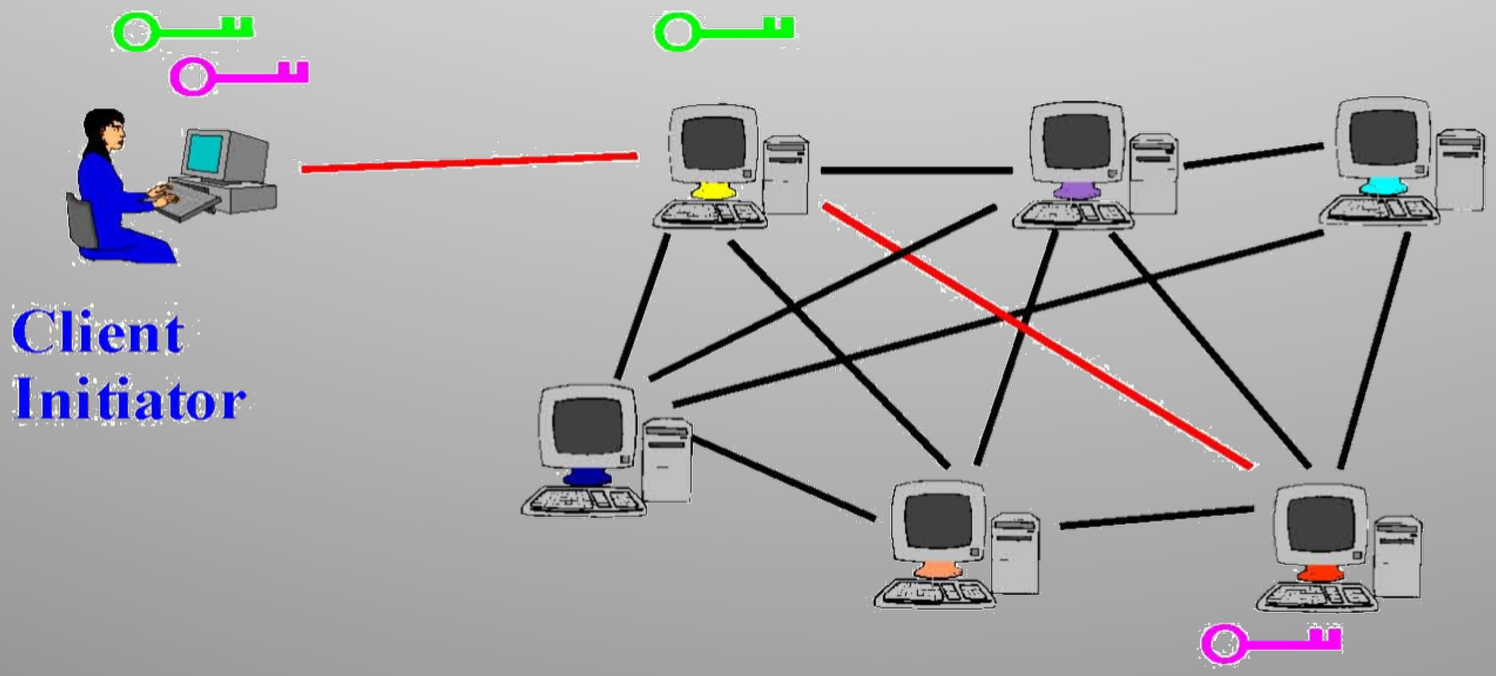
Tor Circuit Setup (1)

- Client proxy establishes a symmetric session key and circuit with Onion Router #1



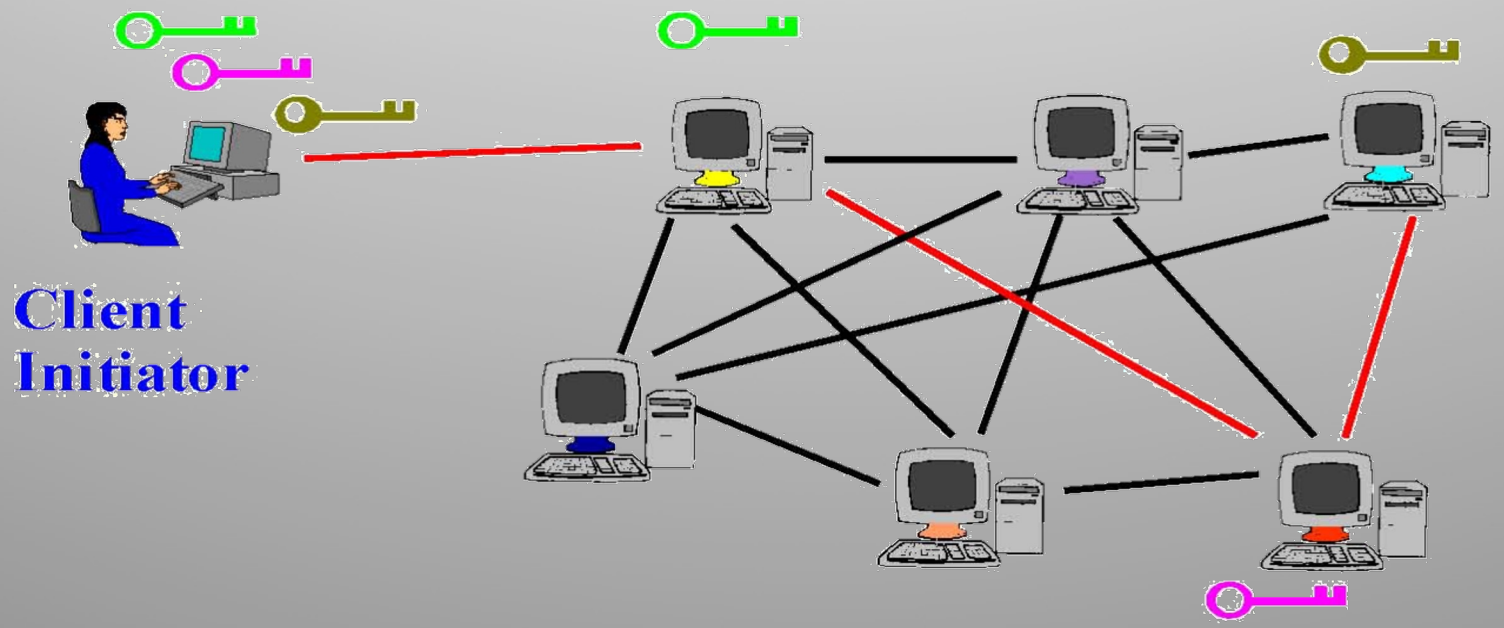
Tor Circuit Setup (2)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #2
  - Tunnel through Onion Router #1



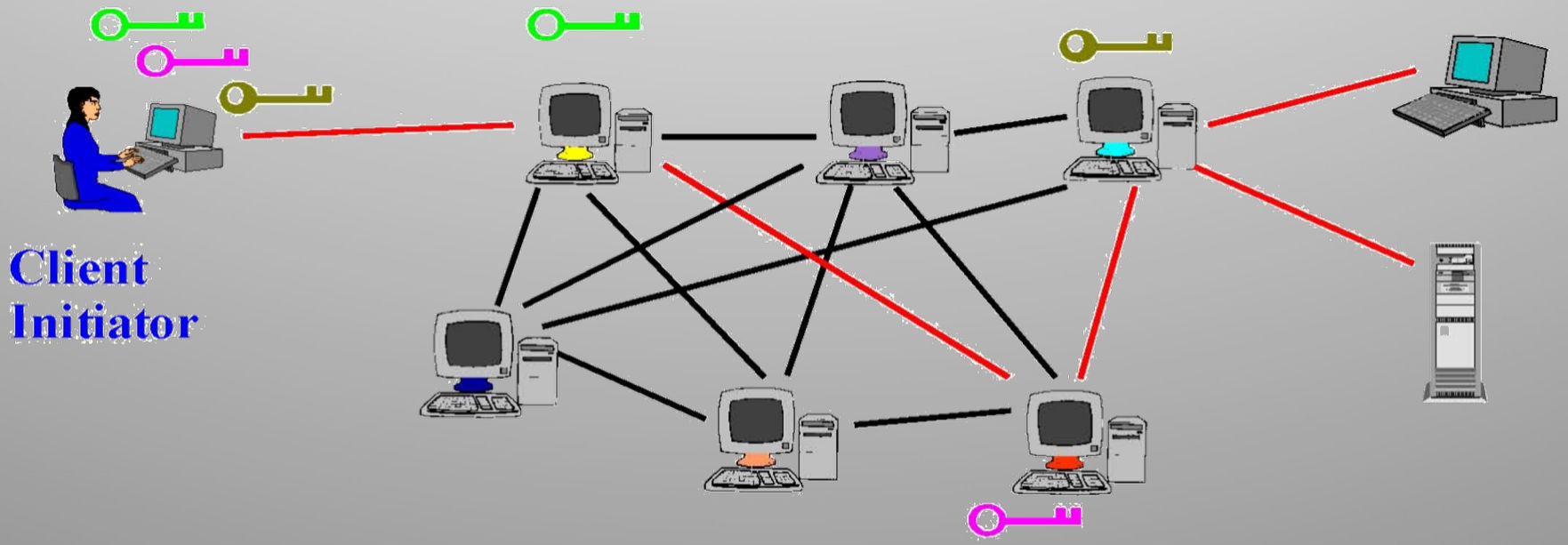
Tor Circuit Setup (3)

- Client proxy extends the circuit by establishing a symmetric session key with Onion Router #3
  - Tunnel through Onion Routers #1 and #2

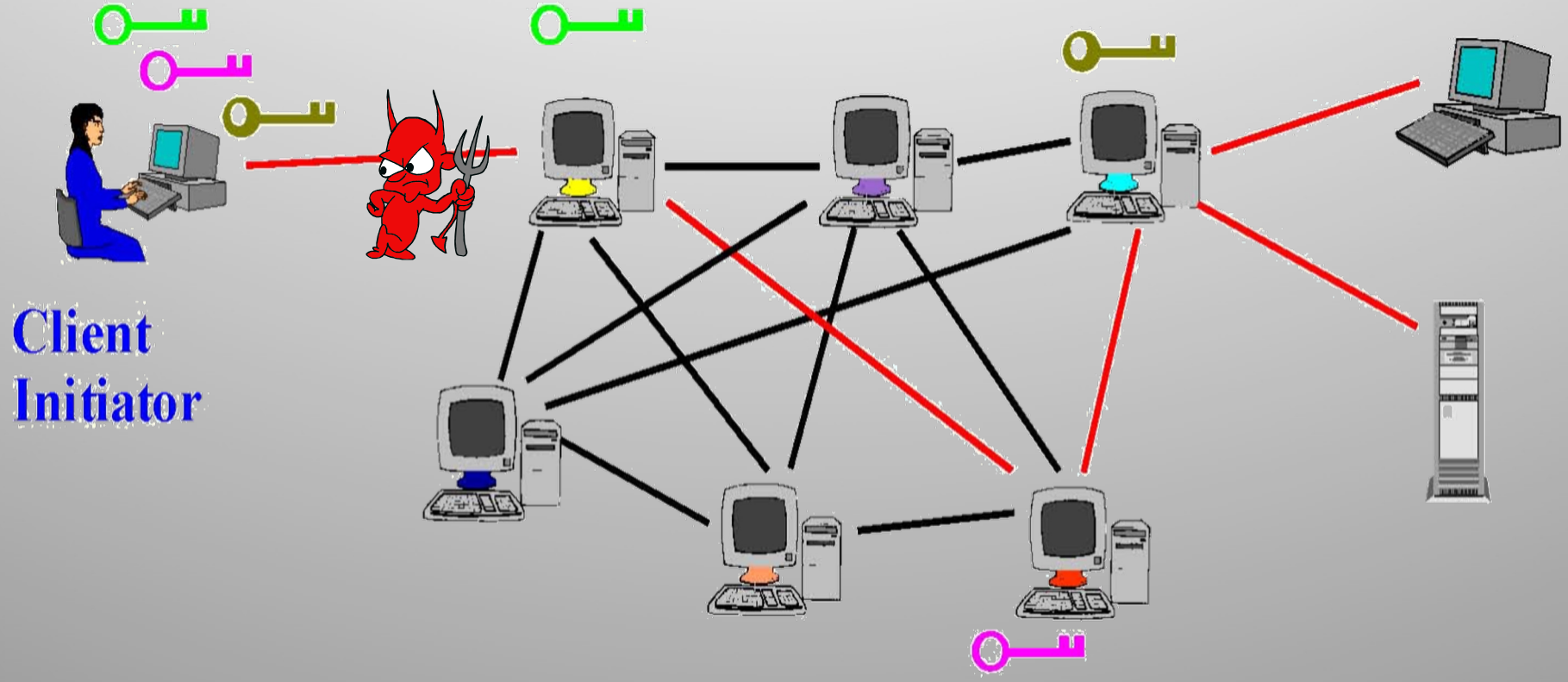


Using a Tor Circuit

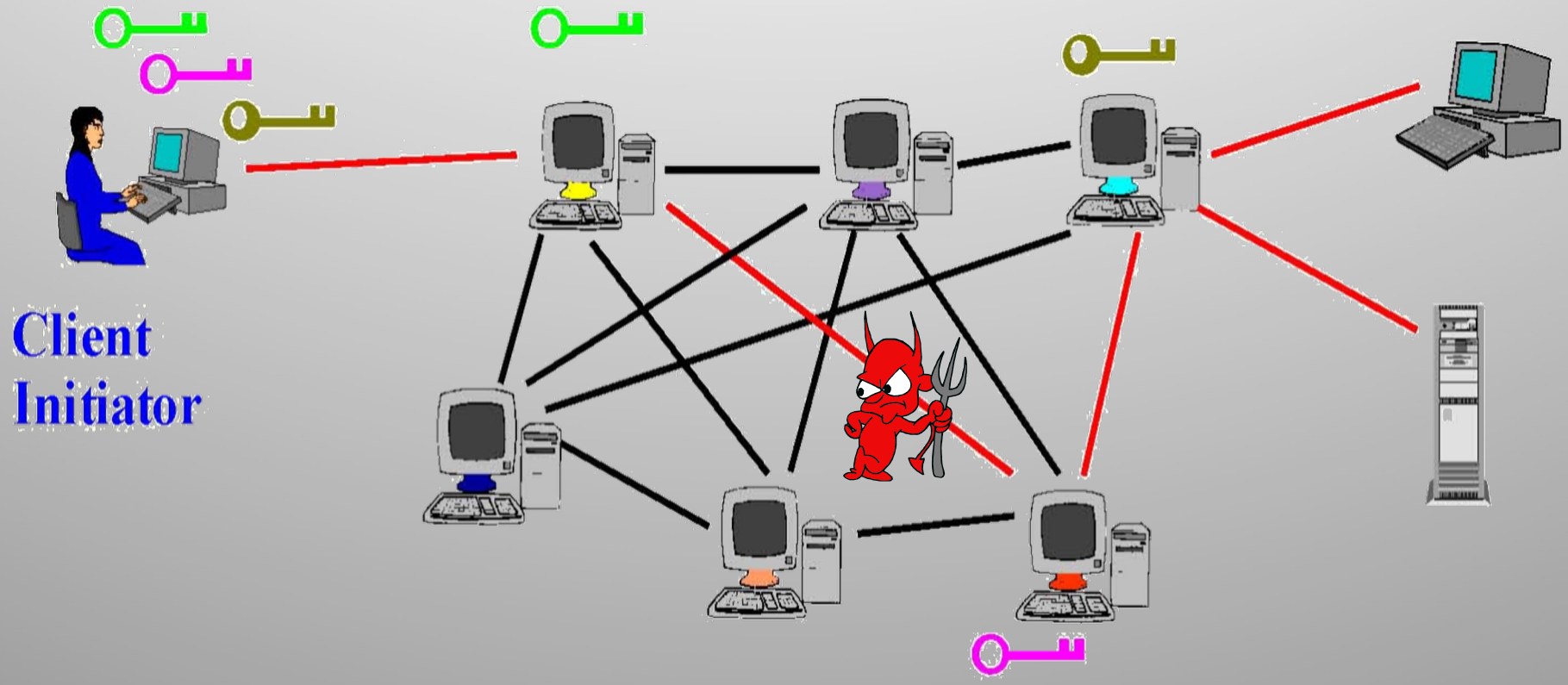
- Client applications connect and communicate over established Tor circuit (also to multiple dst-s)
  - Packets are decrypted and re-encrypted at each link



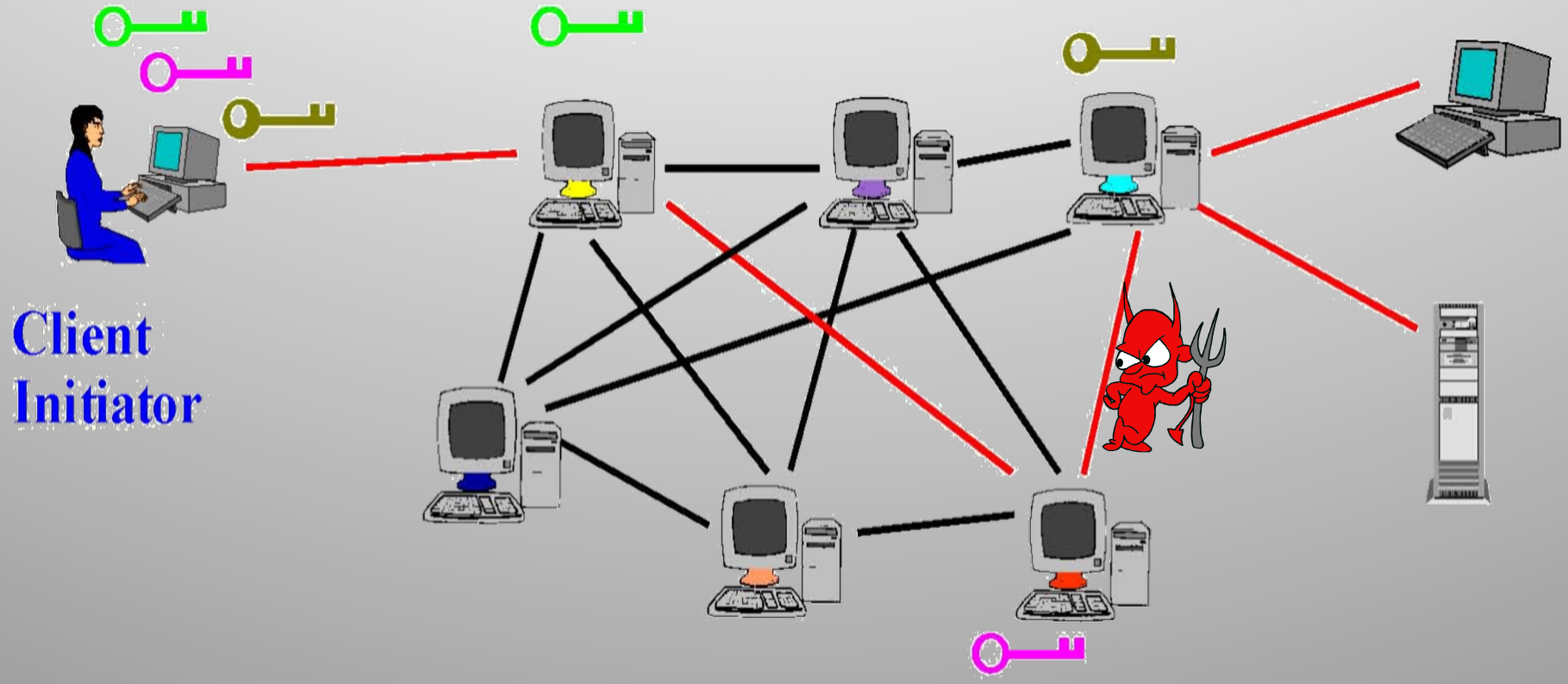
What does the adversary know/see?



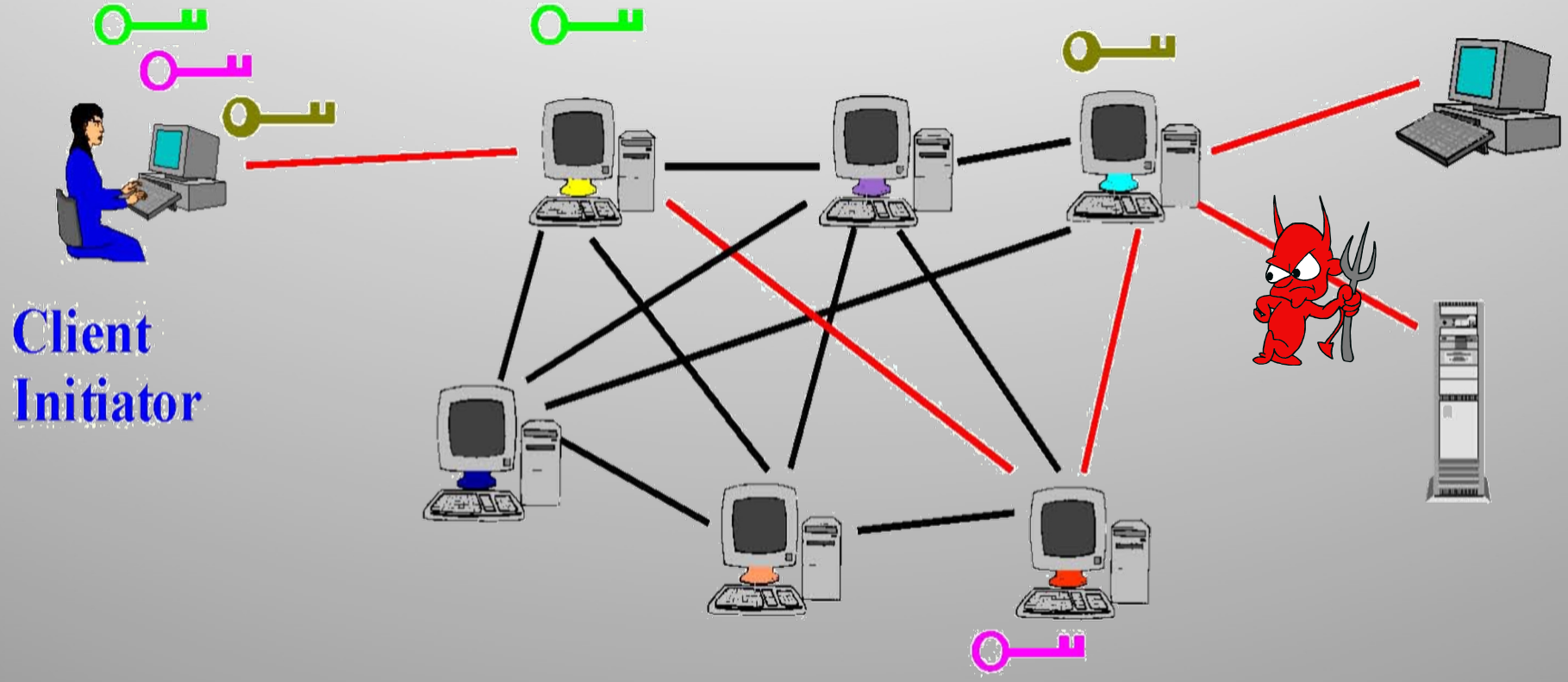
What does the adversary know/see?



What does the adversary know/see?



What does the adversary know/see?



Tor Management Issues

- Many applications can share one circuit
  - Blend multiple TCP streams over one anonymous connection
- Tor router doesn't need root privileges
  - Encourages people to set up their own routers
  - More participants = better anonymity for everyone
- Directory servers
  - Maintain lists of active onion routers, their locations, current public keys, etc.
  - Control how new routers join the network
    - "Sybil attack": attacker creates a large number of routers
  - Directory servers'keys ship with Tor code --- major PoV

Location Hidden Servers

- Goal: deploy a server on the Internet that anyone can connect to without knowing where it is or who runs it
  - Silk Road used this, btw ☺
  - https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
- Accessible from anywhere
- Resistant to censorship
- Can survive a full-blown DoS attack
- Resistant to physical attack
  - Can't find the physical server!

Silk Road

anonymous marketplace

Wel

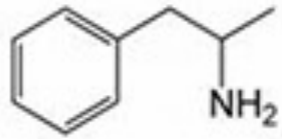
messages(0) | orders(0) | account(฿0.00)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)

10 Grams high grade MDMA 80+%

฿61.17



Amphetamines sulfate / Speed freebase...

฿28.59

2g Jack Frost (weed) *420 SALE****

฿8.54

5 Grams of pure MDMA crystals

฿42.04

100 red Y tablets 111mg (lab tested)...

฿97.77

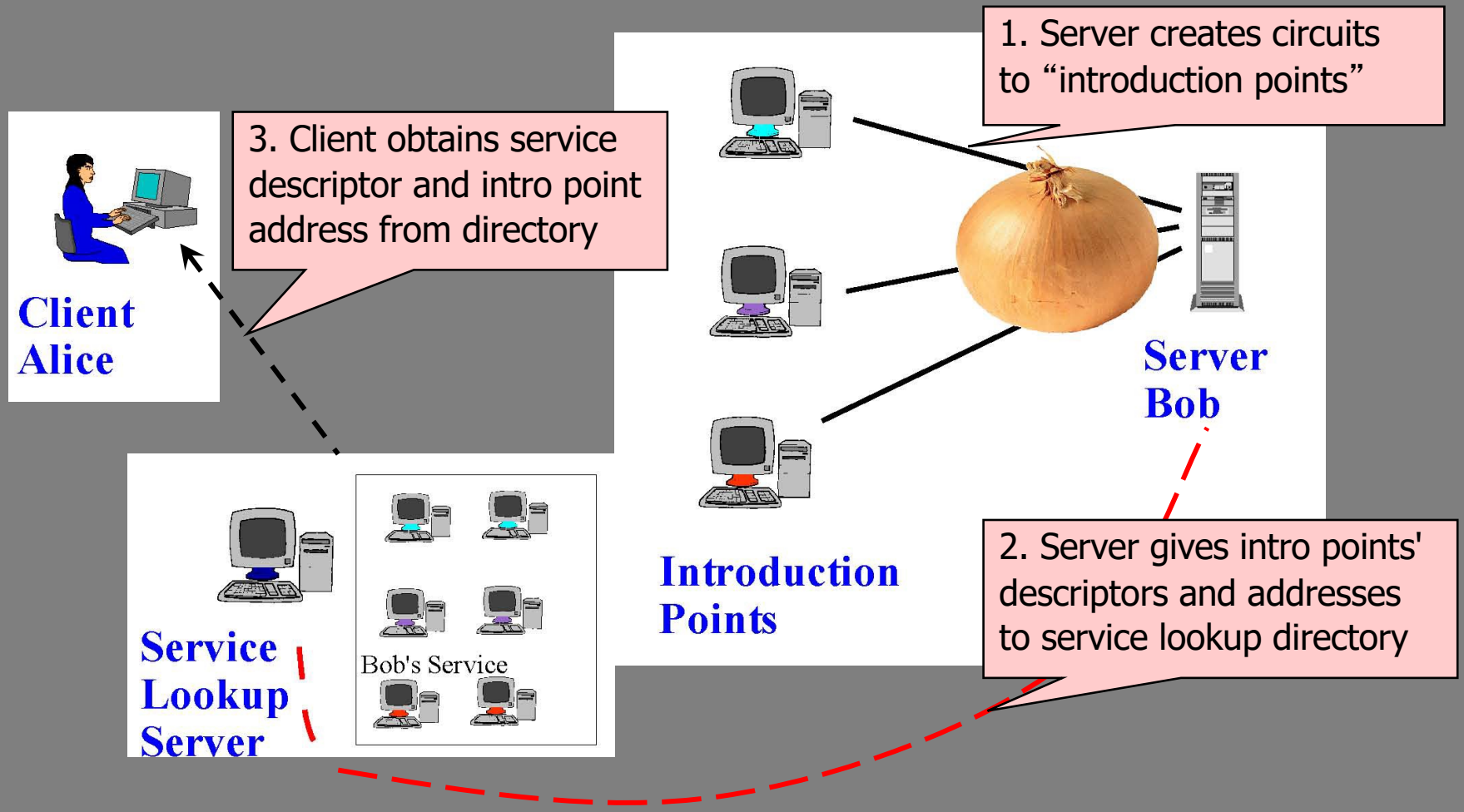
Michael Jackson Discography 1971-2009...

฿2.52

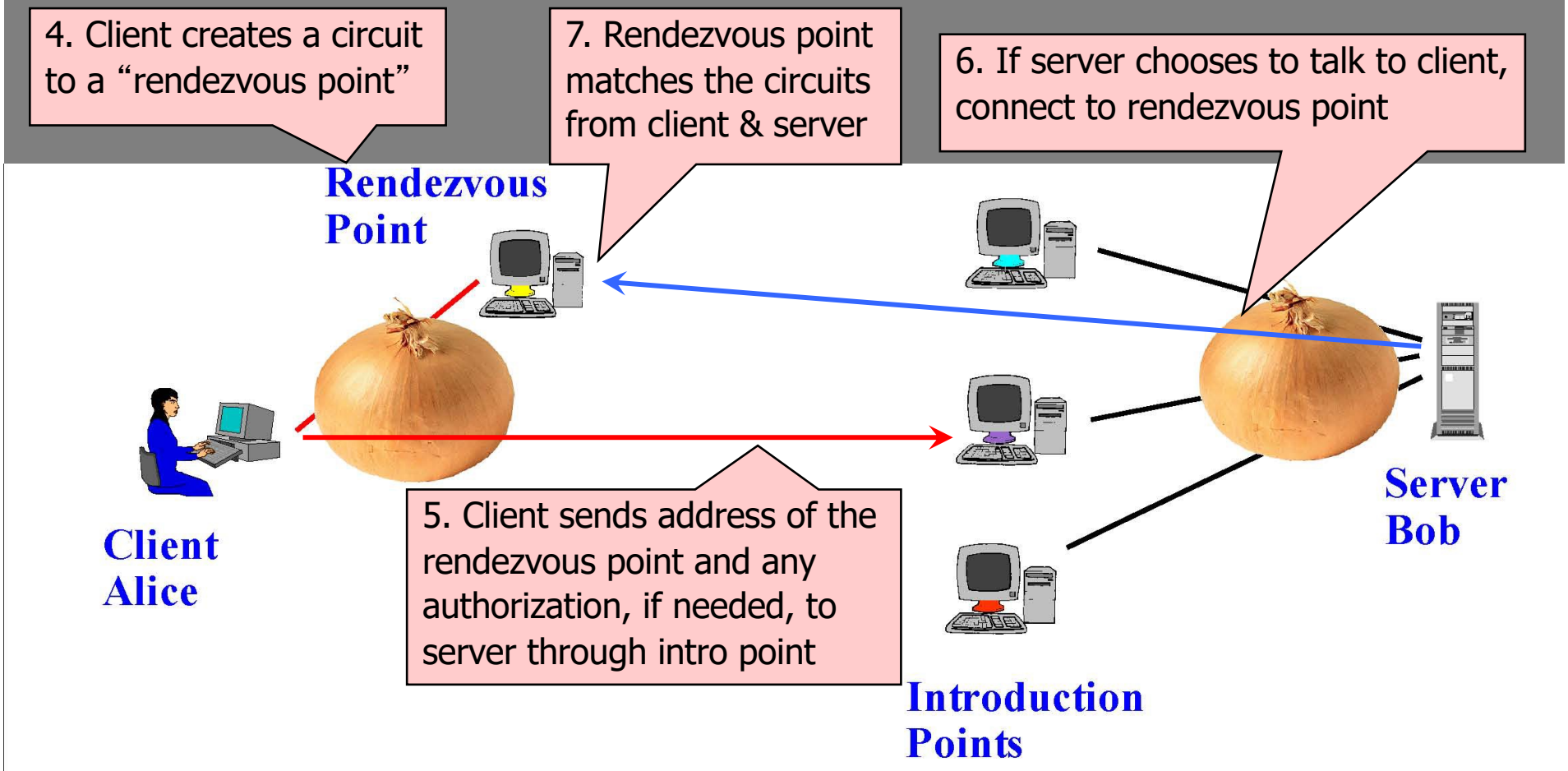
New

- Th
  or
- W
  fa
- Ac
  H
- A
  m
  A
- St
  A

Creating a Location Hidden Server

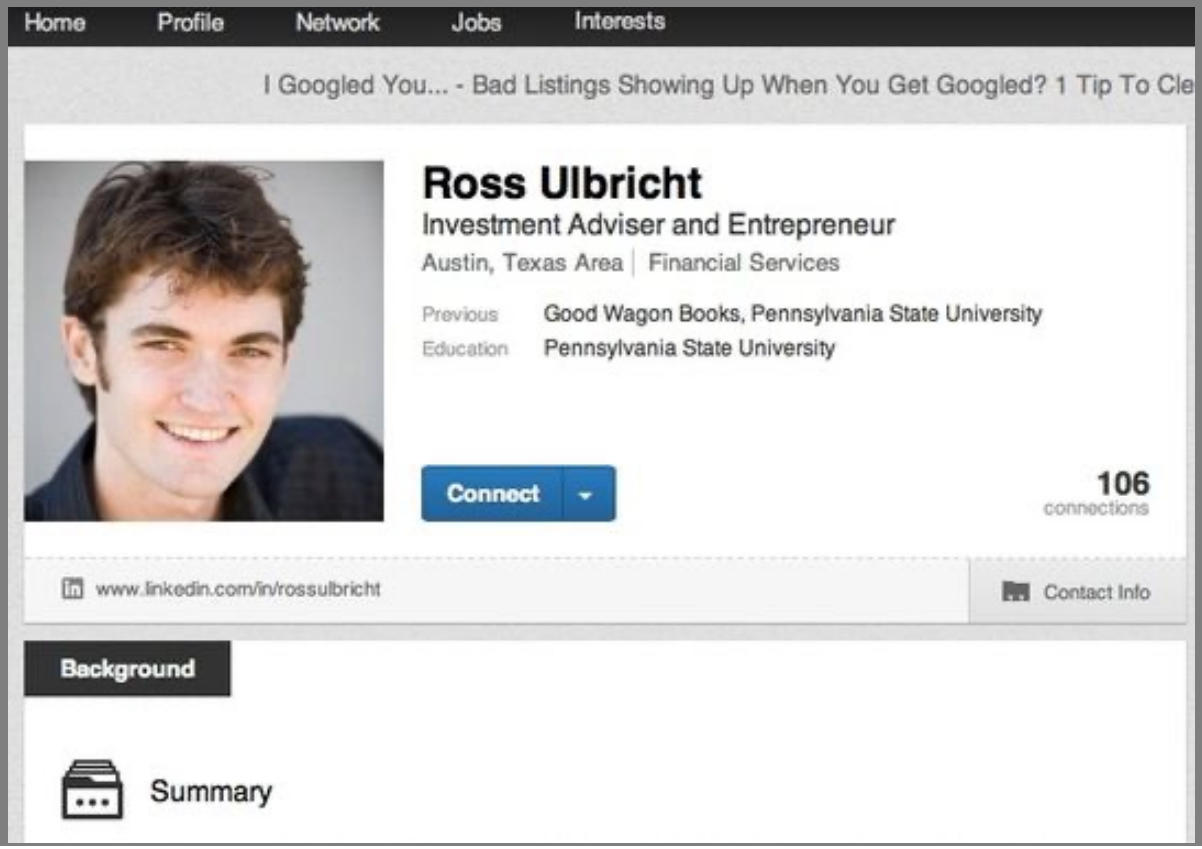


Using a Location Hidden Server



Silk Road Shutdown

- Ross Ulbricht, alleged operator of the Silk Road Marketplace, arrested by the FBI on Oct 1, 2013



Silk Road Shutdown Theories

- A package of fake IDs from Canada traced to an apartment to San Francisco?
- A fake murder-for-hire arranged by DPR?
- A Stack Overflow question accidentally posted by Ulbricht under his real name?
  - "How can I connect to a Tor hidden service using curl in php?"
  - … a few seconds later, changed username to "frosty"
  - … oh, and the encryption key on the Silk Road server ends with the substring "frosty@frosty"
- Probably not due to a weaknesses in Tor

Deployed Anonymity Systems

- Free Haven project has an excellent bibliography on anonymity
  - http://www.freehaven.net/anonbib
- Tor (http://tor.eff.org)
  - Overlay circuit-based anonymity network
  - Best for low-latency applications such as anonymous Web browsing
- Mixminion (http://www.mixminion.net)
  - Network of mixes
  - Best for high-latency applications such as anonymous email
- Mixmaster (http://mixmaster.sourceforge.net)
  - Chaum-like MIX, publicly available code

Dining Cryptographers

- How to make a message public, but in a perfectly untraceable manner
  - David Chaum. "The dining cryptographers problem: unconditional sender and recipient untraceability." Journal of Cryptology, 1988.
- Guarantees information-theoretic anonymity for message senders
  - VERY strong form of anonymity: defeats adversary who has unlimited computational power
- Difficult to make practical
  - In group of size N, need N random bits to send 1 bit

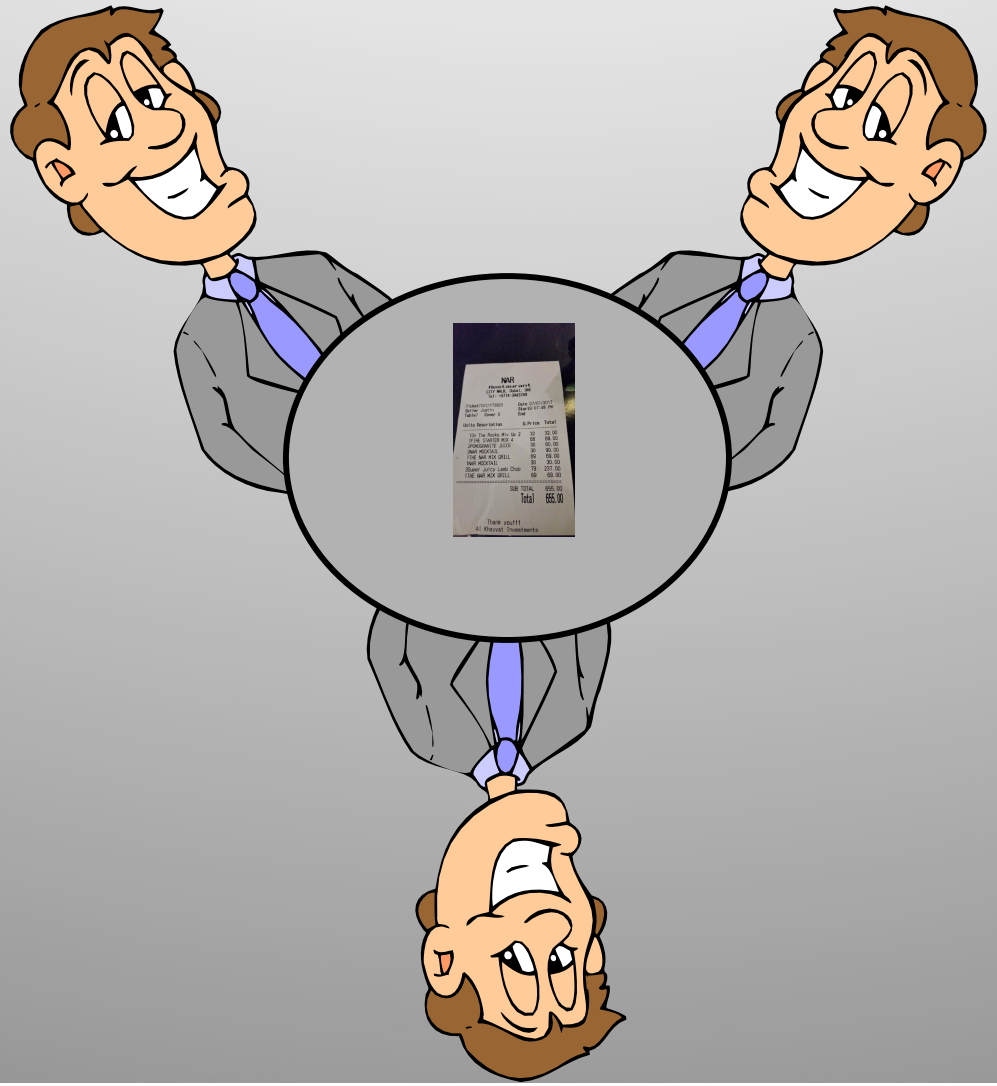
Three-Person DC Protocol

- Three cryptographers are having dinner.
- Either NSA is paying for the dinner, or one of them is paying, but wishes to remain anonymous.

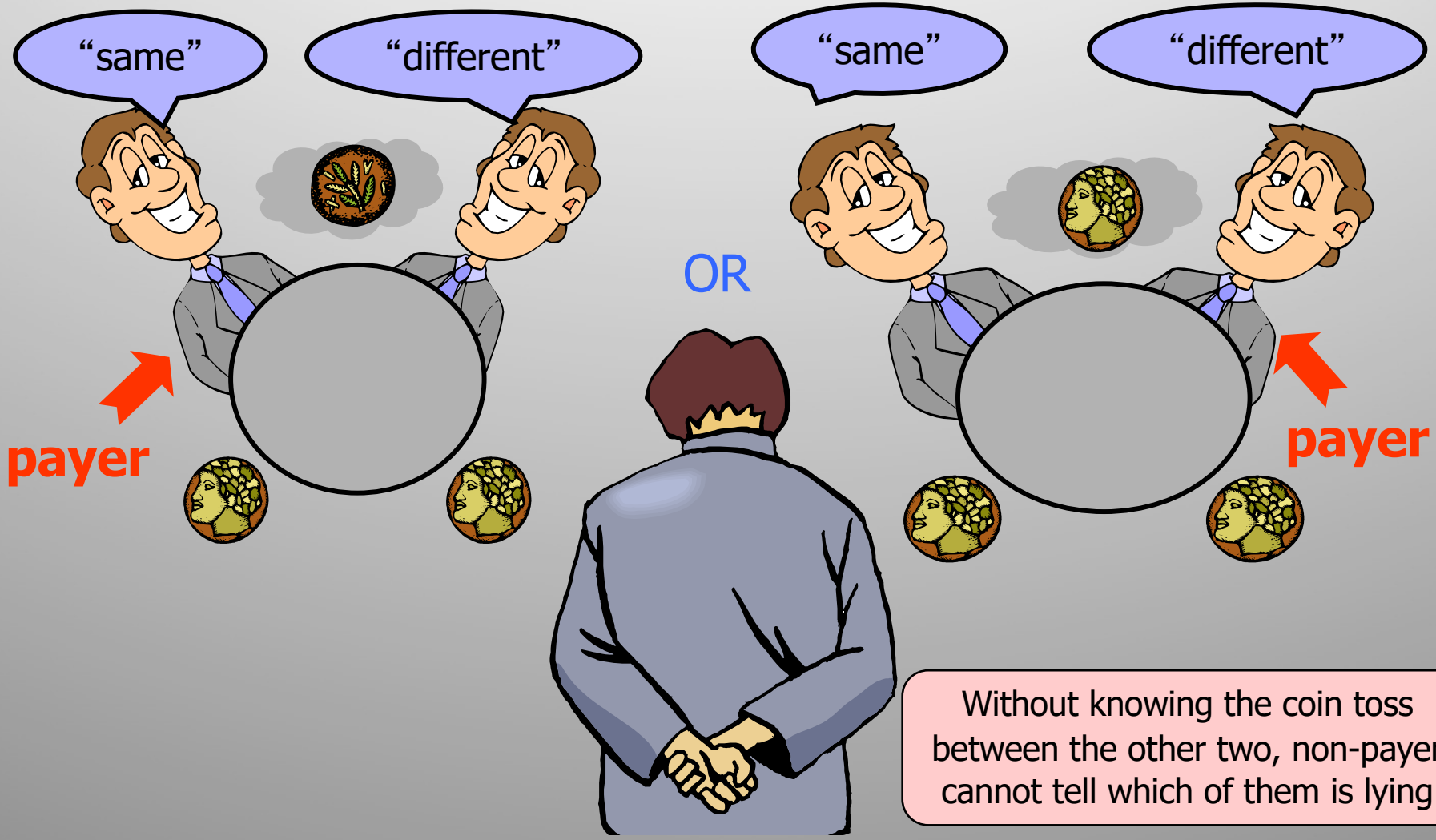
1. Each person flips a coin and shows it to his left neighbor.
   - Every diner sees two coins: his own and his right neighbor's
2. Each person announces whether the two coins are the same. If he is the payer, he lies (says the opposite).
3. IF Number of "same"=1 or 3 $\Rightarrow$ NSA is paying

   IF Number of "same"=0 or 2 $\Rightarrow$ one of them is paying
   - But a non-payer cannot tell which of the other two is paying!

The 3 Dining Cryptographers

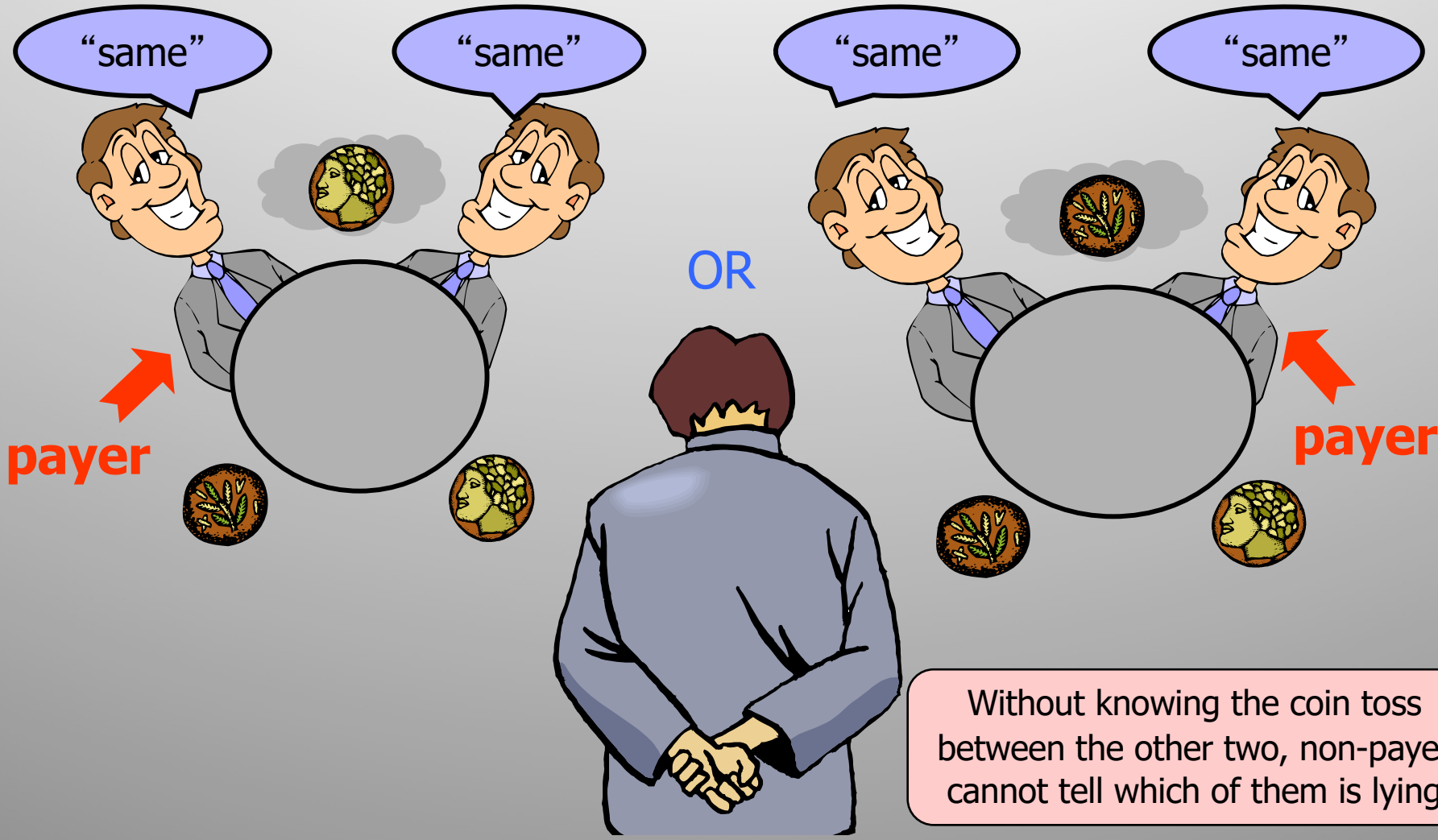


Non-Payer's View: Same Coins



Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying

Non-Payer's View: Different Coins



Without knowing the coin toss between the other two, non-payer cannot tell which of them is lying

Super-Posed Sending

- This idea generalizes to any group of size N
- For each bit of the message, every user generates 1 random bit and sends it to ONE neighbor
  - Every user learns 2 bits (his own and his neighbor's)
- Each user announces own bit, XOR-ed with neighbor's bit
- Sender announces own bit XOR neighbor's bit XOR message bit
- XOR all announcements = message bit
  - Every randomly generated bit occurs in this sum twice (and is canceled by XOR), message bit occurs once