Wait, this is about security *and* privacy?

Secure Systems Engineering Spring 2024

🛡️ `EE G7701`

April 2, 2024
Tushar Jois

Grades

- Exam 1 grades are available on Blackboard
  - To get back your exam and rubric, email me from your CCNY email with the subject line “EE G7701 Exam 1 `[LastName]`”
- Thoughts on Exam 1
- Aside: Most other grades are also now available
  - Some “edge case” Assignment 2 grading that still needs to be done
  - Working on Assignment 3 grades now

Recap

- Secure systems can be backdoored in a myriad of ways
- The use of computing systems requires accepting large chains of trust
- Balancing the risks of cybersecurity vulnerabilities with the ease of open-source integration is a challenge

Lesson objectives

- Work through, step by step, the operation of the Signal protocol
- Describe how Tor uses onion routing to provide censorship resistance
- Understand the political and societal ramifications of privacy

Defining privacy

- What are the goals of security?
- What are the goals of privacy?

(it’s okay if some of them are the same!)

- Order the following data types by how valuable privacy is to the data:
    a. Browser history
    b. Financial statements
    c. Medical records
    d. Text messages
    e. Grade transcript

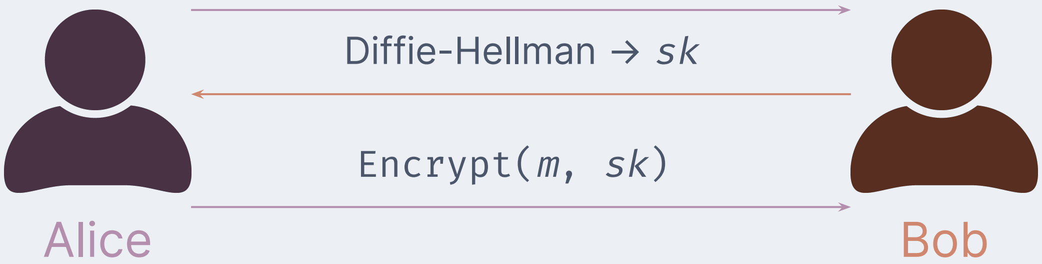
The importance of secure messaging

- Facebook Messenger, Instagram are not “end-to-end”
  - Facebook reads the messages, delivers ads about them
  - Governments can subpoena Facebook for your messages, reconstruct your digital life
- “Surveillance capitalism”
  - The person is the product
  - “Free” services provided by Big Tech powered by the selling of your data
- Data sharing agreements
  - Seen ads for things you’ve talked about on Amazon?

“But I have nothing to hide!”

- Solidarity with those who do
  - Snowden/whistleblowers, but also “The Feeling of Being Watched” subjects
- You might not realize how much data is out there
  - “We kill people based on metadata”
- Data lasts forever, and you might have to someday
  - Data lasts *forever* -- and companies/banks/governments are looking

Attempt 0



Diffie-Hellman → sk

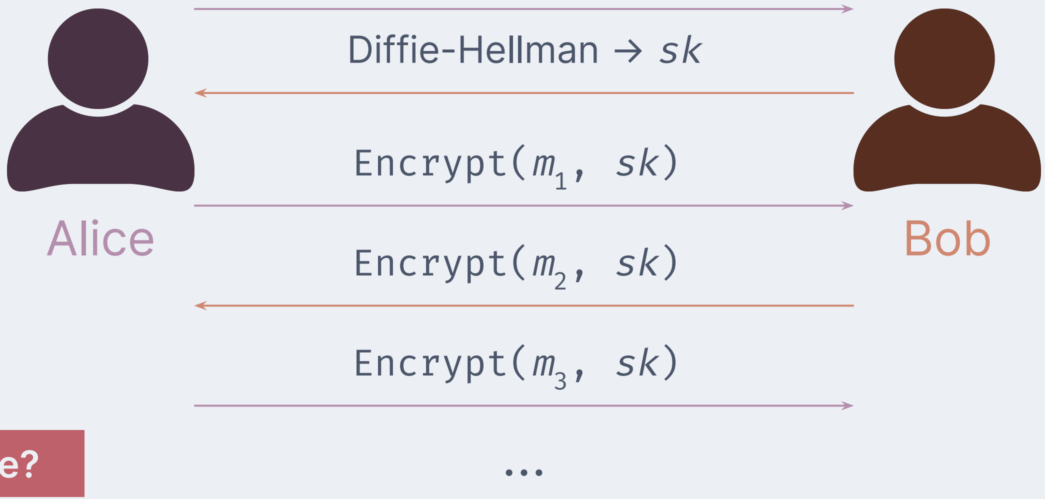
Encrypt(m, sk)

Alice

Bob

More than one message?

Attempt 1



Alice

Bob

Diffie-Hellman → sk

Encrypt(m_1, sk)

Encrypt(m_2, sk)

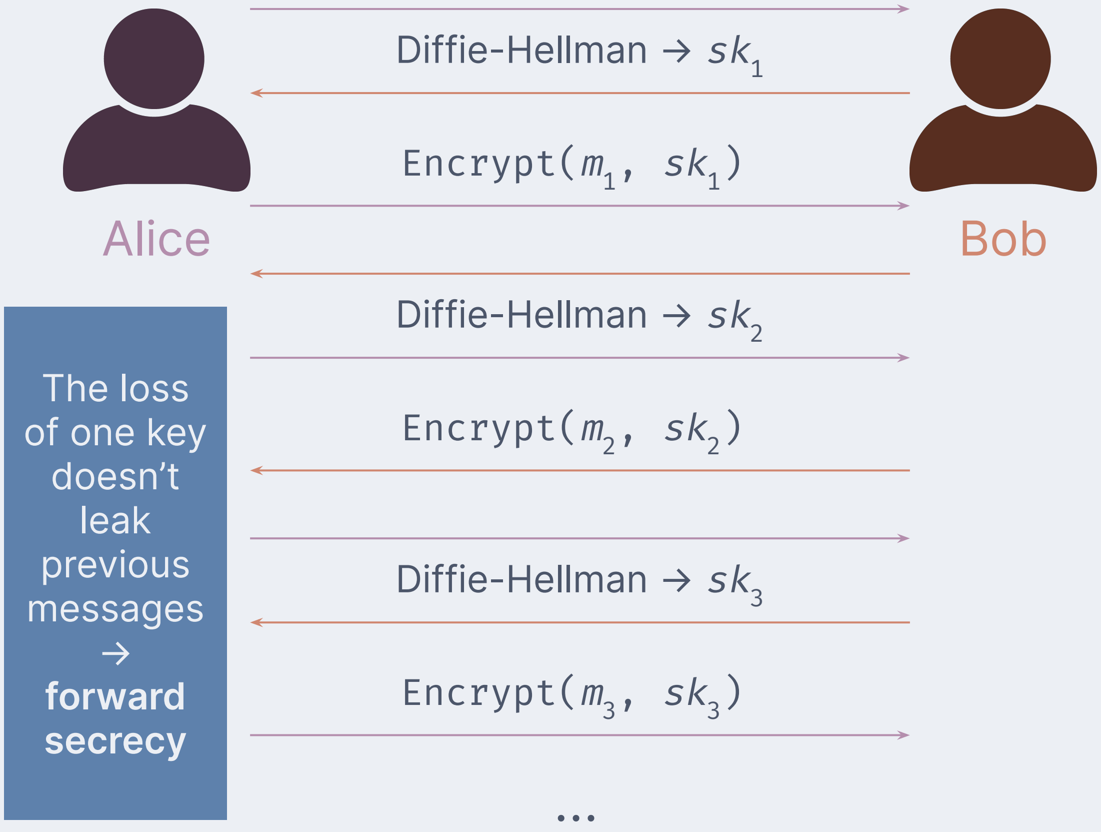
Encrypt(m_3, sk)

…

Key compromise?

- If Alice loses sk, the entire message history is disclosed
  - Phone loss
  - Forensic extraction
- Can we do better?

Attempt 2



Alice

Bob

Diffie-Hellman → sk_1

Encrypt(m_1, sk_1)

Diffie-Hellman → sk_2

Encrypt(m_2, sk_2)

Diffie-Hellman → sk_3

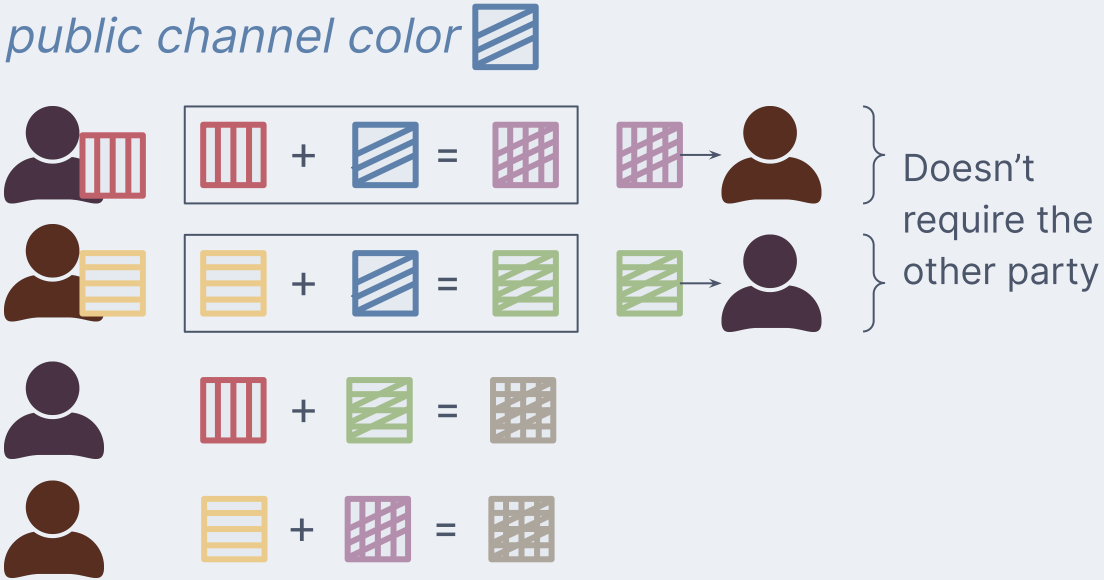
Encrypt(m_3, sk_3)

…

What if a party is offline?

Requires interaction

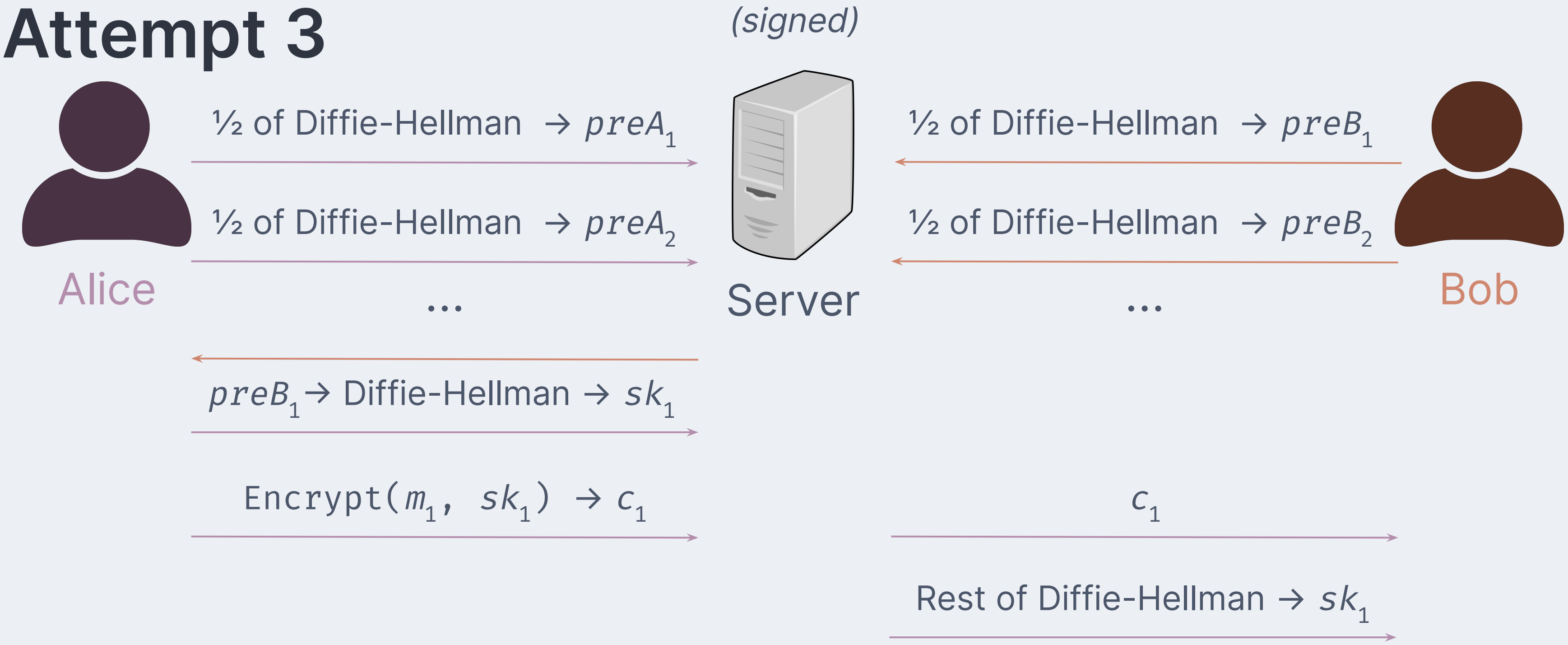
The loss of one key doesn't leak previous messages → **forward secrecy**



public channel color

Doesn't require the other party

Attempt 3



(signed)

Server

Alice

½ of Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preA_2$

…

$preB_1$ → Diffie-Hellman → sk_1

`Encrypt(`m_1`, `sk_1`)` → c_1

Bob

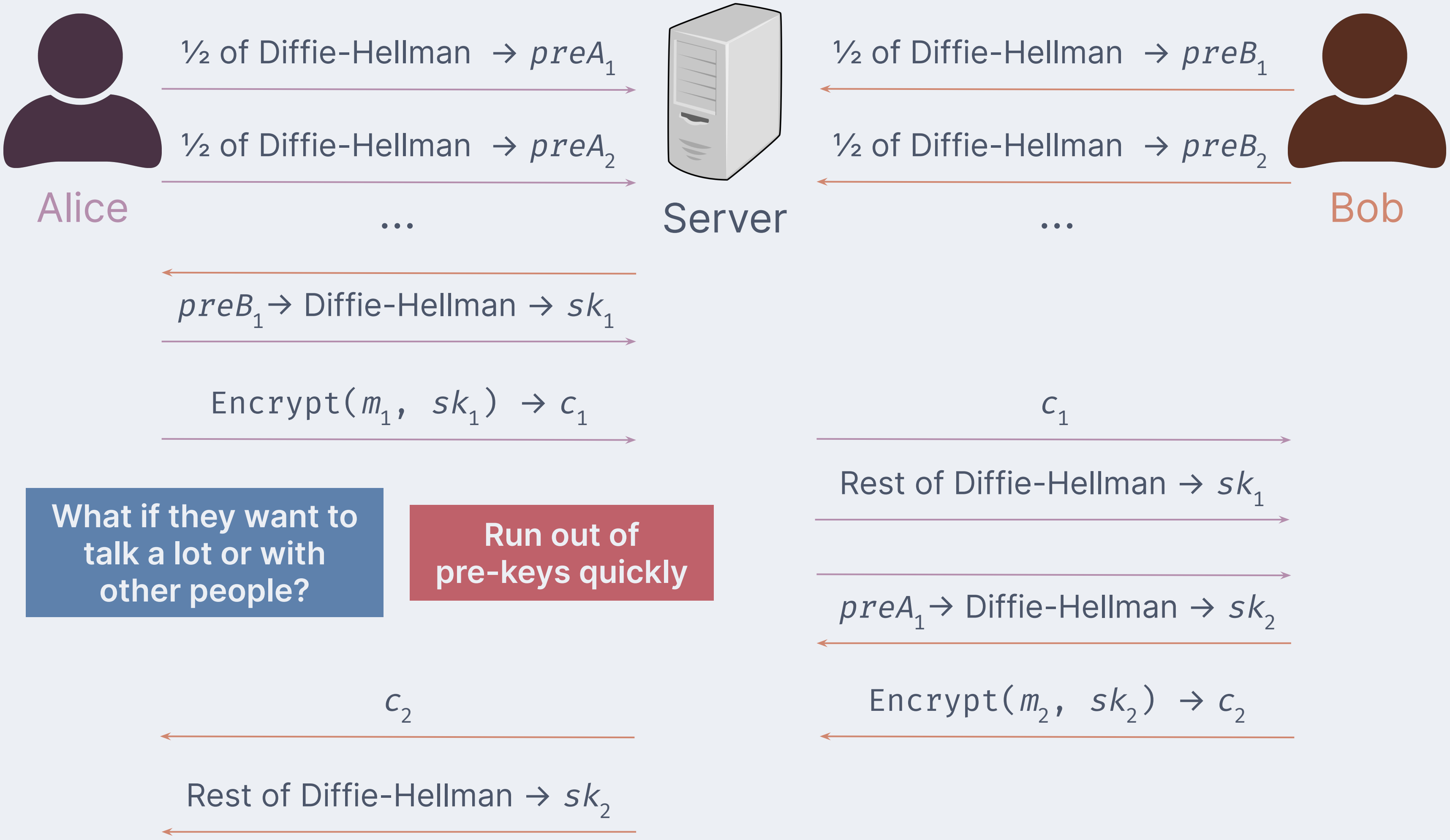
½ of Diffie-Hellman → $preB_1$

½ of Diffie-Hellman → $preB_2$

…

c_1

Rest of Diffie-Hellman → sk_1



Alice

Server

Bob

½ of Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preB_1$

½ of Diffie-Hellman → $preA_2$

½ of Diffie-Hellman → $preB_2$

…

…

$preB_1$ → Diffie-Hellman → sk_1

$\mathtt{Encrypt}(m_1,\ sk_1) \rightarrow c_1$

c_1

Rest of Diffie-Hellman → sk_1

What if they want to talk a lot or with other people?

Run out of pre-keys quickly

$preA_1$ → Diffie-Hellman → sk_2

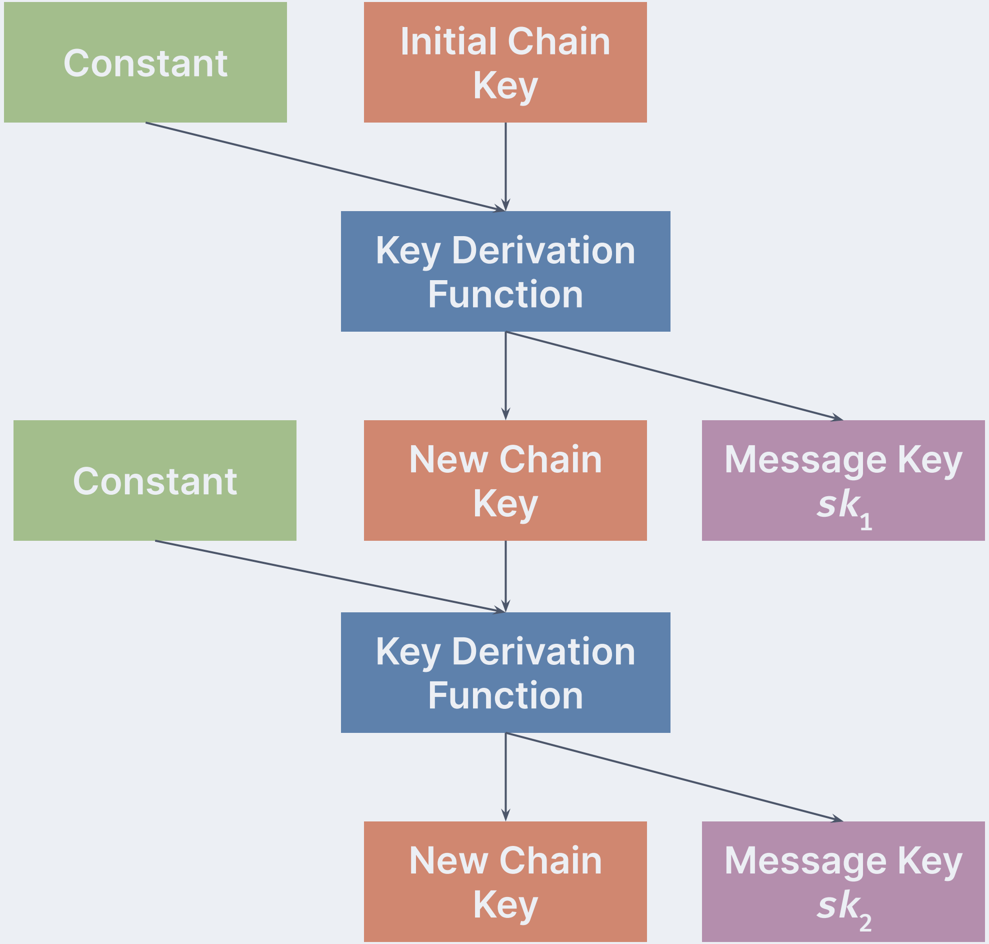
$\mathtt{Encrypt}(m_2,\ sk_2) \rightarrow c_2$

c_2

Rest of Diffie-Hellman → sk_2

KDF chain

- Special cryptographic construct that generates new keys from old keys
  - We can use the new keys for subsequent messages
  - Requires both parties to be in the same “state” of the ratchet
- Send a message, Alice encrypts with a key, and then “ratchets it forward”
  - Bob receives the message, decrypts it, and then “ratchets it forward”
  - Forward secrecy without significant interaction
  - Both have to keep in sync



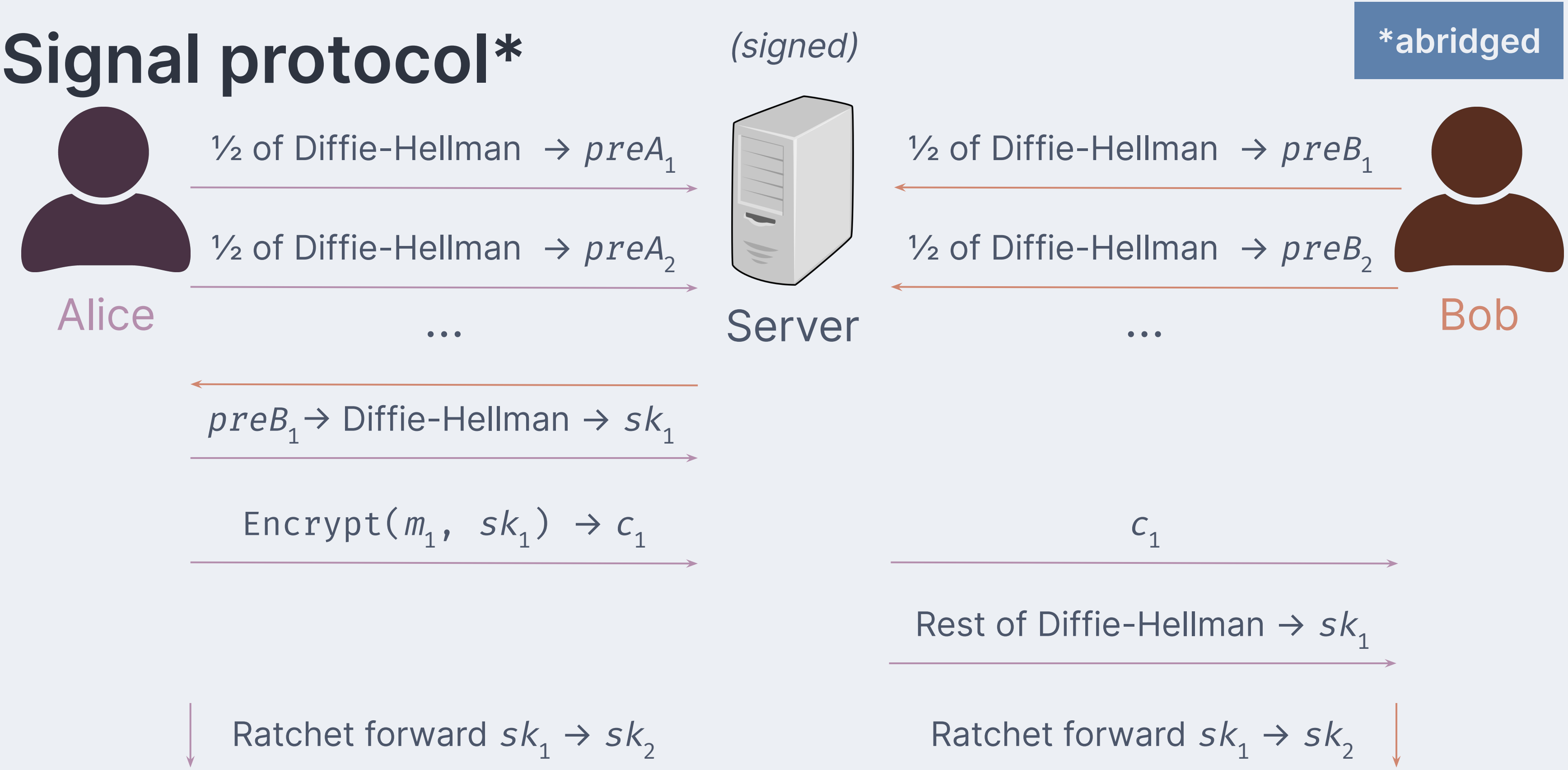
Symmetric ratcheting

“The parties derive new keys for every Double Ratchet message so that earlier keys cannot be calculated from later ones… [giving] some protection to earlier or later encrypted messages in case of a compromise of a party's keys.”

Perrin and Marlinspike, “The Double Ratchet Algorithm” (2016)

Signal protocol*

*abridged



(signed)

Alice

Server

Bob

½ of Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preA_2$

…

½ of Diffie-Hellman → $preB_1$

½ of Diffie-Hellman → $preB_2$

…

$preB_1$ → Diffie-Hellman → sk_1

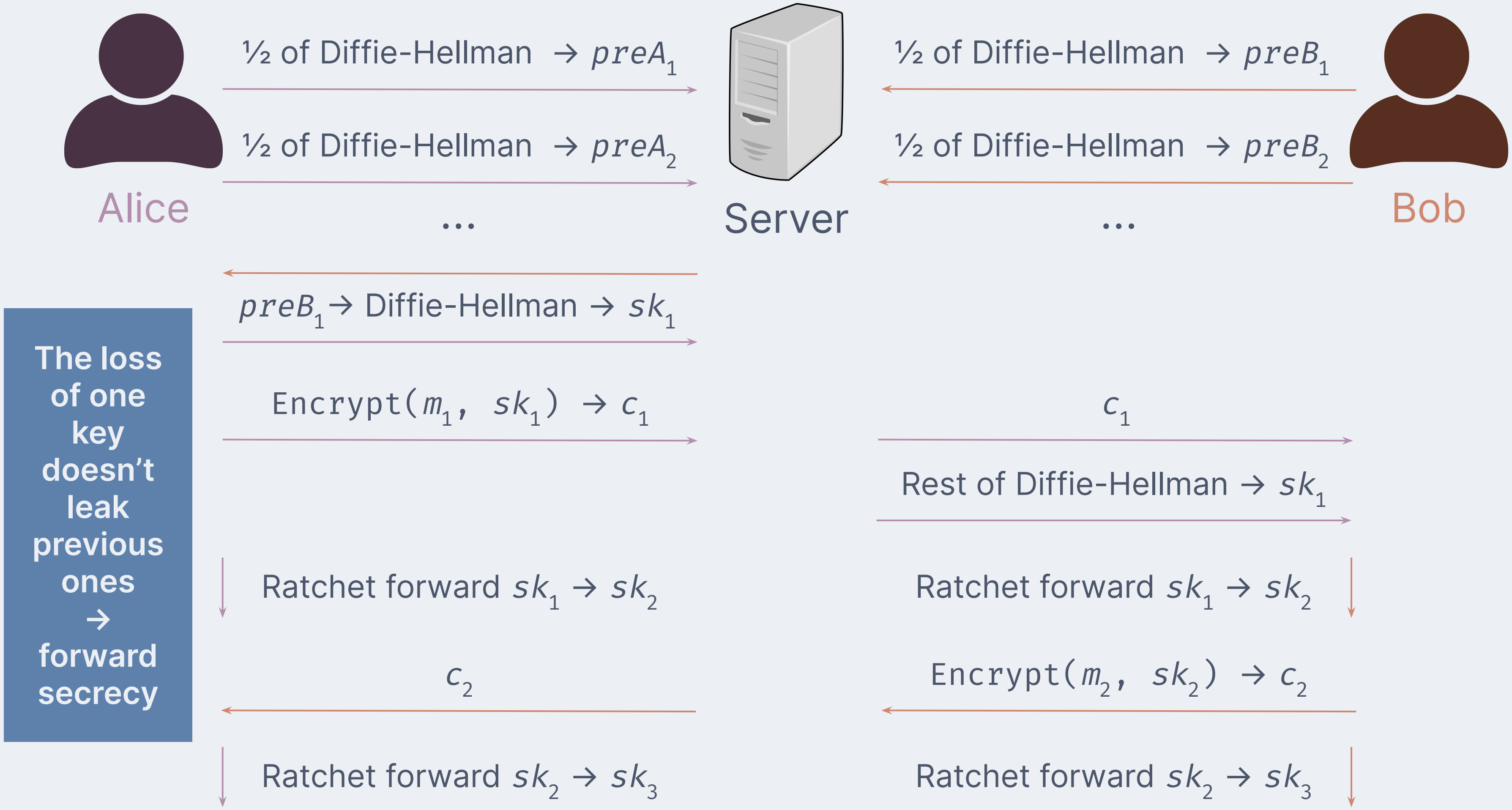
`Encrypt(`m_1`, `sk_1`)` → c_1

c_1

Rest of Diffie-Hellman → sk_1

Ratchet forward sk_1 → sk_2

Ratchet forward sk_1 → sk_2



Alice

Server

Bob

½ of Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preA_2$

...

½ of Diffie-Hellman → $preB_1$

½ of Diffie-Hellman → $preB_2$

...

$preB_1$ → Diffie-Hellman → sk_1

Encrypt(m_1, sk_1) → c_1

c_1

Rest of Diffie-Hellman → sk_1

Ratchet forward sk_1 → sk_2

Ratchet forward sk_1 → sk_2

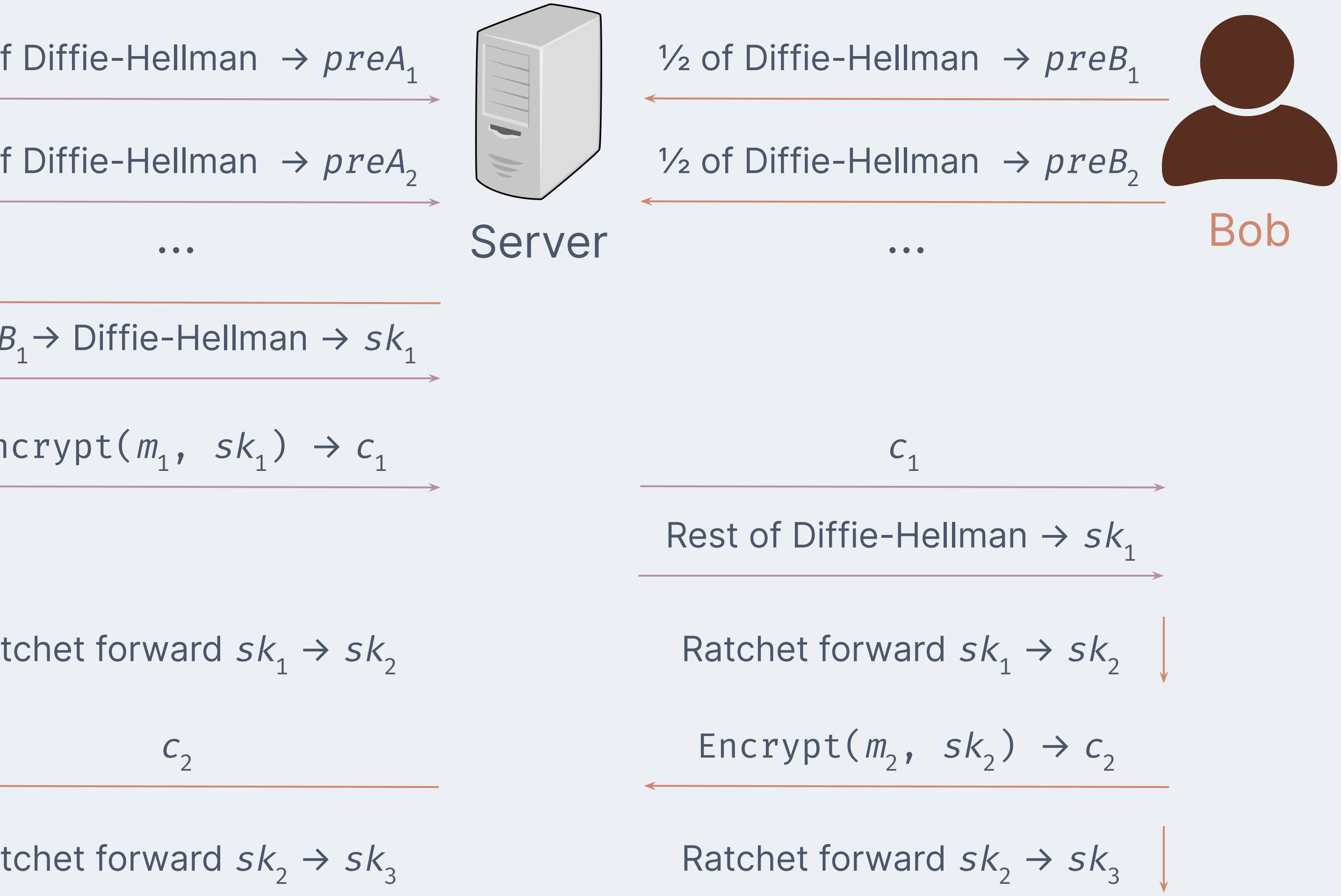
c_2

Encrypt(m_2, sk_2) → c_2

Ratchet forward sk_2 → sk_3

Ratchet forward sk_2 → sk_3

The loss of one key doesn’t leak previous ones → forward secrecy



f Diffie-Hellman → $preA_1$

½ of Diffie-Hellman → $preB_1$

f Diffie-Hellman → $preA_2$

½ of Diffie-Hellman → $preB_2$

…

Server

…

Bob

B_1 → Diffie-Hellman → sk_1

ncrypt(m_1, sk_1) → c_1

c_1

Rest of Diffie-Hellman → sk_1

tchet forward sk_1 → sk_2

Ratchet forward sk_1 → sk_2

c_2

Encrypt(m_2, sk_2) → c_2

tchet forward sk_2 → sk_3

Ratchet forward sk_2 → sk_3

Sidebar

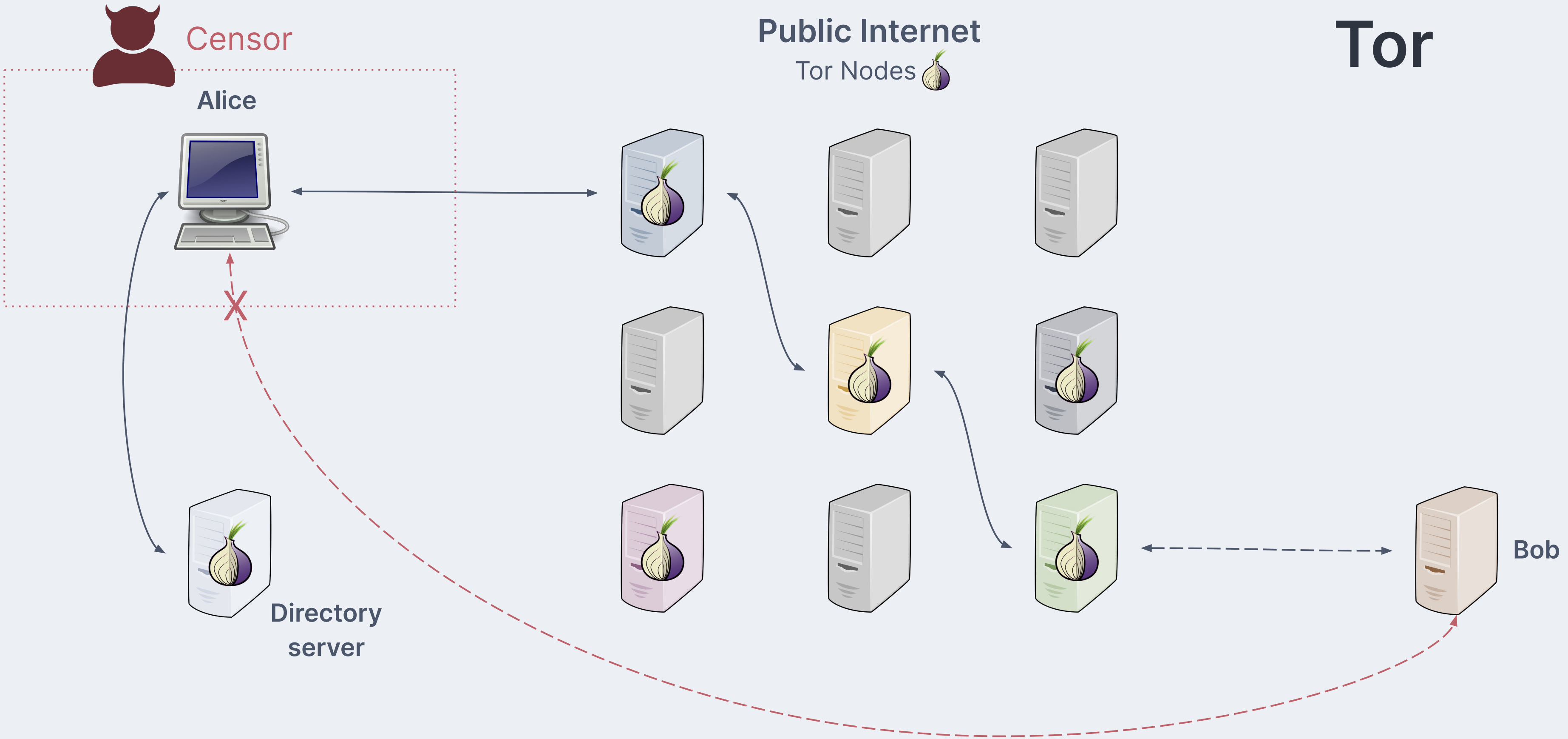
- Not a trivial protocol
- Complicated to provide forward secrecy, limited interaction, and efficiency
- Good example of security engineering in practice
- Needs to be usable in practice

Censorship resistance

- Some users live under regimes with authoritarian Internet policies
- They are forbidden from accessing content that the government deems subversive
  - A government's "subversive content" could be a group's "civil rights protest"
- A system like Signal prevents direct observation of content by governments
  - So, the Signal server is blocked by an authoritarian government

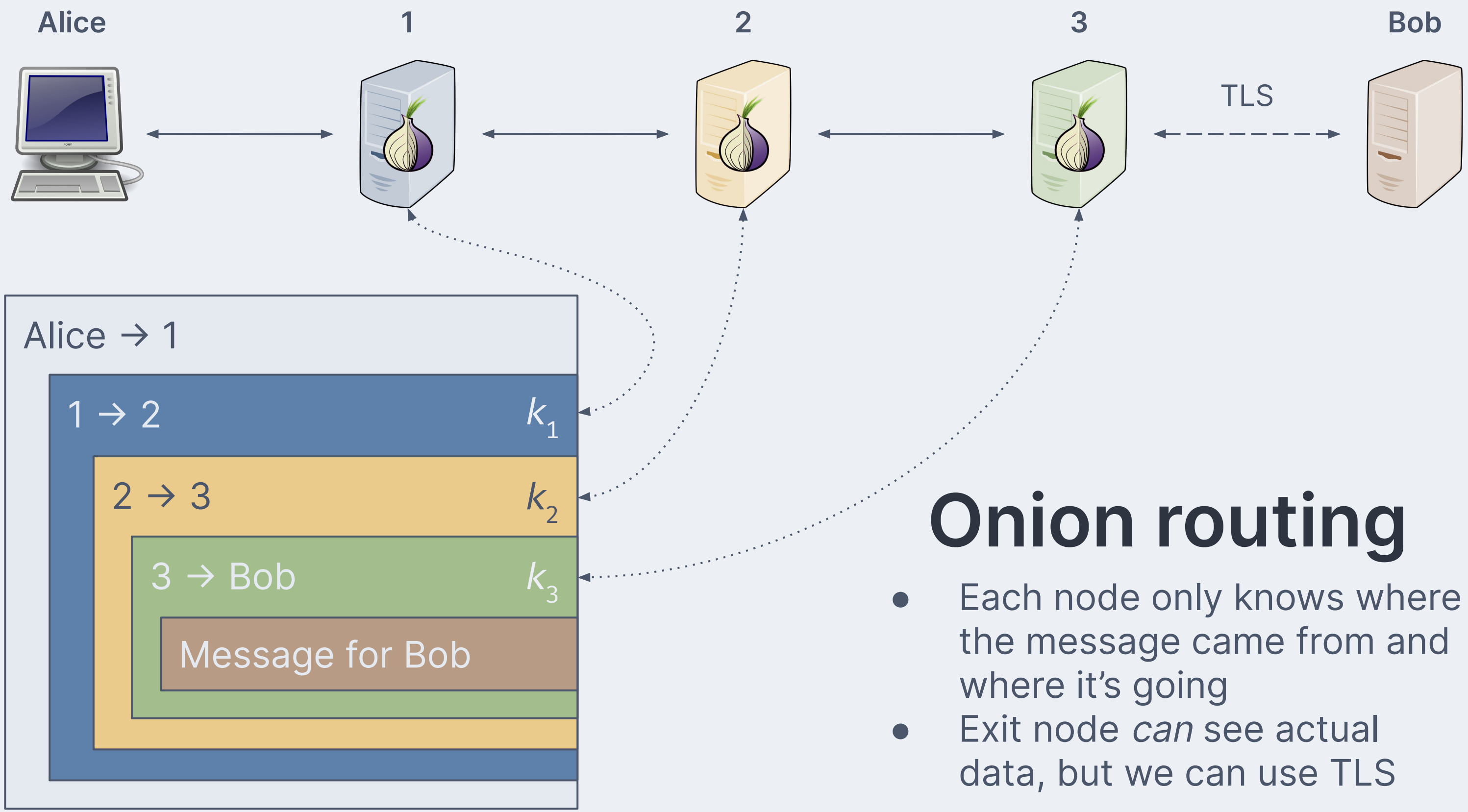
- What if we decided that *all* users should be able to access any content*?*
  - This choice lies in opposition to the existence of censorship
  - Society gets to decide which values we keep
- So, there's a valid use case for technology that combats censorship

Tor

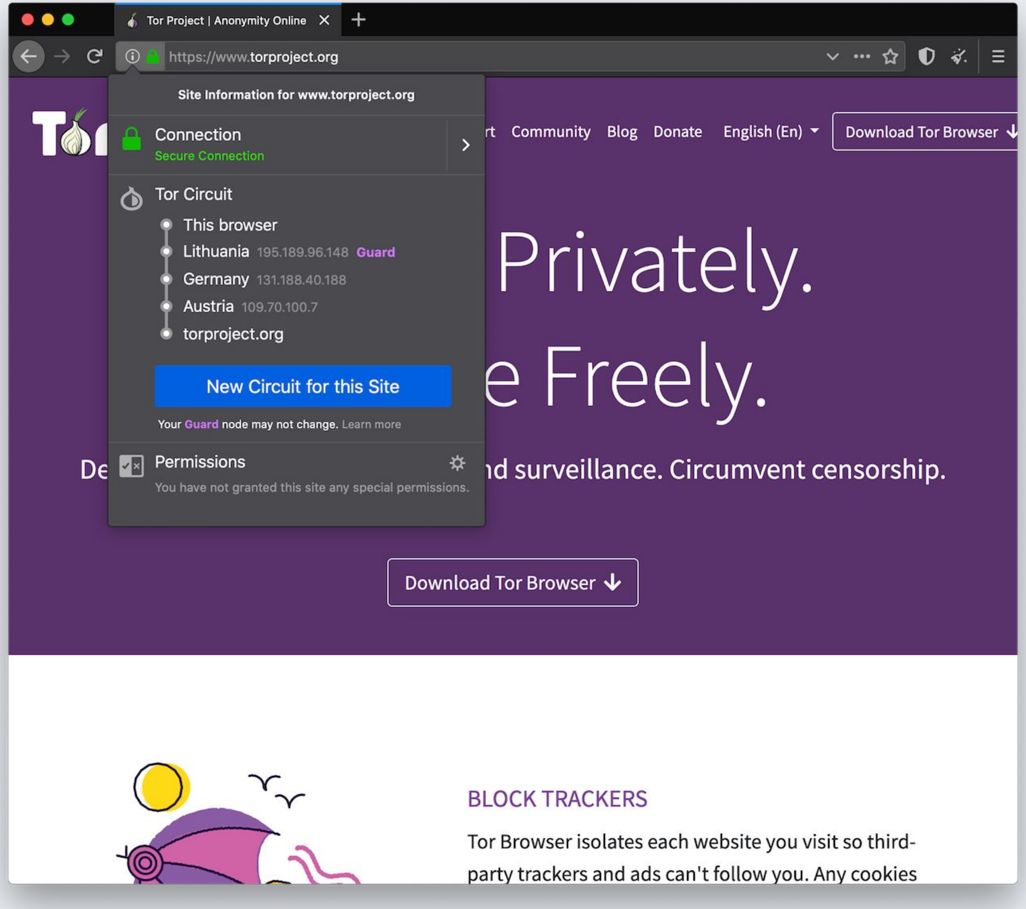

Censor
Public Internet
Tor Nodes
Alice
Directory server
Bob

Onion routing

Tor Circuit



- Each node only knows where the message came from and where it’s going
- Exit node *can* see actual data, but we can use TLS



Tor Project | Anonymity Online
https://www.torproject.org
rt
Community
Blog
Donate
English (En)
Download Tor Browser
New Circuit for this Site
Download Tor Browser

Site Information for www.torproject.org

Connection
Secure Connection

Tor Circuit

- This browser
- Lithuania 195.189.96.148 Guard
- Germany 131.188.40.188
- Austria 109.70.100.7
- torproject.org

Your Guard node may not change. Learn more

Permissions
You have not granted this site any special permissions.

Privately.

e Freely.

De … nd surveillance. Circumvent censorship.

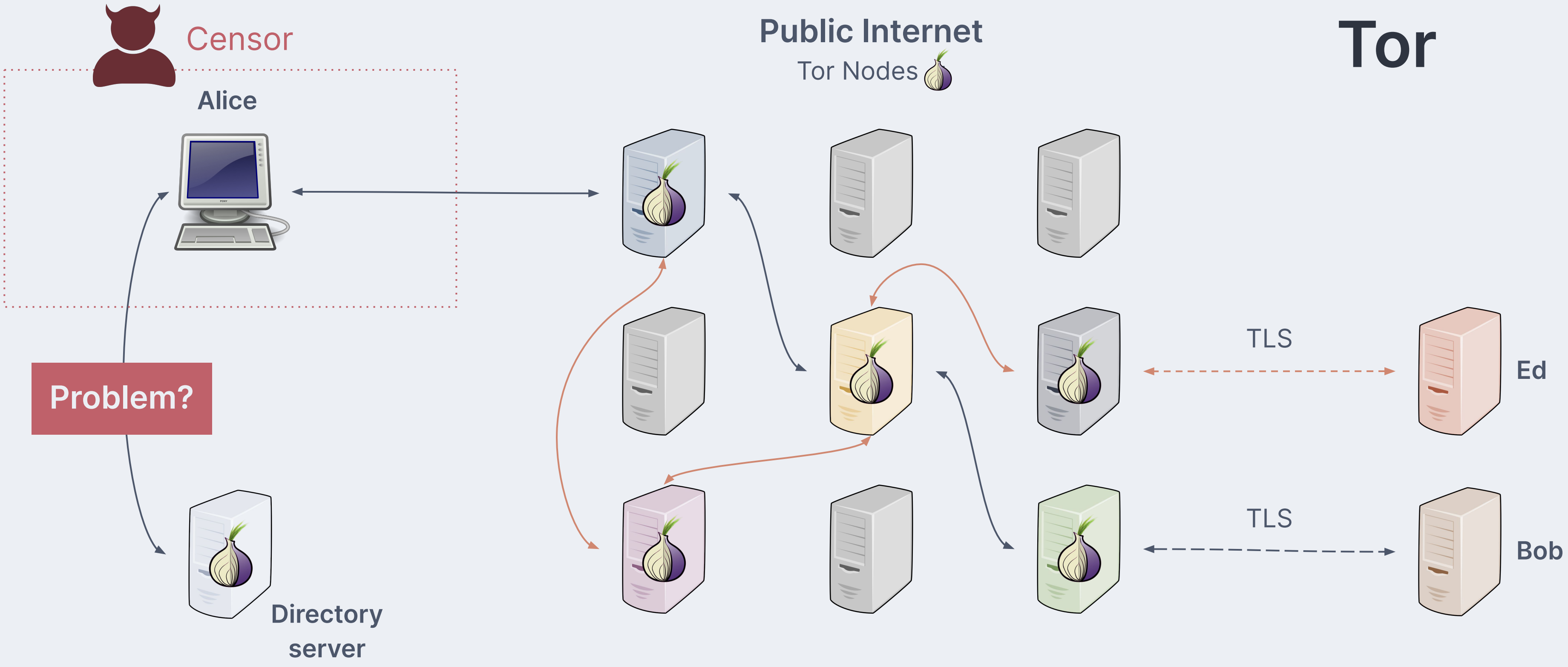
BLOCK TRACKERS

Tor Browser isolates each website you visit so third-party trackers and ads can't follow you. Any cookies

Some thoughts on Tor

- Trusting Tor
  - Tor is another system we have to trust
  - Funded by lots of people (incl. US) but mostly written by volunteers (open source)
- Virtual Private Networks and Tor
  - VPNs are similar to Tor (having another computer request traffic for you)
  - No guarantees that a VPN will not read/store/log your actions
    - VPNs claim terms of use, audits, etc but no formal promises
    - Tor has cryptographic guarantees (encrypted traffic)
- Exit nodes on Tor
  - Exit node needs to see your data to perform a web request
  - Can potentially break your privacy, but also can use TLS
- But, there's a more fundamental problem...

Tor



Censor

Alice

Problem?

Directory server

Public Internet

Tor Nodes

TLS

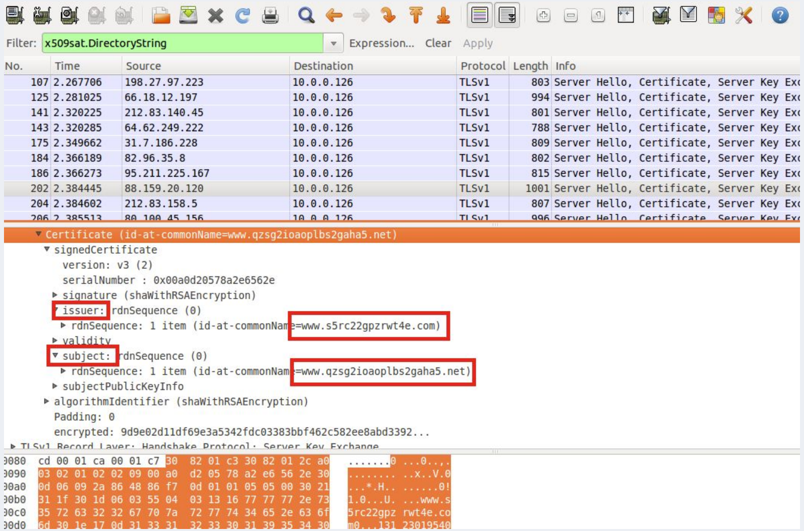
Ed

TLS

Bob

Censoring censorship resistance

- Censor can clearly identify traffic that’s going to a Tor network
    - Single point of failure: directory server
    - Block access to directory server → block access to Tor
    - China’s “Great Firewall” does this
- Use of Tor could endanger your life
    - Protestors/dissidents/whistleblowers
    - Still need to access free communication



Filter: x509sat.DirectoryString

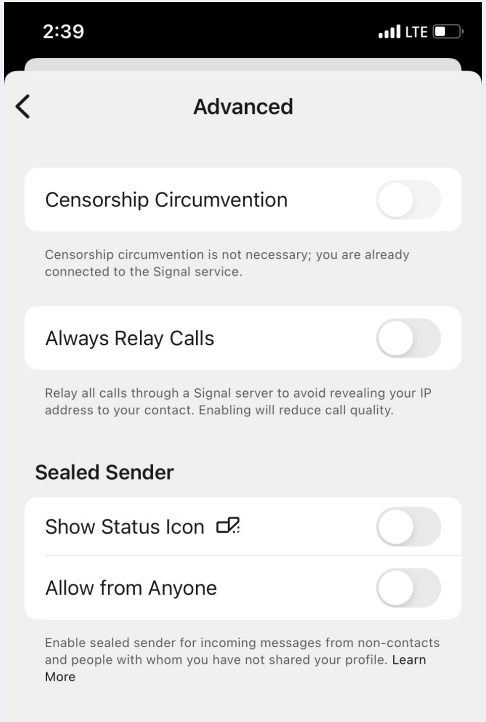
```
No.  Time      Source           Destination  Protocol Length Info
 107 2.267706  198.27.97.223    10.0.0.126   TLSv1       803 Server Hello, Certificate, Server Key Exc
 125 2.281025  66.18.12.197     10.0.0.126   TLSv1       994 Server Hello, Certificate, Server Key Exc
 141 2.320225  212.83.140.45    10.0.0.126   TLSv1       801 Server Hello, Certificate, Server Key Exc
 143 2.320285  64.62.249.222    10.0.0.126   TLSv1       788 Server Hello, Certificate, Server Key Exc
 175 2.349662  31.7.186.228     10.0.0.126   TLSv1       809 Server Hello, Certificate, Server Key Exc
 184 2.366189  82.96.35.8       10.0.0.126   TLSv1       802 Server Hello, Certificate, Server Key Exc
 186 2.366273  95.211.225.167   10.0.0.126   TLSv1       815 Server Hello, Certificate, Server Key Exc
 202 2.384445  88.159.20.120    10.0.0.126   TLSv1      1001 Server Hello, Certificate, Server Key Exc
 204 2.384602  212.83.158.5     10.0.0.126   TLSv1       807 Server Hello, Certificate, Server Key Exc
 206 2.385513  80.100.45.156    10.0.0.126   TLSv1       996 Server Hello, Certificate, Server Key Exc
```

```
▼ Certificate (id-at-commonName=www.qzsg2ioaoplbs2gaha5.net)
  ▼ signedCertificate
      version: v3 (2)
      serialNumber : 0x00a0d20578a2e6562e
    ▶ signature (shaWithRSAEncryption)
    ▼ issuer: rdnSequence (0)
      ▶ rdnSequence: 1 item (id-at-commonName=www.s5rc22gpzrwt4e.com)
    ▶ validity
    ▼ subject: rdnSequence (0)
      ▶ rdnSequence: 1 item (id-at-commonName=www.qzsg2ioaoplbs2gaha5.net)
    ▶ subjectPublicKeyInfo
  ▶ algorithmIdentifier (shaWithRSAEncryption)
    Padding: 0
    encrypted: 9d9e02d11df69e3a5342fdc03383bbf462c582ee8abd3392...
▶ TLSv1 Record Layer: Handshake Protocol: Server Key Exchange
```

```
0080  cd 00 01 ca 00 01 c7 30  82 01 c3 30 82 01 2c a0   .......0 ...0..,.
0090  03 02 01 02 02 09 00 a0  d2 05 78 a2 e6 56 2e 30   ........ ..x..V.0
00a0  0d 06 09 2a 86 48 86 f7  0d 01 01 05 05 00 30 21   ...*.H.. ......0!
00b0  31 1f 30 1d 06 03 55 04  03 13 16 77 77 77 2e 73   1.0...U. ...www.s
00c0  35 72 63 32 32 67 70 7a  72 77 74 34 65 2e 63 6f   5rc22gpz rwt4e.co
00d0  6d 30 1e 17 0d 31 33 31  32 33 30 31 39 35 34 30   m0...131 23019540
```

Society

- Signal and Tor banned in several countries
  - Brittle censorship circumvention
  - Make messages look like other messages -- steganography
- “Going Dark”
  - FBI’s initiative to reduce prevalence of end-to-end encryption
- EARN IT Act (2020)
  - Providers that provide end-to-end encrypted messaging must monitor messages for CSAM
  - Defeats end-to-end protections in the name of detecting abuse
  - Horrible, abusive content -- but universal scanning might not be the answer
- The debate rages on



Censorship Circumvention ○

Censorship circumvention is not necessary; you are already connected to the Signal service.

Always Relay Calls ○

Relay all calls through a Signal server to avoid revealing your IP address to your contact. Enabling will reduce call quality.

Sealed Sender

Show Status Icon ○

Allow from Anyone ○

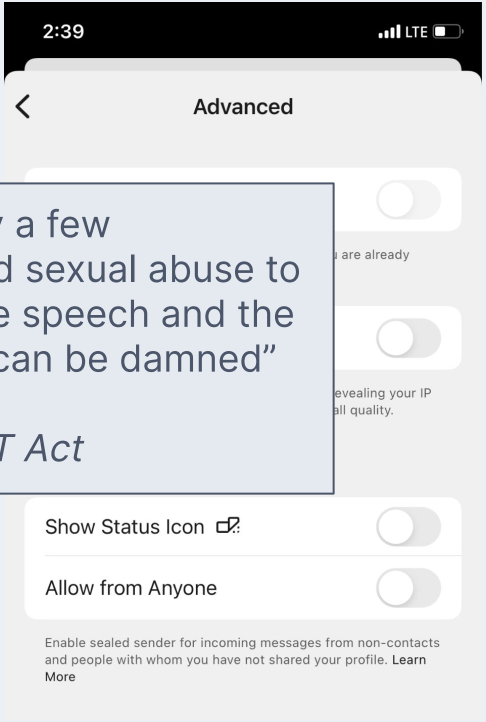
Enable sealed sender for incoming messages from non-contacts and people with whom you have not shared your profile. Learn More

Society

- Signal and Tor banned in several countries
  - Brittle censorship circumvention
  - Make messages look like other messages -- steganography
- "Going Dark"
  - FBI's initi
    end-to-e
- EARN IT Act (
  - Providers
    messagi
  - Defeats end-to-end protections in the name of detecting abuse
  - Horrible, abusive content -- but universal scanning might not be the answer
- The debate rages on

"a transparent and deeply cynical effort by a few well-connected corporations ... to use child sexual abuse to their political advantage, the impact to free speech and the security and privacy of every single American be damned"

Senator Ron Wyden (D-OR) on the EARN IT Act



u are already

evealing your IP
all quality.

Show Status Icon ○

Allow from Anyone ○

Enable sealed sender for incoming messages from non-contacts and people with whom you have not shared your profile. Learn More

Looking ahead

- Be reflective about your progress, and reach out if you need help
  - Key dates for the remainder of the semester
    - Apr 15: Project code due
    - Apr 16: Exam 2
    - May 7: Project demo day
    - May 14: Project presentations
  - Send an email with the subject “EE G7701 Exam 1 `[LastName]`” to get your exam back
- **Today’s activity**: personal privacy check-up lab

Lesson objectives

- Work through, step by step, the operation of the Signal protocol
- Describe how Tor uses onion routing to provide censorship resistance
- Understand the political and societal ramifications of privacy