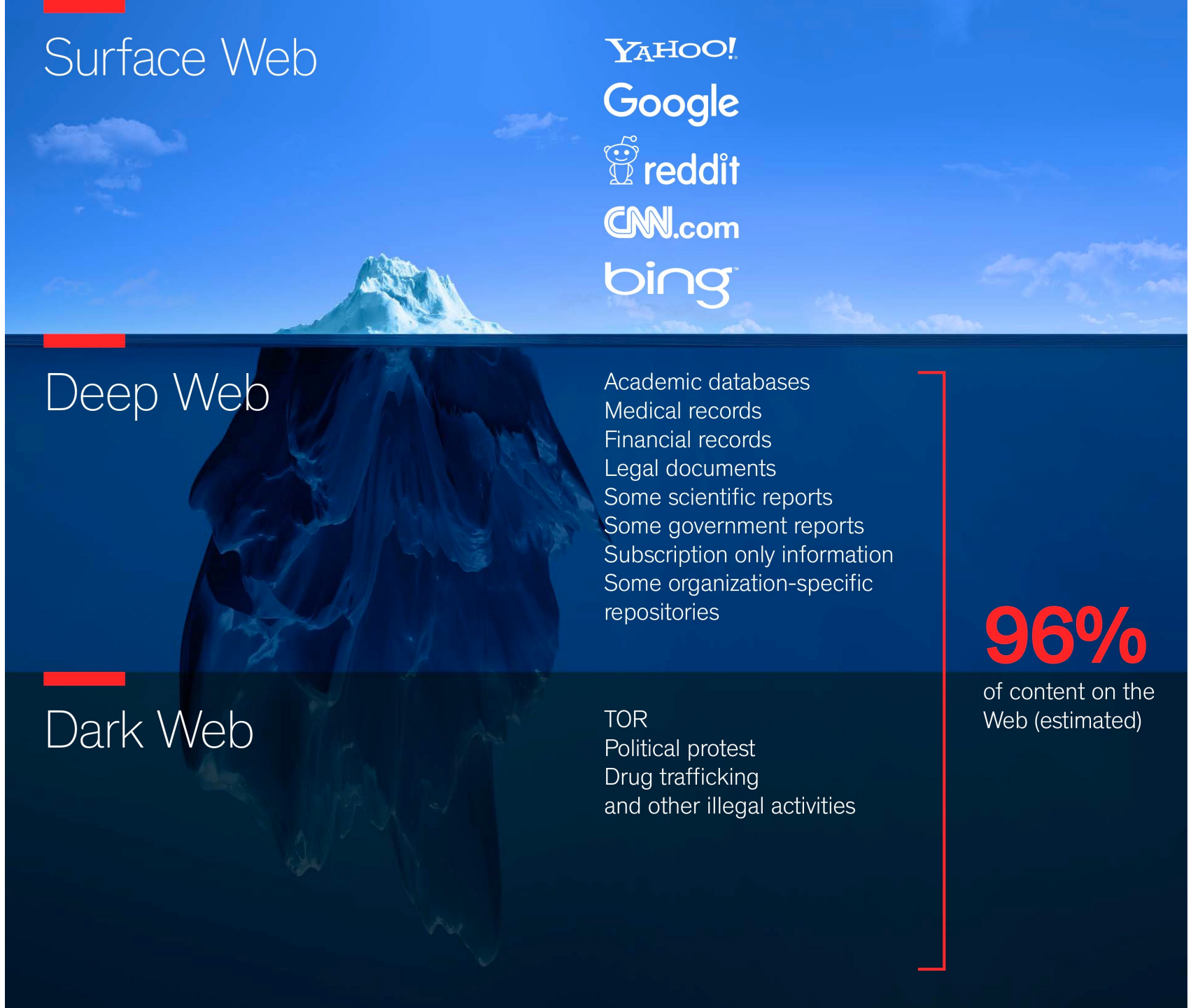
Lesson 07-02:
Network Security - Tor Hidden Service

CS 356 Computer Networks

Mikyung Han

mhan@cs.utexas.edu

Tor: Enabling Anonymous Communication Over the Internet

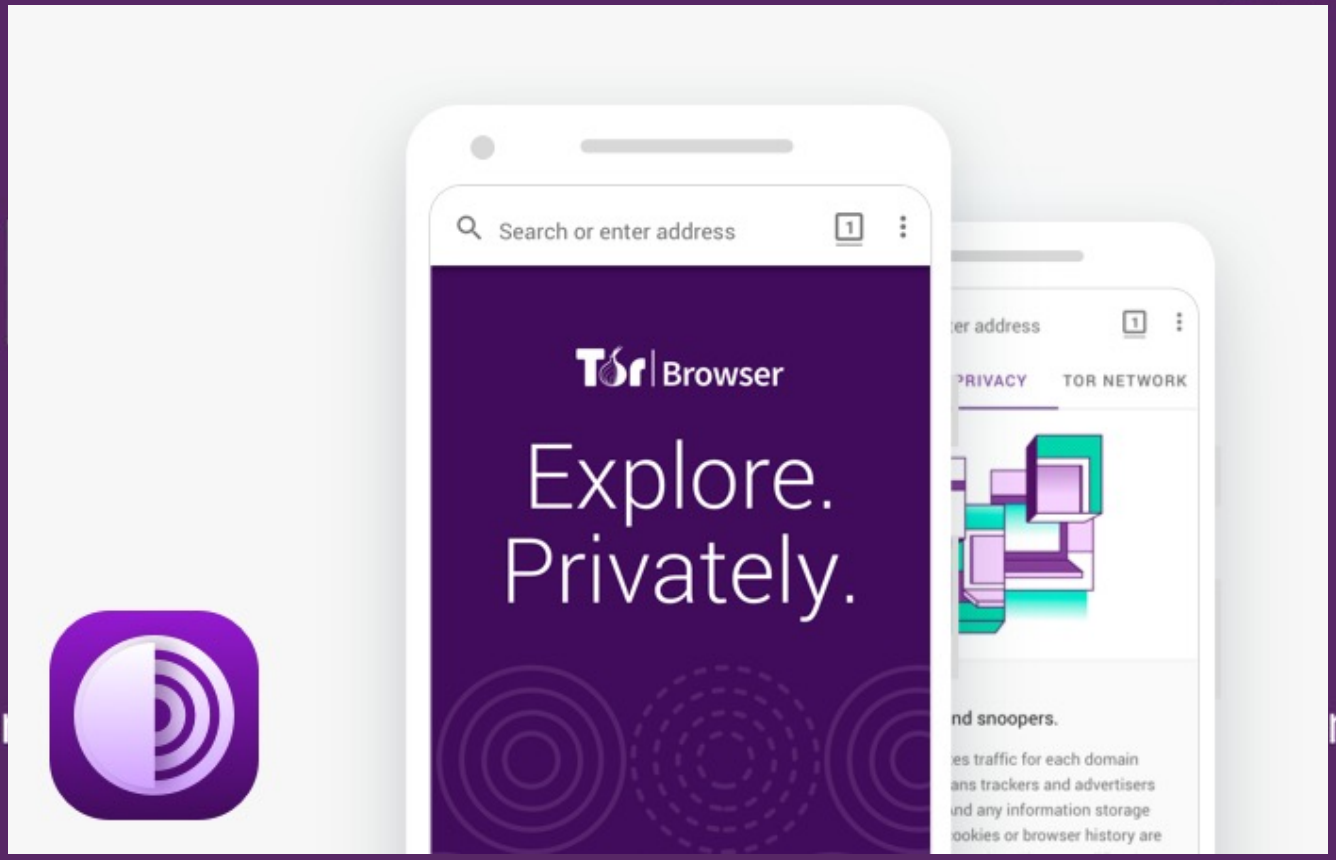

Surface Web
YAHOO!
Google
reddit
CNN.com
bing
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization-specific repositories
Dark Web
TOR
Political protest
Drug trafficking
and other illegal activities
96%
of content on the Web (estimated)

Tor Project | Anonymity Online

https://www.torproject.org

DONATE NOW

About Documentation Support Blog Donate English (En) Download Tor Browser



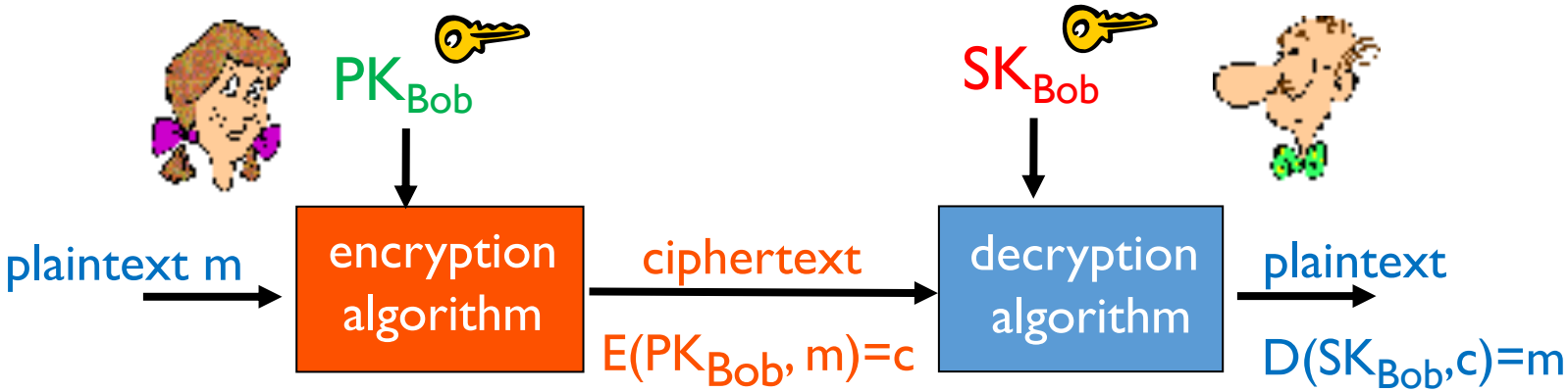
Defend your nsorship.

Download Tor Browser

Outline

1. Network Security Recap

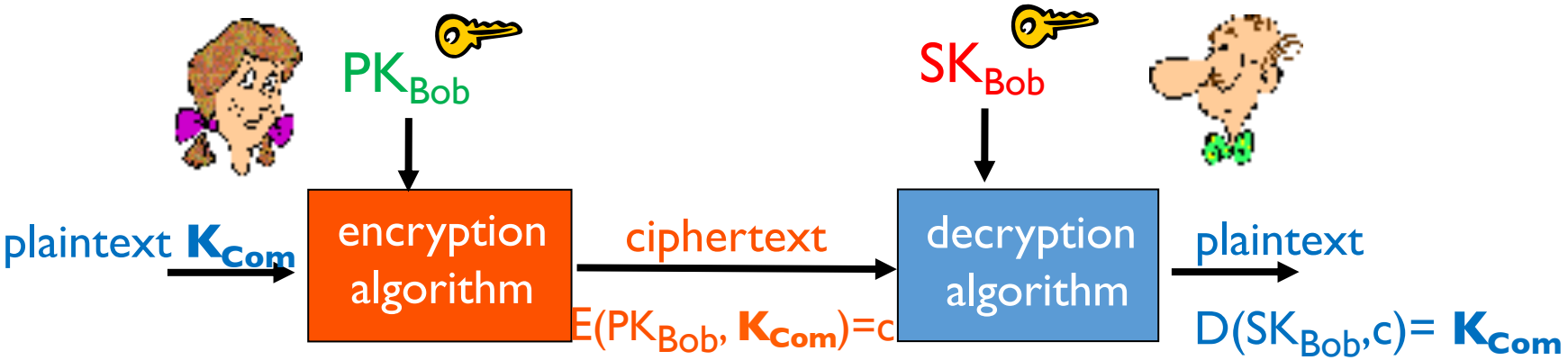
Public Key Infrastructure (PKI)



ex) RSA, Elliptic Curve, etc.

PK public key
SK private key

Alice can send the suggested share key to Bob encrypting with Bob's public key

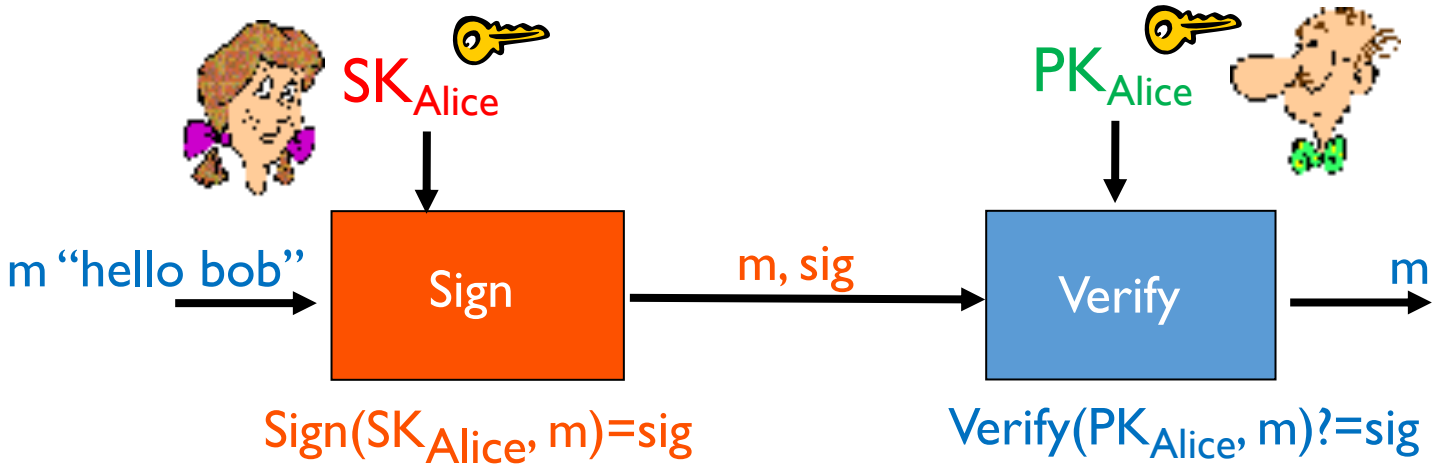


PK public key
SK private key

PKI is also used in digital signature

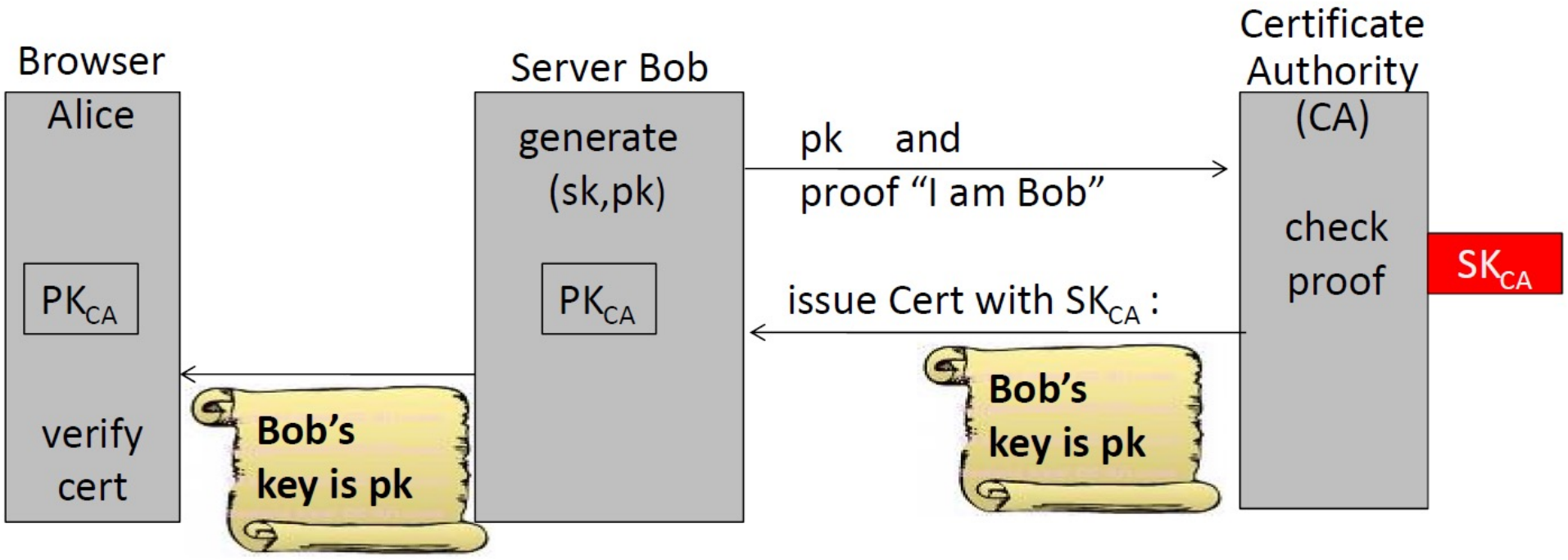
Provides authenticity and integrity of digital messages

- Authenticity: The message was created by the known sender
- Integrity: The message was not altered in transit



PK public key
SK private key

How does Alice obtain Bob's PK?



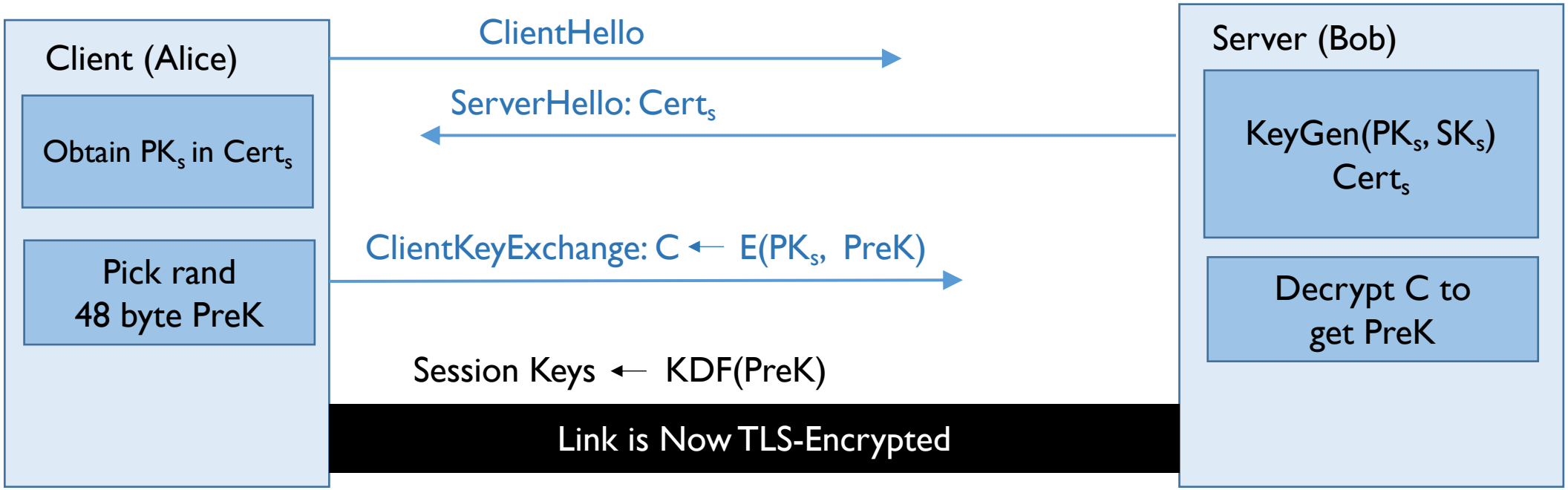
Certificates bind Bob's ID to his PK

Outline

1. Network Security Recap
2. TLS handshake

TLS Handshake v1

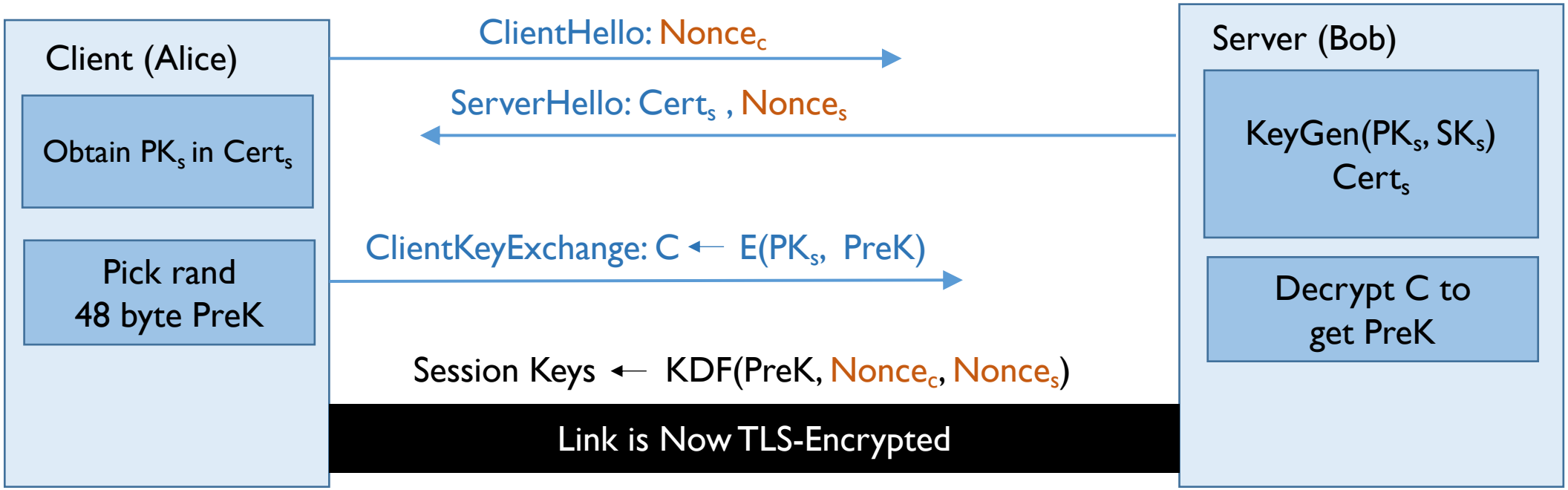
- Goal: Establish common session keys



Replay attack can happen!

TLS Handshake v2
Adding randomness protects against replay attack

- Goal: Establish common session keys



What if SKs gets compromised?

What if Bob's SK got lost or compromised?

- Bob's certificate has to be revoked
- Bob regenerates (PK, SK) pair and get a new certificate from CA

If an attacker has recorded past message exchange,
he can encrypt/decrypt with
the compromised private key!

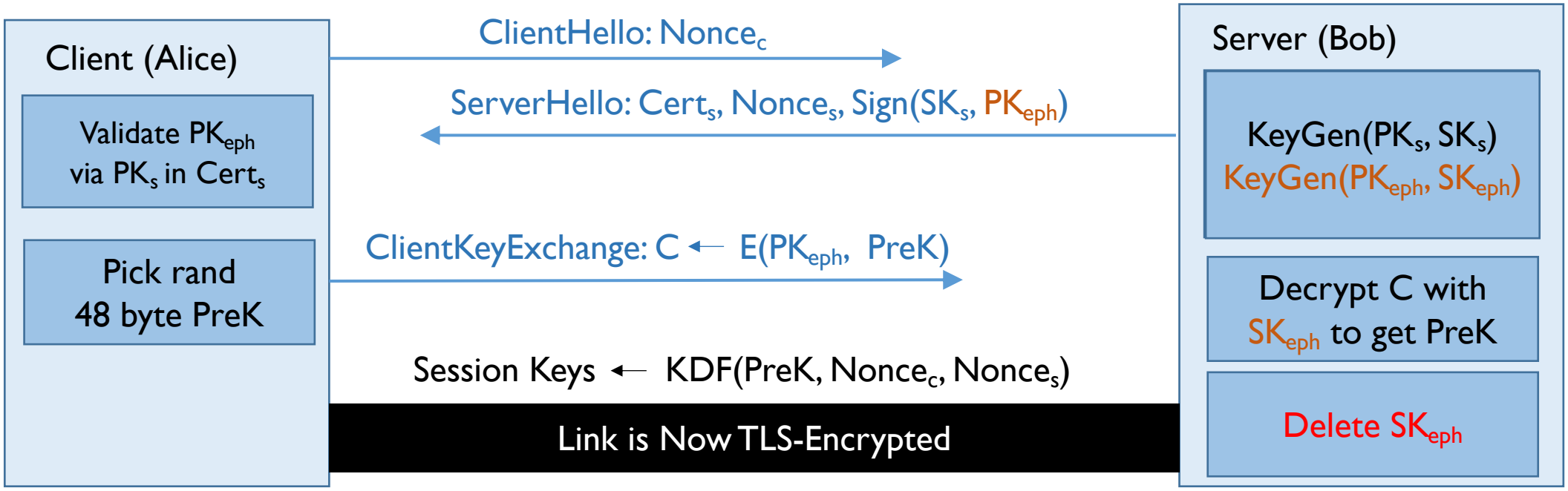
Key exchange should provide forward secrecy

Future compromise of secret key should NOT affect past sessions

- Need a separate session key other than the private key
- Computationally less burdensome

TLS Handshake with forward secrecy

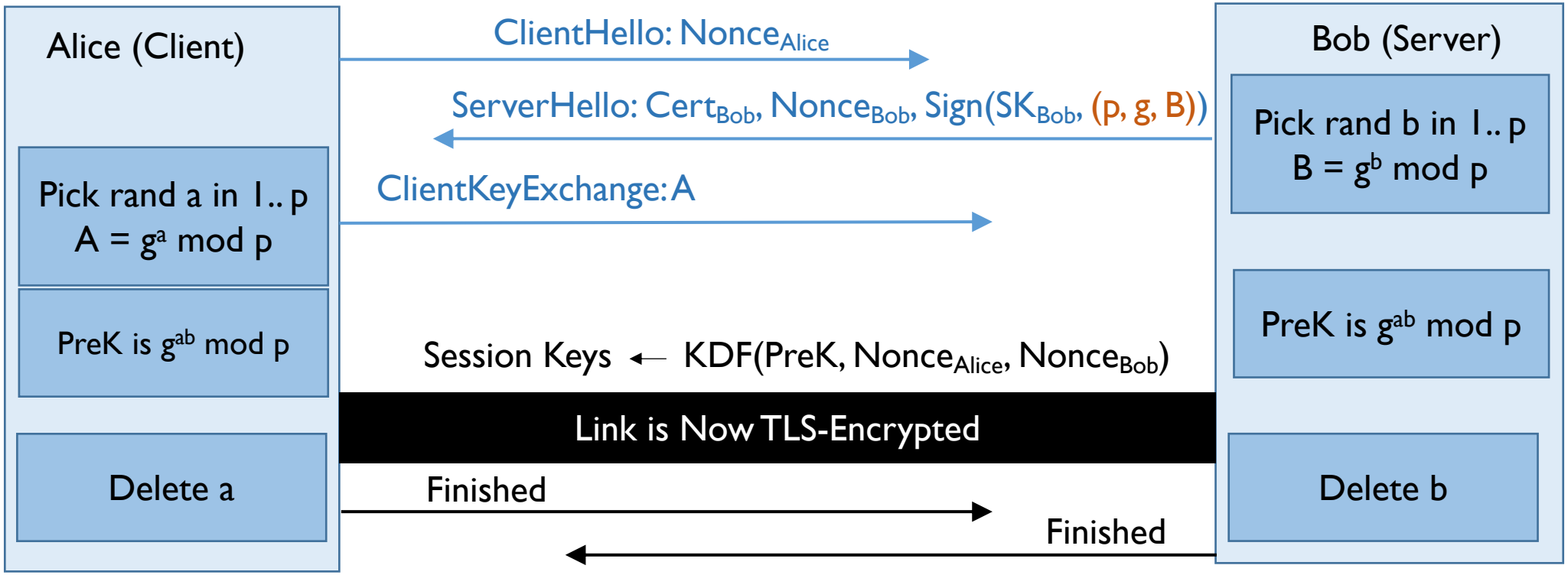
- Goal: Establish common session keys



RSA Key Gen is Slow. Can we do better?

TLS Handshake via Diffie Hellman

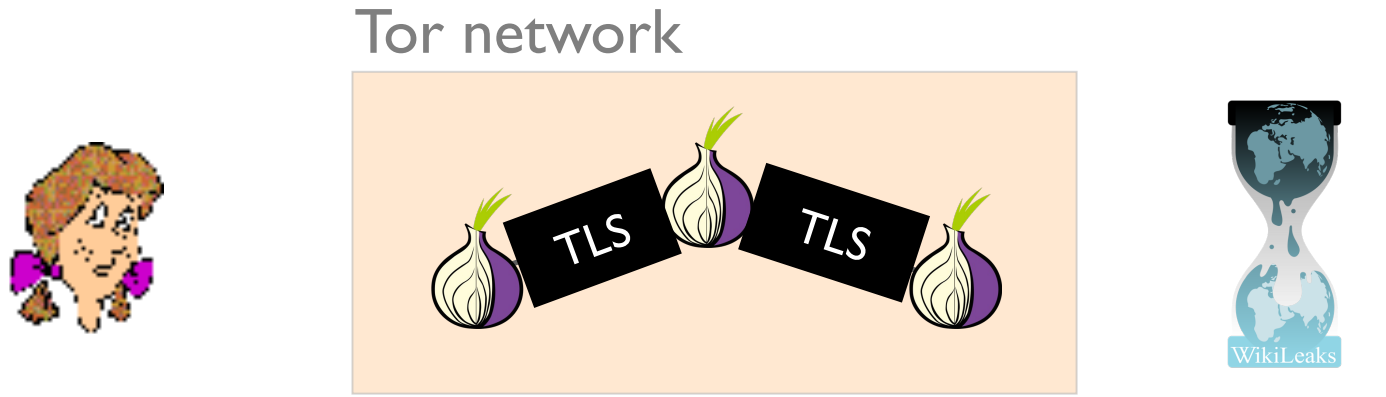
- Goal: Symmetric key exchange



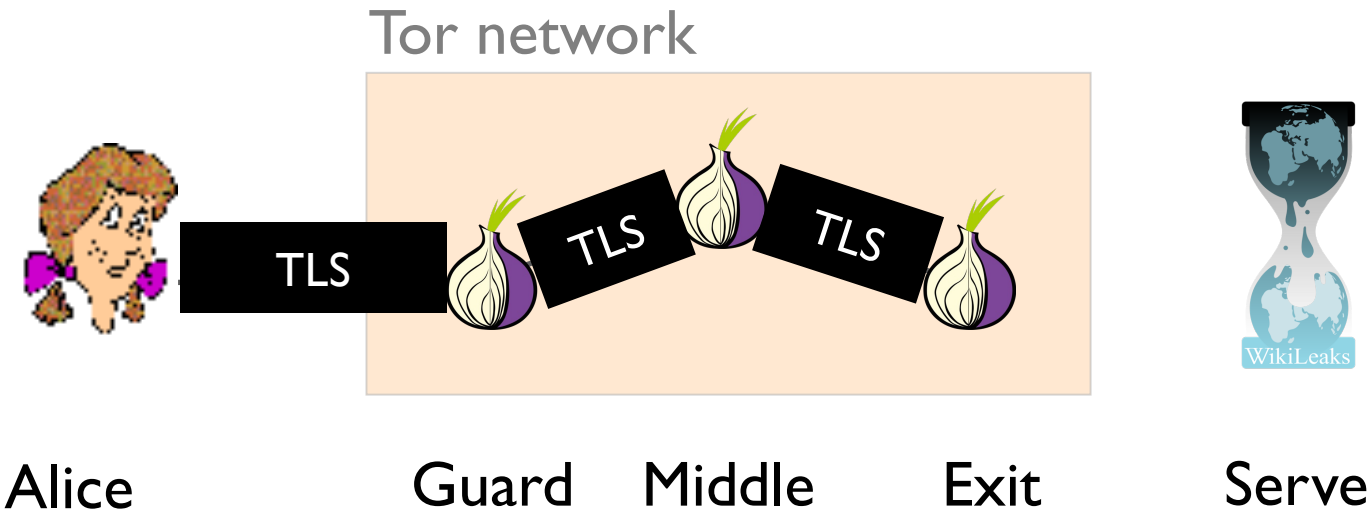
Outline

1. Network Security Recap
2. TLS handshake
3. The full story of Tor Circuit

TLS connections are pre-established among Tor nodes

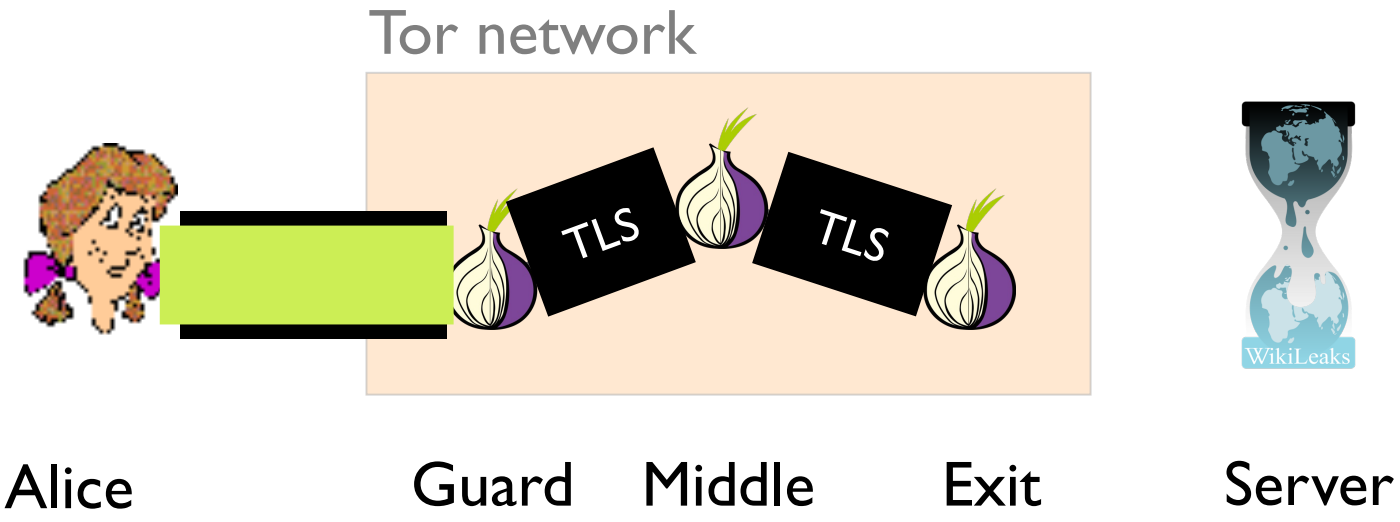


TLS connection first needs to be established between Alice and Guard



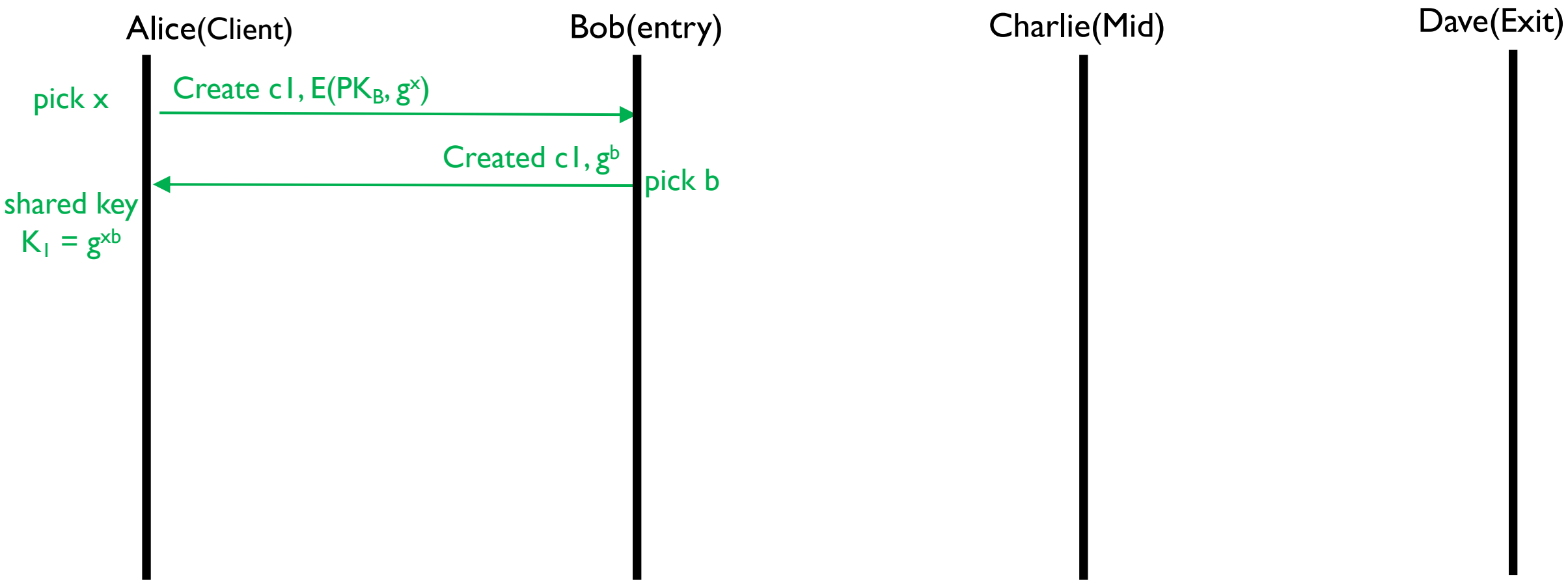
ANY messages exchanged between each connection
is encrypted using the set of session keys (connection key in Tor)

With TLS tunnel already established
Alice starts the steps to build the Tor circuit

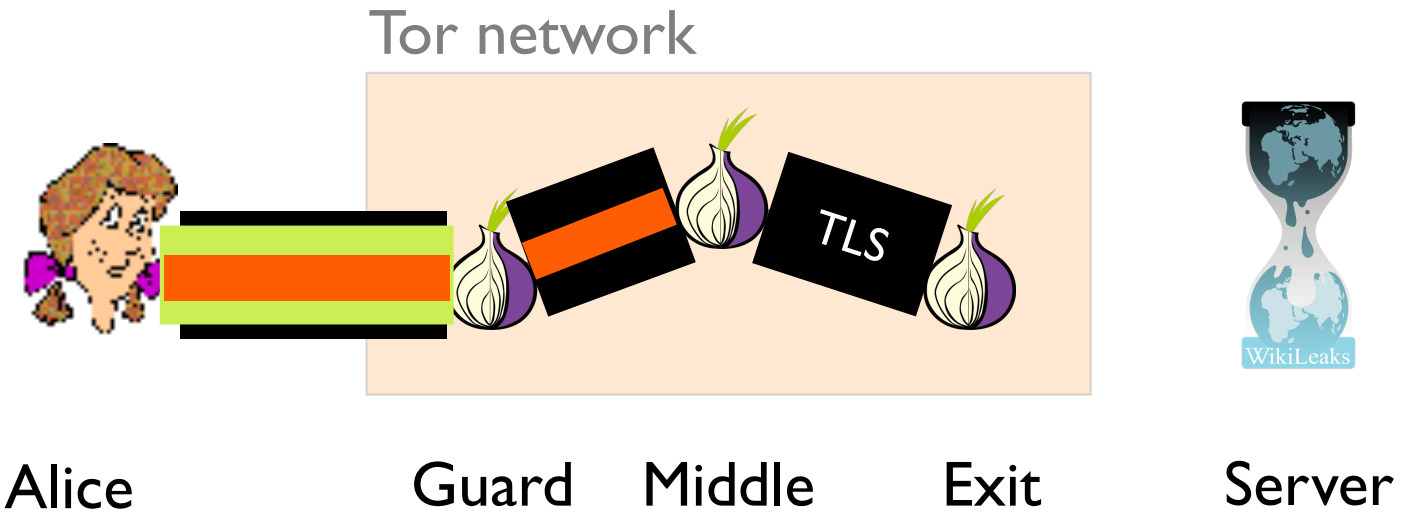


Tor Circuit Construction: 1st hop

- How Alice – Bob establish shared session key K_1

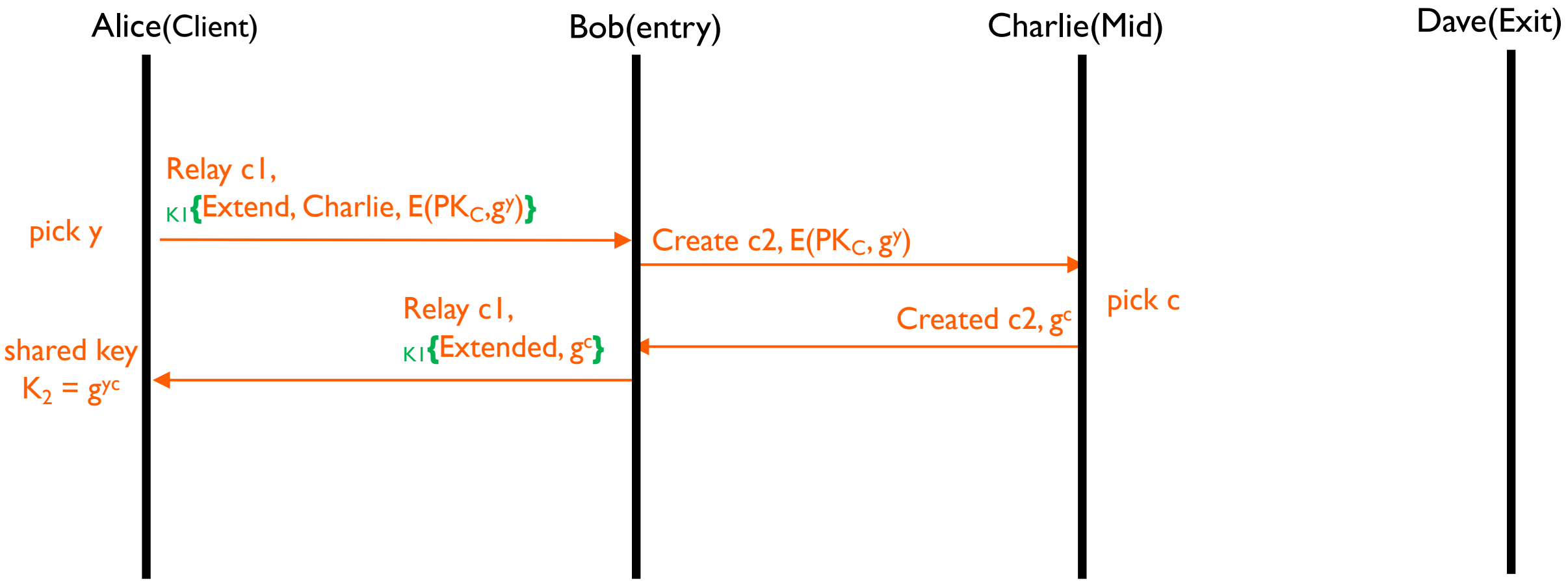


With TLS tunnel already established
Alice starts the steps to build the Tor circuit

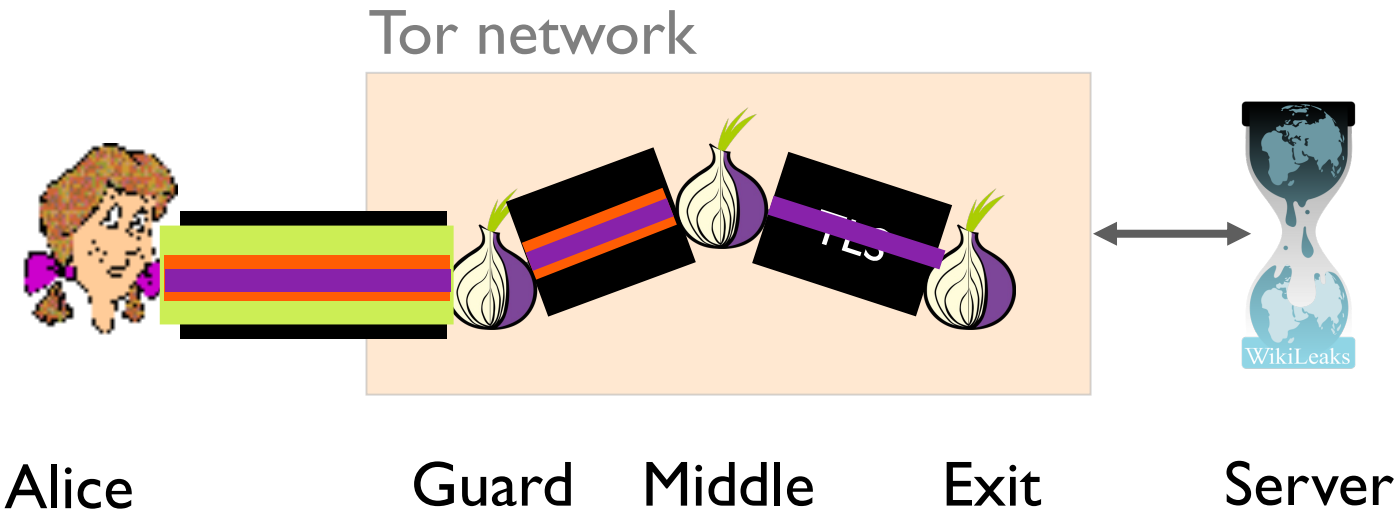


Tor Circuit Construction: 2nd hop

- How Alice – Charlie establish shared session key K_2

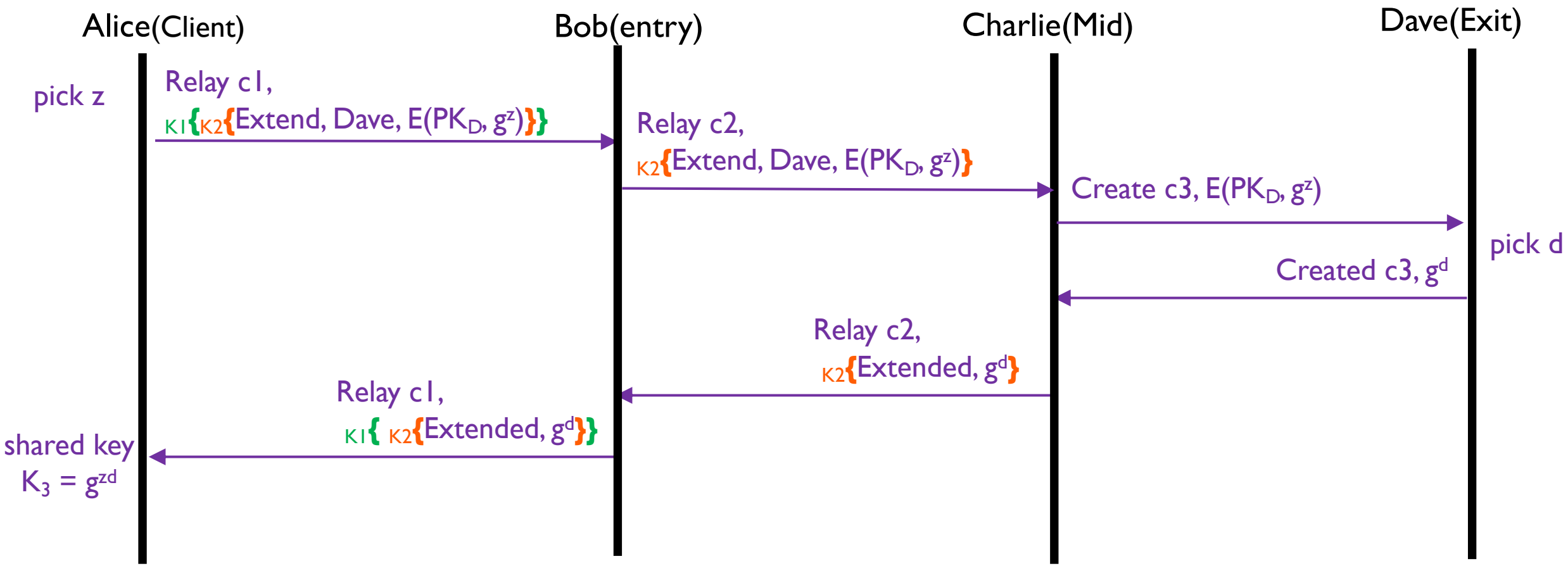


With TLS tunnel already established
Alice starts the steps to build the Tor circuit

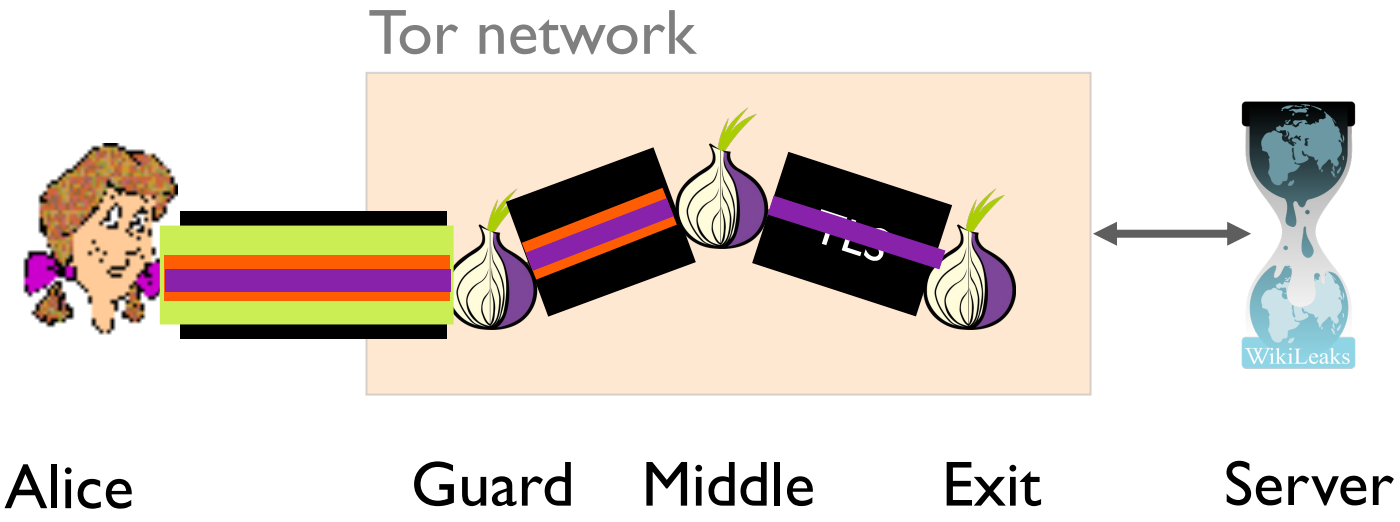


Tor Circuit Construction: 3rd hop

- How Alice – Dave establish shared session key K_3



ALL Tor messages are exchanged inside TLS tunnels



This makes it hard to distinguish Tor traffic from normal TLS traffic

Tor Packet Forwarding via 3 hop Circuit

- Alice – Bob, Alice – Charlie, Alice – Dave has shared session key K_1, K_2 and K_3