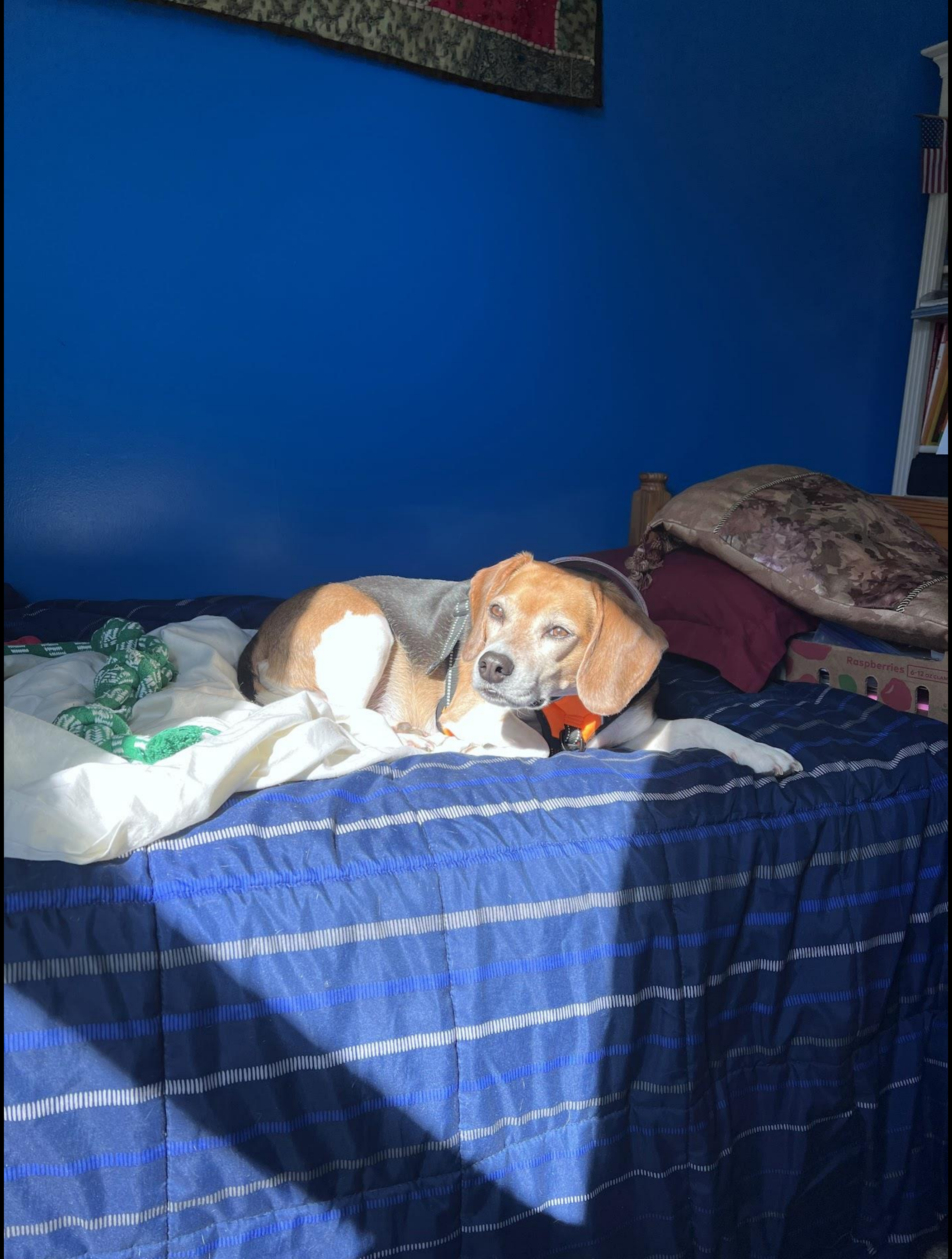
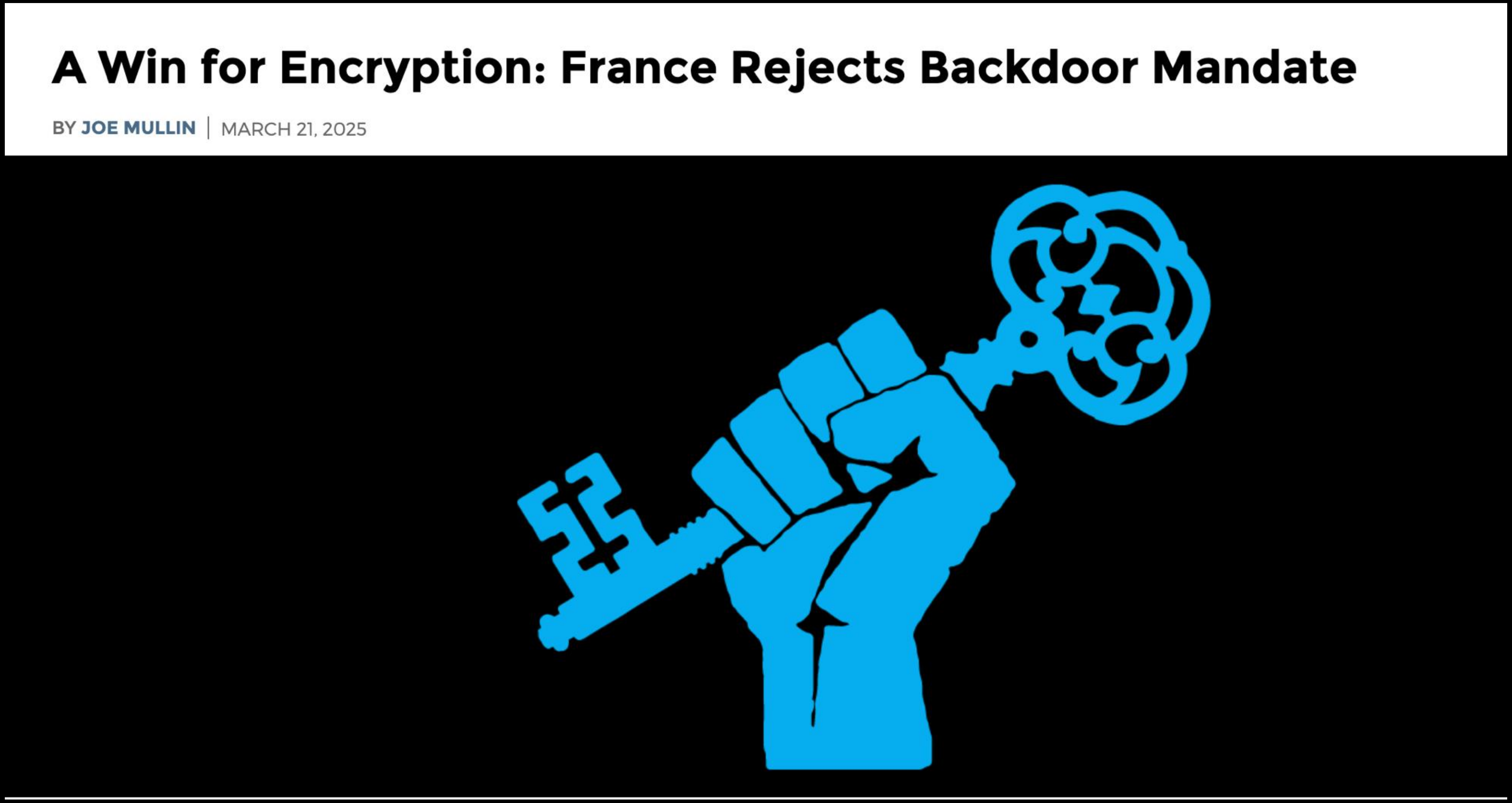
DS 593: Privacy in Practice

Systems for Privacy Cont’d

Instructor: Alishah Chator

News?





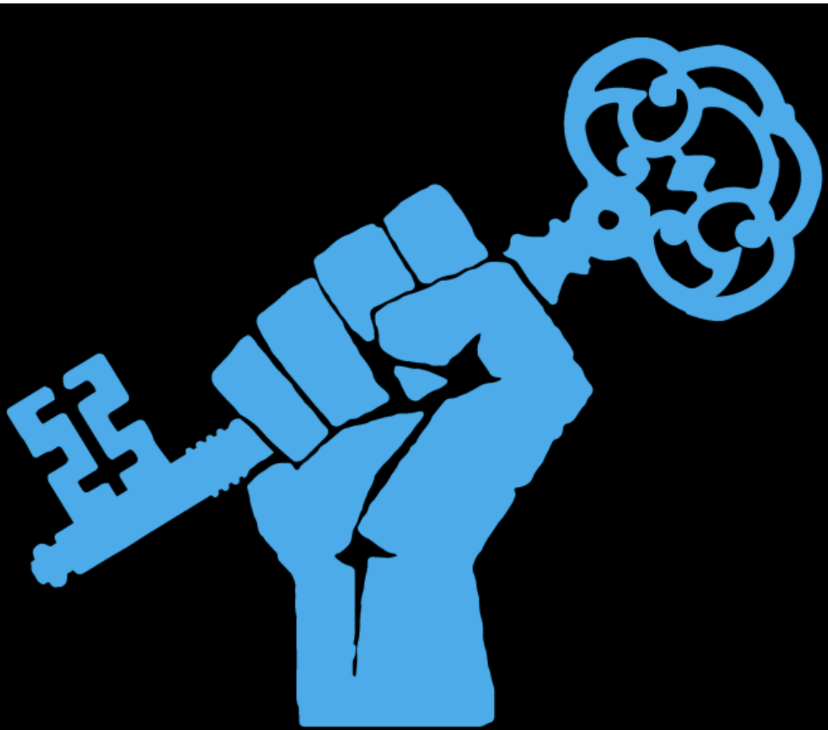
A Win for Encryption: France Rejects Backdoor Mandate

BY **JOE MULLIN** | MARCH 21, 2025

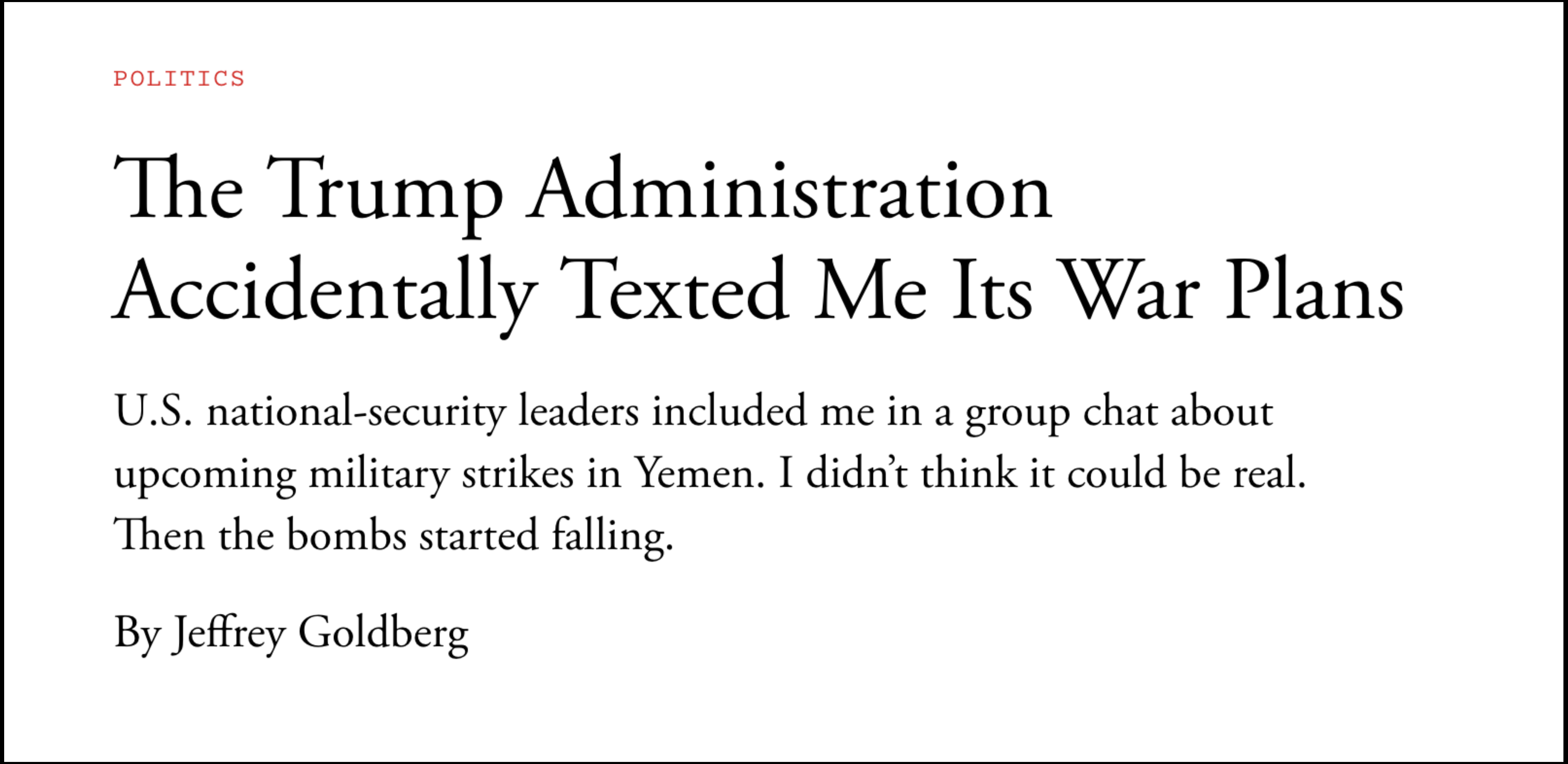
https://www.eff.org/deeplinks/2025/03/win-encryption-france-rejects-backdoor-mandate

Give Up the Ghost: A Backdoor by Another Name

BY NATE CARDOZO | JANUARY 7, 2019



https://www.eff.org/deeplinks/2019/01/give-ghost-backdoor-another-name



POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

By Jeffrey Goldberg

https://archive.ph/pmLkg

Last time

- How do we use these building blocks for privacy online?

Today

- How do we use these building blocks for privacy online?

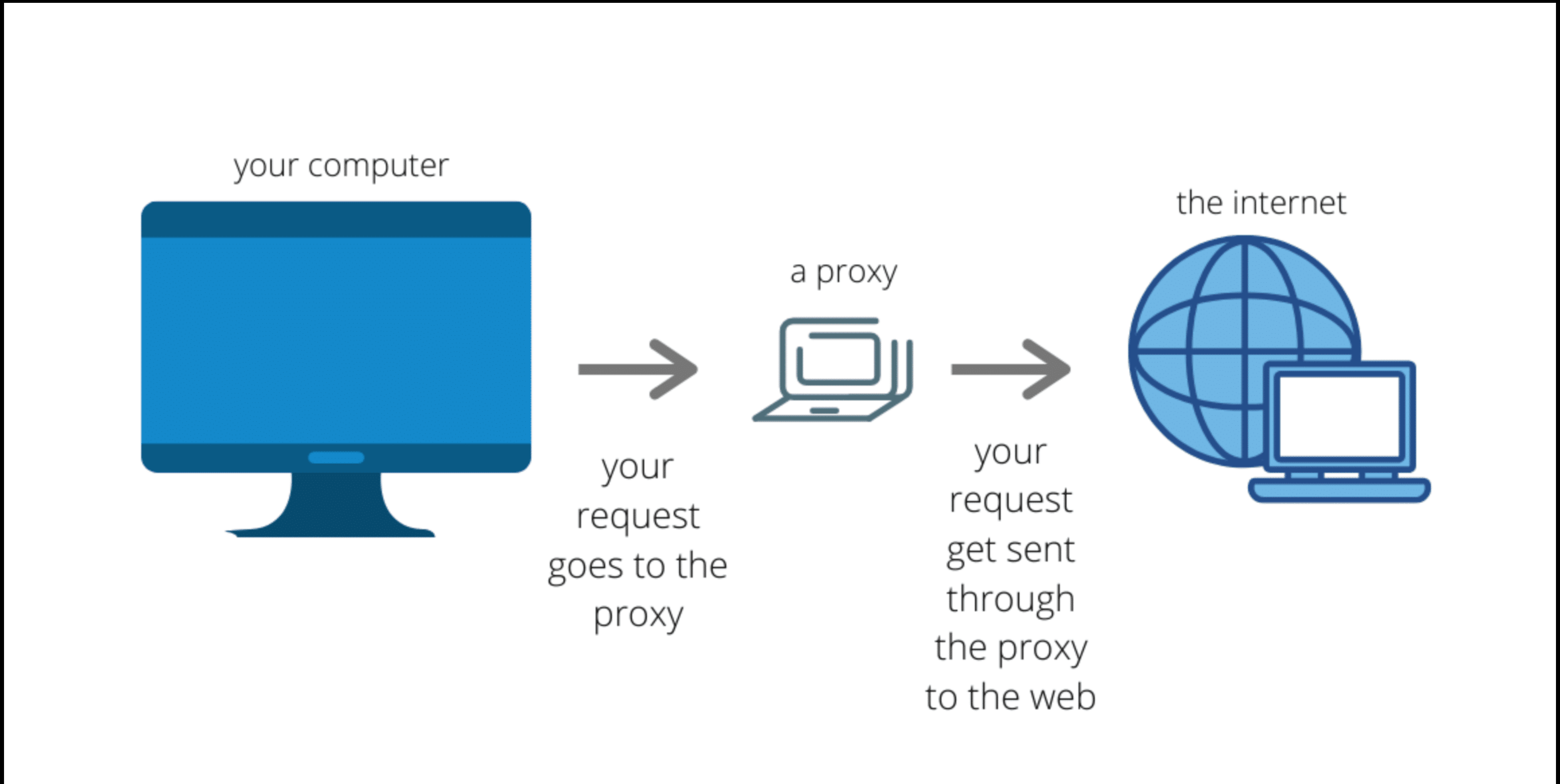
Virtual Private Networks (VPN)

- The internet is large public system with many intermediaries
  - Can we pretend it is actually just a small closed network of only the computers I care about or trust?

- Problem: how to hide my browsing from intermediaries between me and the ”private network?”
  - Proxying

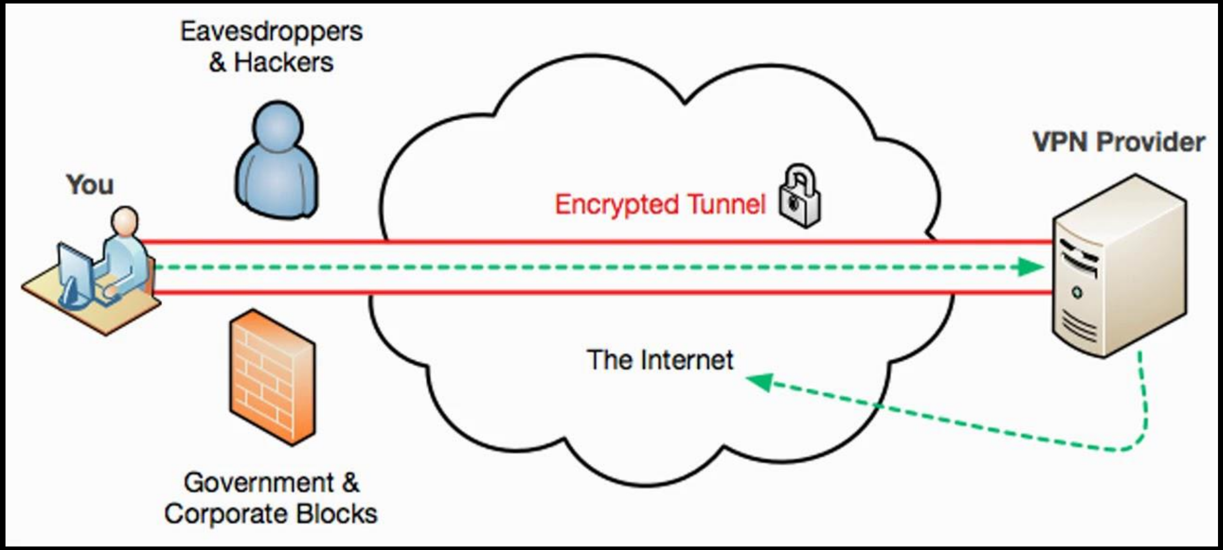
  - Tunneling

Web Proxy


your computer
your request goes to the proxy
a proxy
your request get sent through the proxy to the web
the internet

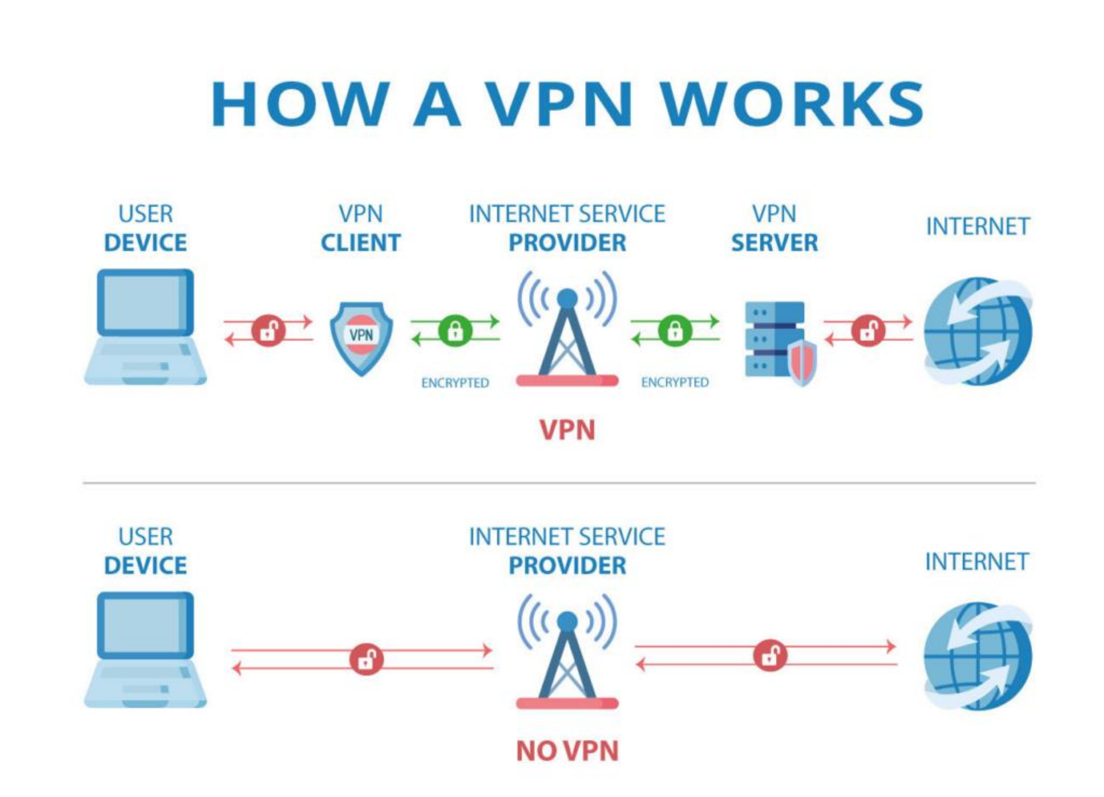
Tunneling

- A way to build a secure connection to a particular server
- You encapsulate your actual network packet in a packet that is sent to the desired server



- A VPN sets up a secure tunnel to a VPN server which then acts as a proxy to forward your packets to the internet

- Depending on the location of the VPN server, this can allow for bypassing censorship or geolocation restrictions

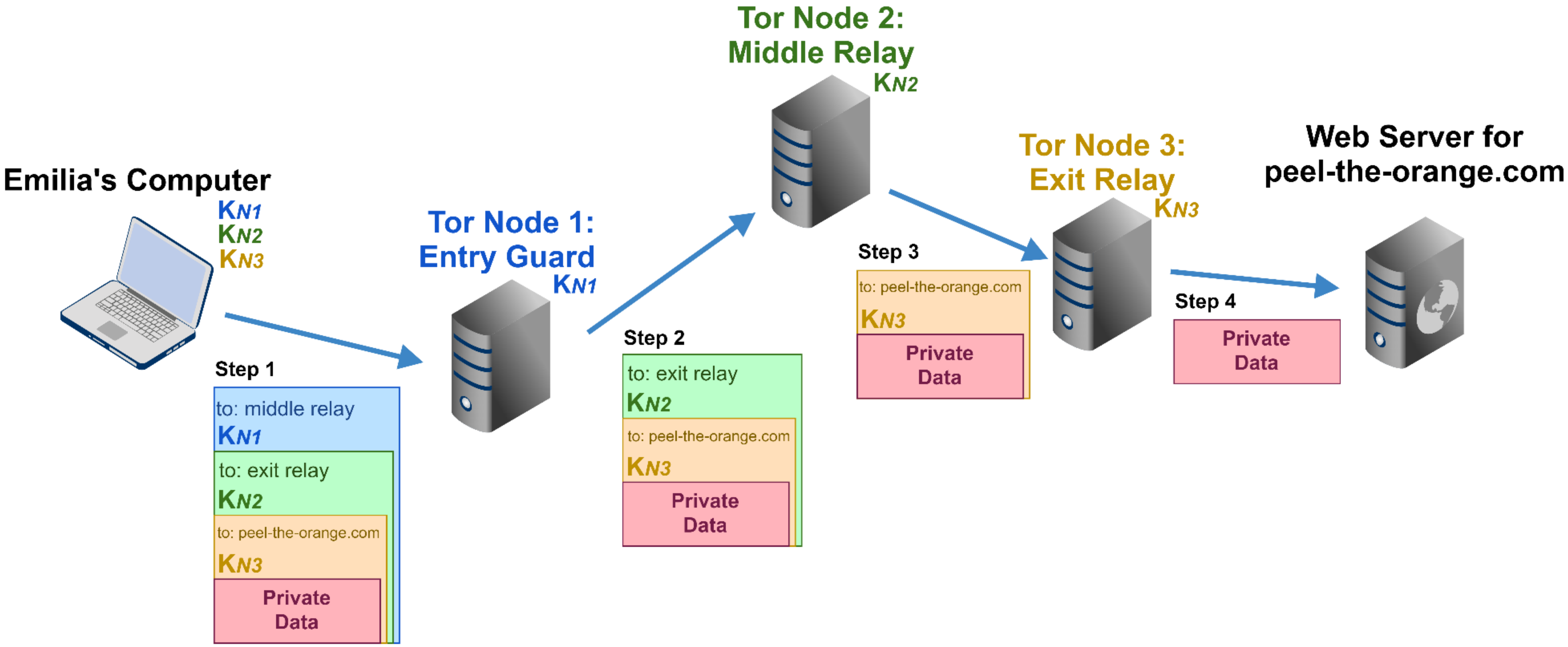


VPN Considerations

- Primarily hides your data from ISP
- The VPN server needs to be trusted
  - Learns your IP, your browsing data, etc
  - Could log all this
- VPN Servers are often publicly known and easy to identify
- Important to make sure all traffic goes through the VPN

The onion router (Tor)

- Goal is to provide a strong guarantee of hiding your browsing data in a robust and decentralized way
    - Mitigating limitations of VPNs
- Tor does this by adding multiple layers of encapsulation to ensure no single entity learns everything about your browsing



Emilia's Computer

K_{N1}
K_{N2}
K_{N3}

Step 1

to: middle relay
K_{N1}
to: exit relay
K_{N2}
to: peel-the-orange.com
K_{N3}
Private Data

Tor Node 1: Entry Guard

K_{N1}

Step 2

to: exit relay
K_{N2}
to: peel-the-orange.com
K_{N3}
Private Data

Tor Node 2: Middle Relay

K_{N2}

Step 3

to: peel-the-orange.com
K_{N3}
Private Data

Tor Node 3: Exit Relay

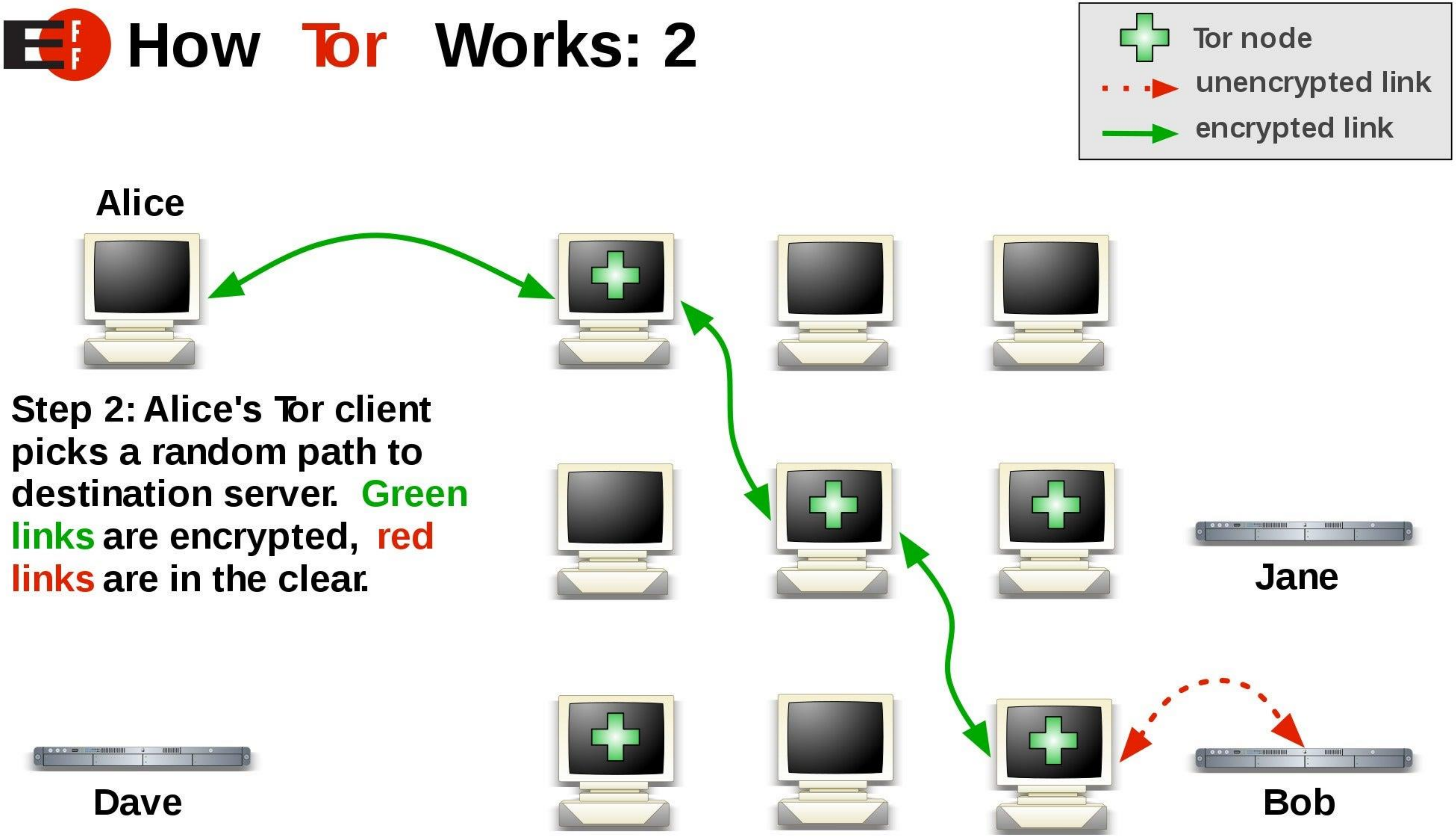
K_{N3}

Step 4

Private Data

Web Server for peel-the-orange.com

How Tor Works: 2



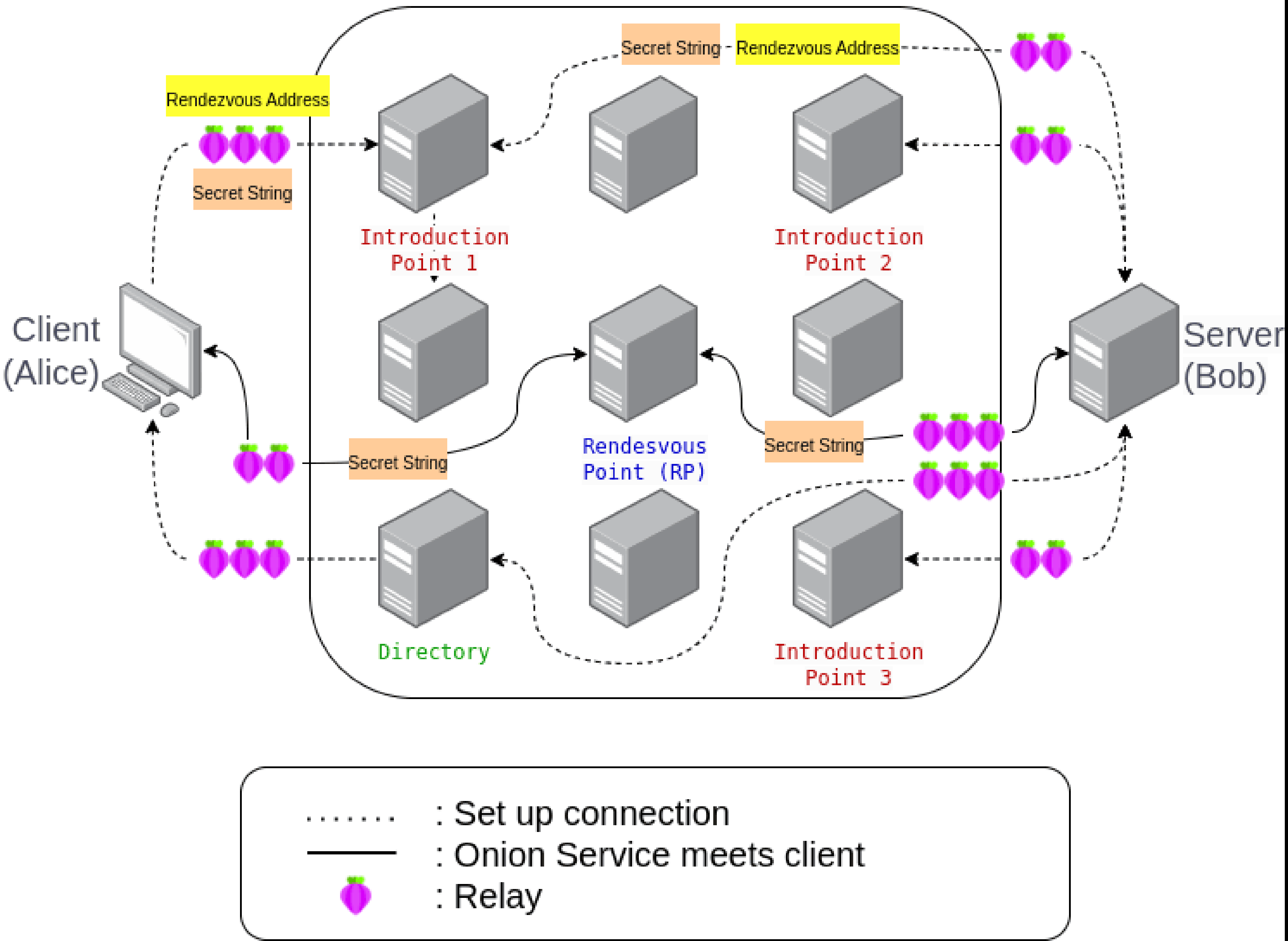
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

Other aspects of Tor

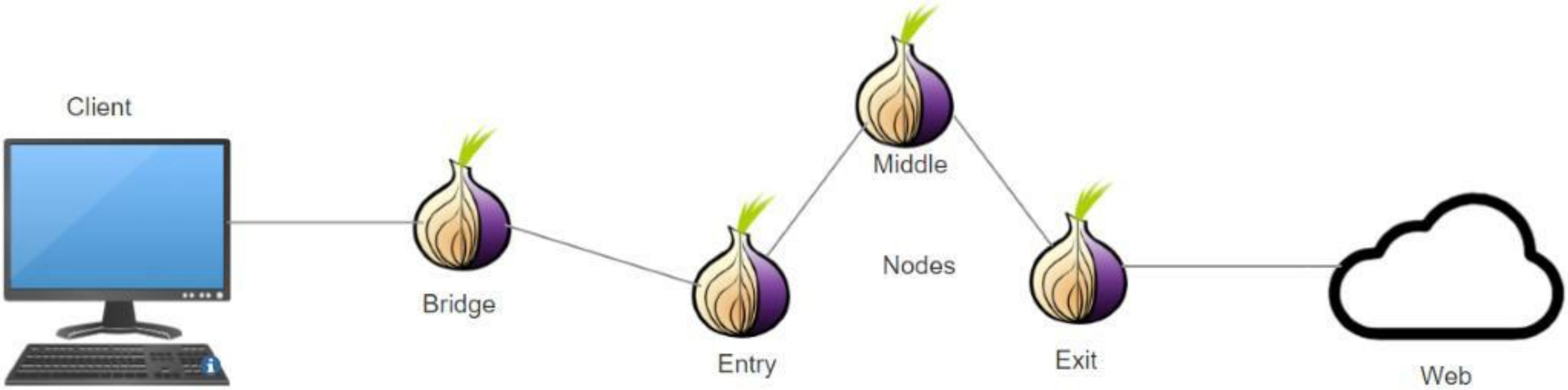
- Tor alone cannot bypass censorship as the relays can be blocked
  - Tor Bridges are a way to get around this

- Tor additionally has what are called hidden services, which can only be accessed within the Tor network

TOR Network


Rendezvous Address
Secret String
Secret String
Rendezvous Address
Introduction Point 1
Introduction Point 2
Client (Alice)
Server (Bob)
Rendesvous Point (RP)
Secret String
Secret String
Directory
Introduction Point 3
: Set up connection
: Onion Service meets client
: Relay

Tor Bridges



Tor considerations

- Possibility of leakage if multiple relays on your circuit are compromised
    - How to avoid this?

- Need to make sure you are using secure application layer protocols as well (ex: HTTPS)

- Crucial to keep your Tor and non-Tor logins separate

End to End Encryption (E2EE)

- So far we have focused on how to protect information as it passes through a network
- However, the end server may be able to see all of this
  - HTTPS only has data encrypted to and from the server
- E2EE is when the server only stores encrypted user data, *encrypted under a key that the server does not know*

Fig. 1a: Encryption in transit

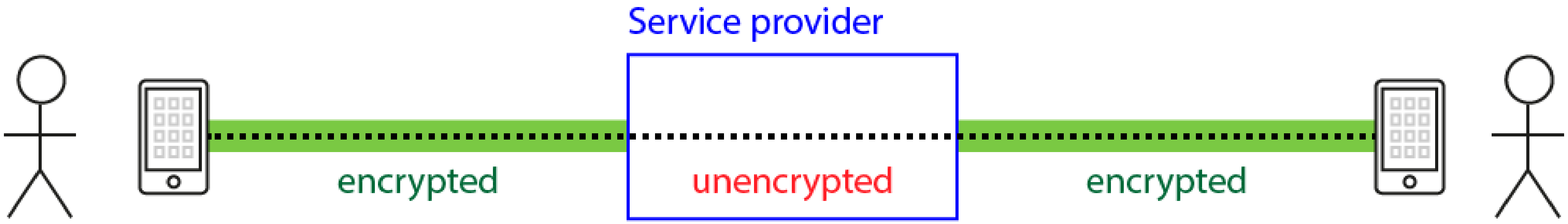


Fig. 1b: End-to-end encryption

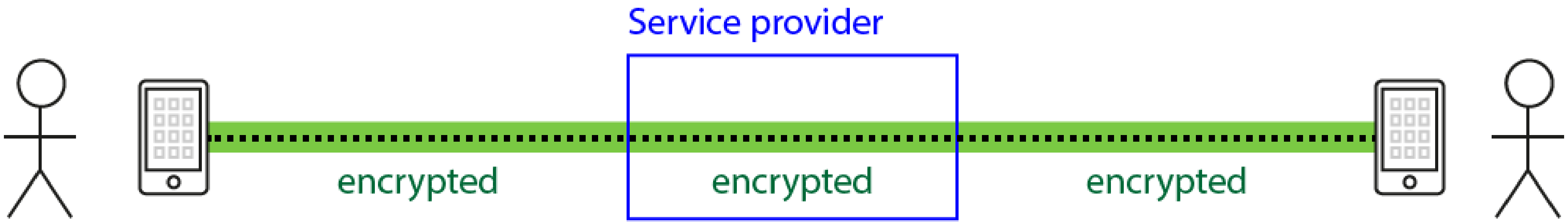
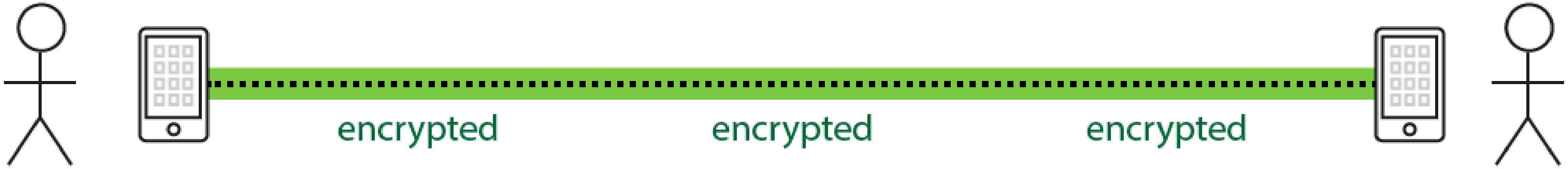
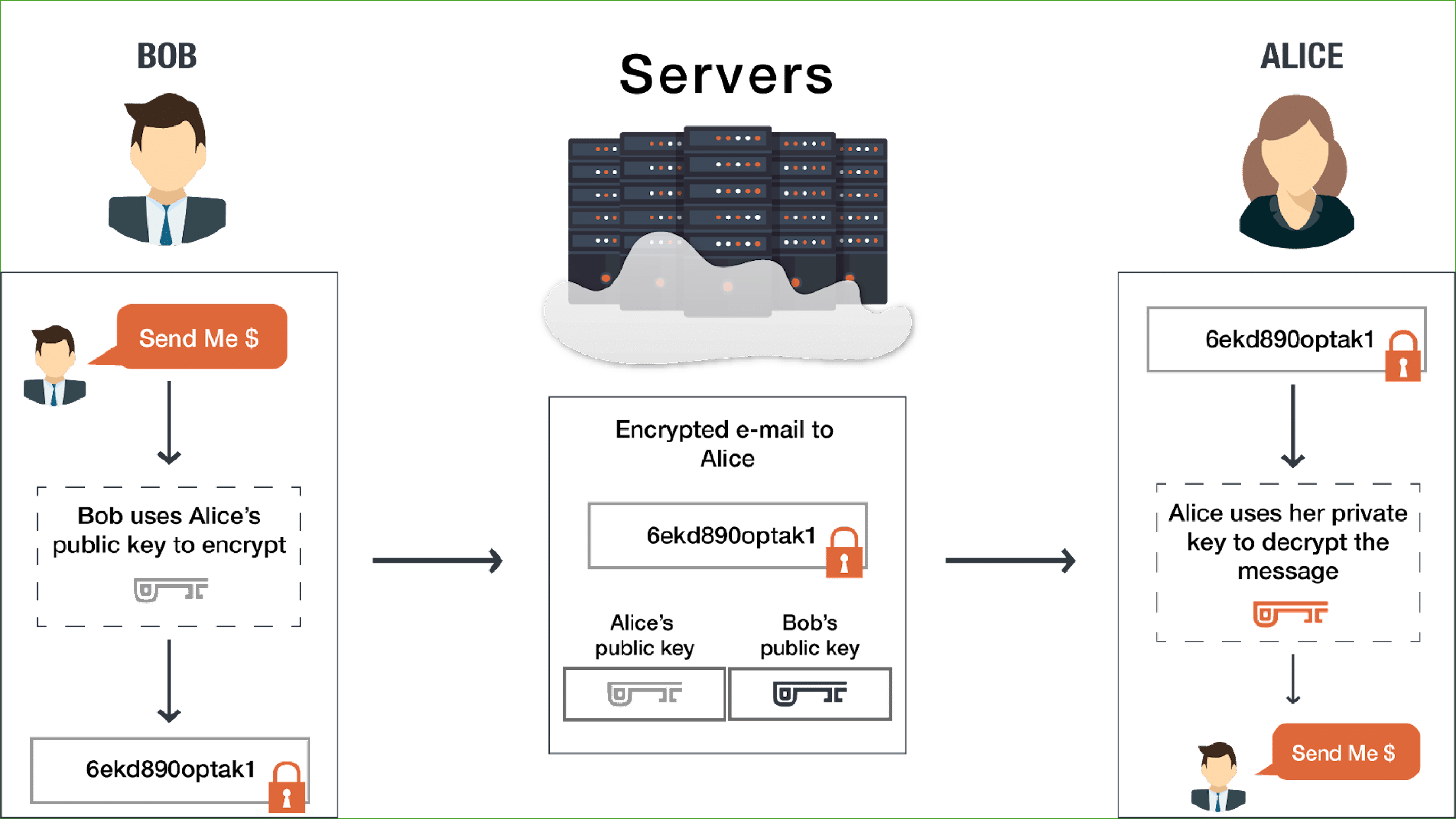


Fig. 1c: End-to-end encryption (no service provider)





BOB

Servers

ALICE

Send Me $

Bob uses Alice’s public key to encrypt

6ekd890optak1

Encrypted e-mail to Alice

6ekd890optak1

Alice’s public key

Bob’s public key

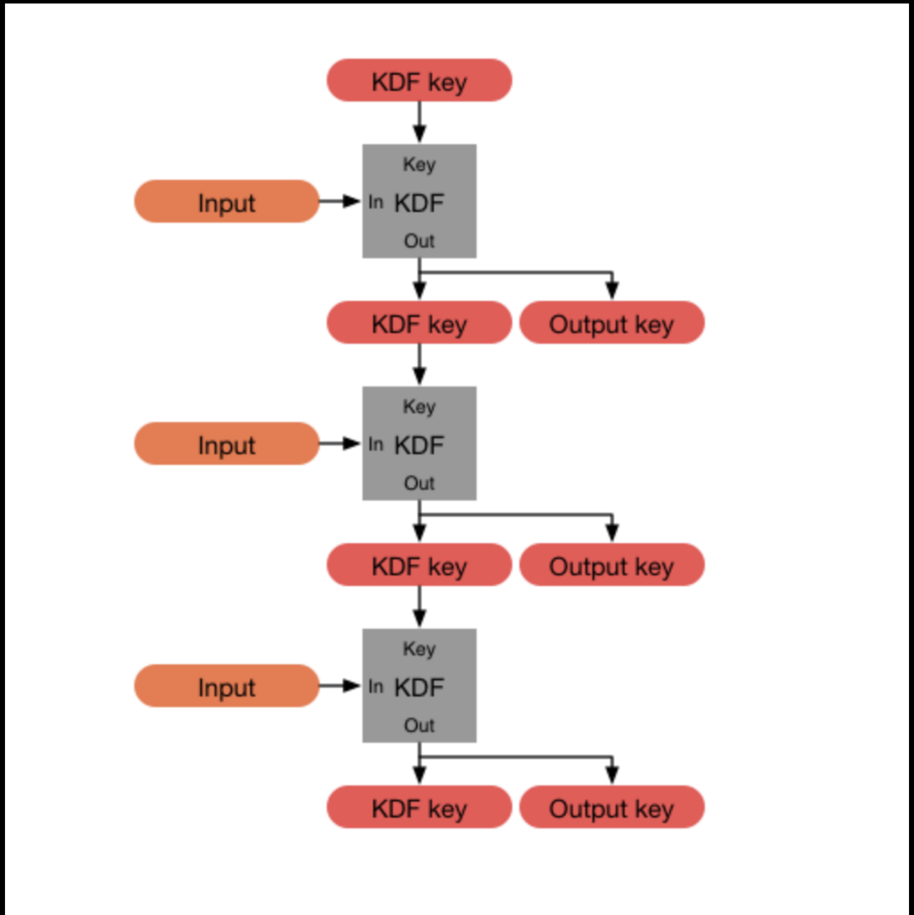
6ekd890optak1

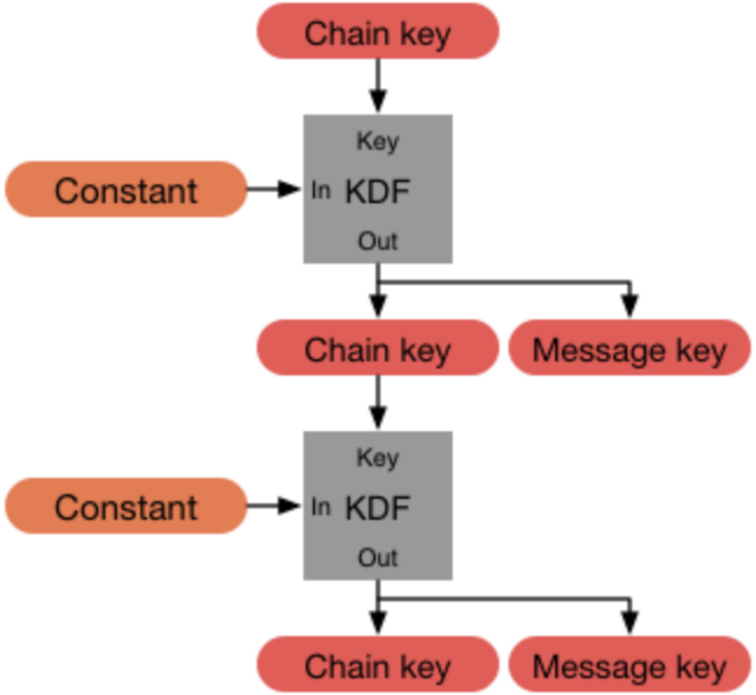
Alice uses her private key to decrypt the message

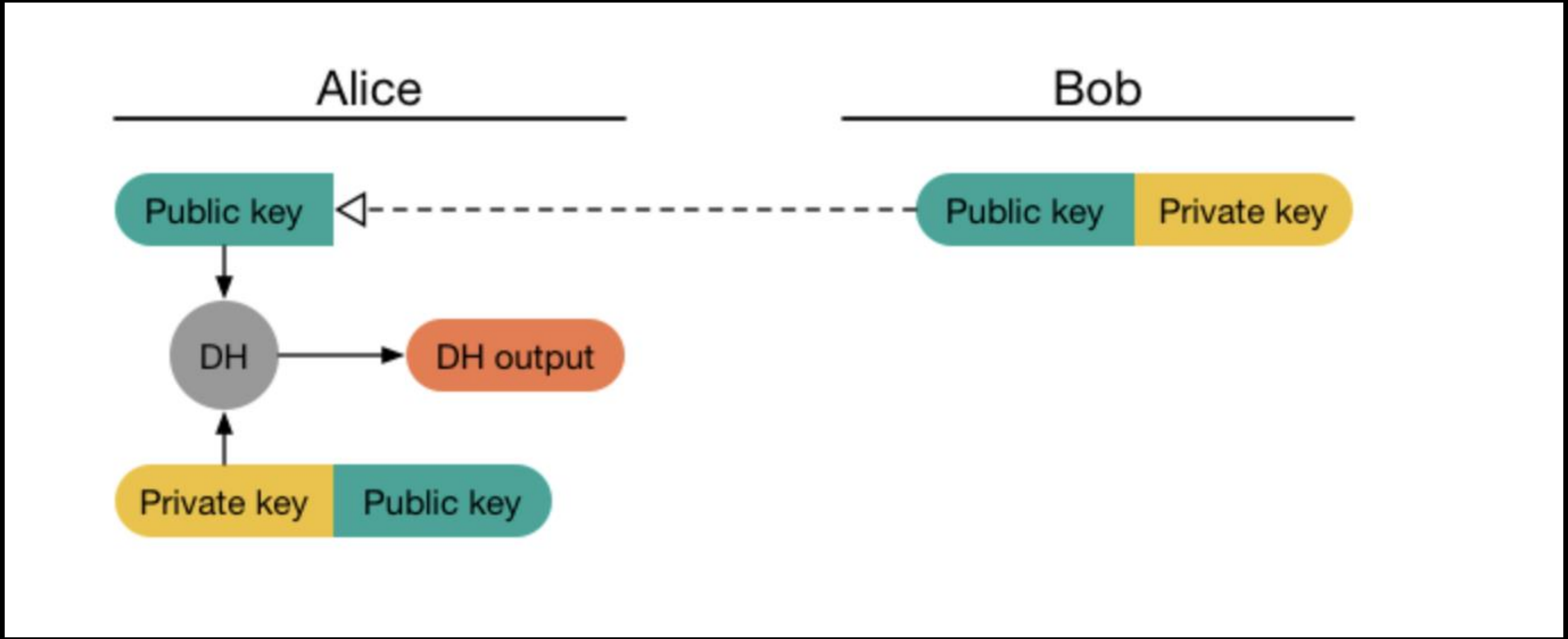
Send Me $

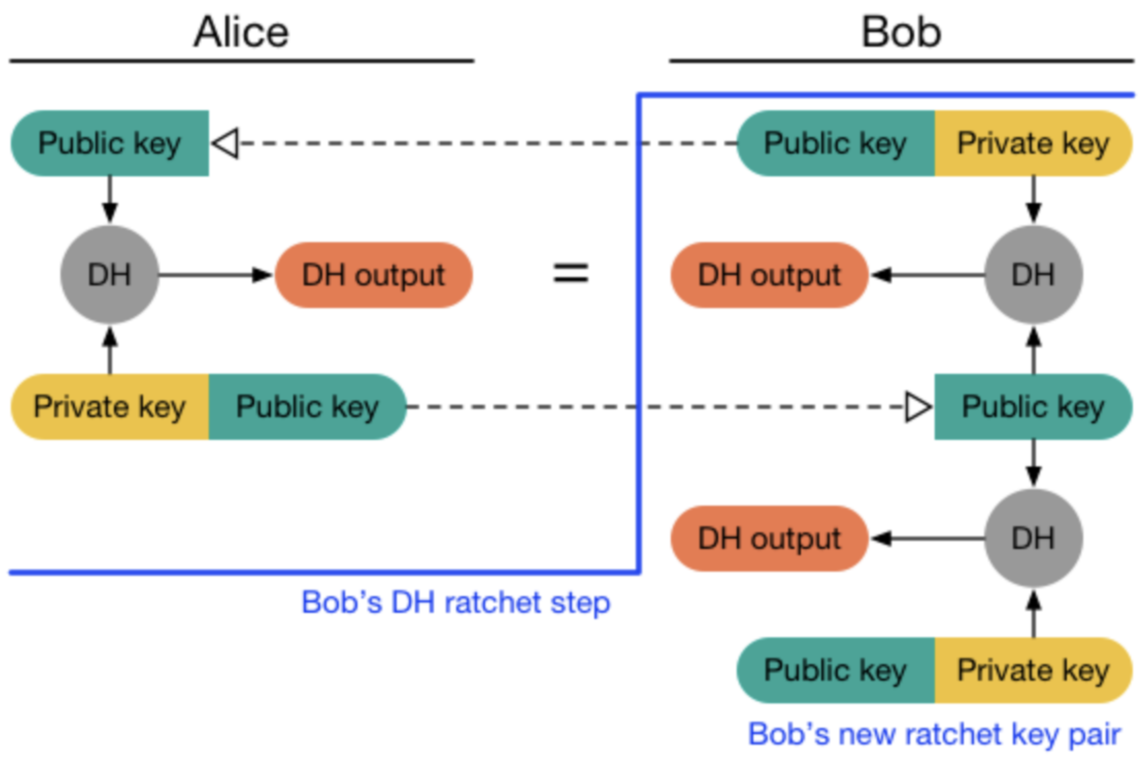
The Signal Protocol

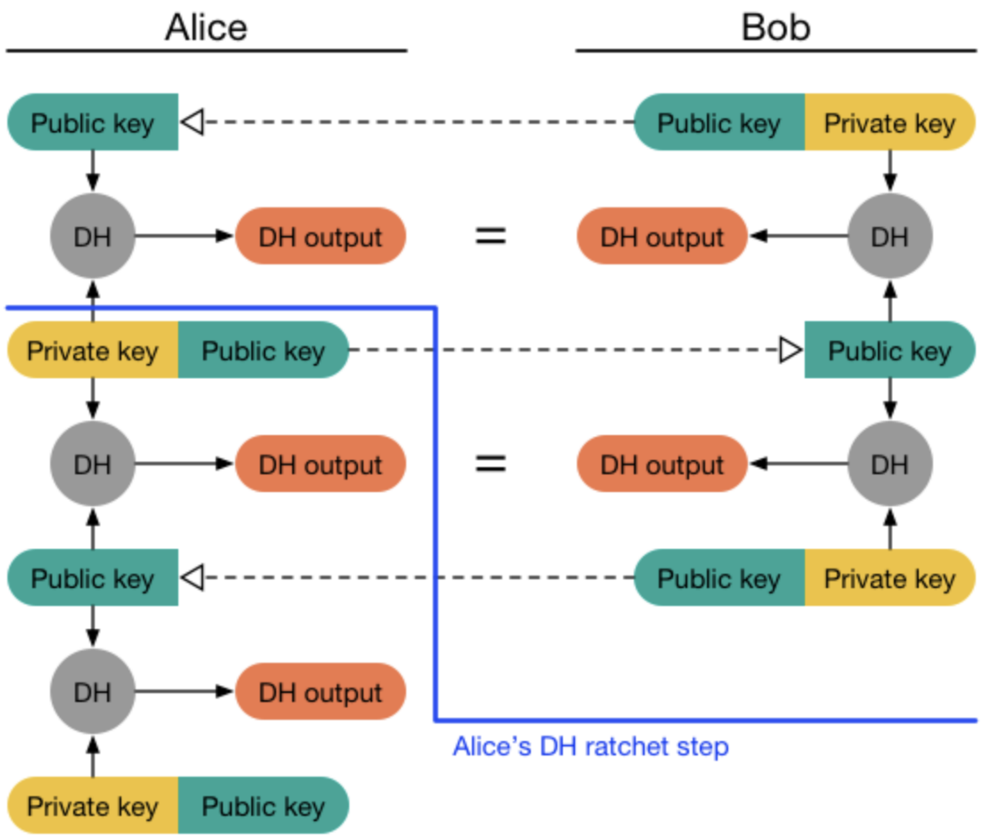
- A protocol for E2EE messaging
  - Also an open-source app
- Messages are only readable by the users in a chat through their device specific keys
  - Lose access to device -> loss access to messages
- Many other platforms such as Whatsapp, Messenger, use an implementation of the protocol as well
- Provides *forward* and *post-compromise* security
  - The Double Ratchet regularly changes the public keys and per-message symmetric keys used


KDF key
Key
Input
In
KDF
Out
KDF key
Output key
Key
Input
In
KDF
Out
KDF key
Output key
Key
Input
In
KDF
Out
KDF key
Output key


Chain key
Key
Constant
In
KDF
Out
Chain key
Message key
Key
Constant
In
KDF
Out
Chain key
Message key


Alice
Bob
Public key
Public key
Private key
DH
DH output
Private key
Public key


Alice
Bob
Public key
Public key
Private key
DH
DH output
=
DH output
DH
Private key
Public key
Public key
DH output
DH
Bob's DH ratchet step
Public key
Private key
Bob's new ratchet key pair


Alice
Bob
Public key
Public key
Private key
DH
DH output
=
DH output
DH
Private key
Public key
Public key
DH
DH output
=
DH output
DH
Public key
Public key
Private key
DH
DH output
Alice's DH ratchet step
Private key
Public key

Next Time

Defining Surveillance