Tor Circuits

We want to hide metadata.

→ Idea 1: route message through proxy
   But now the proxy knows the recipient

→ Idea 2: Enlist a bunch of intermediaries
   & build a circuit.

→ choose among a set of volunteer relays
   & construct a circuit.

So the adversary will lose track of msgs
once they enter this relay.
Core communication piece in Tor®:

"Cells" like TLS has packets, Tor has cells. It's just a name to call communication units.

Types of "Cells":

- Command Cells - Help to build/destroy circuits
- Relay Cells - Carry data
- ... (other types)

All relays R have a public key Pkr.

Server

Client $\xrightarrow{TLS} R_1 \xrightarrow{R_2} R_2 \xrightarrow{R_3}$

Randomly sampled nodes from a list

Relays have existing TLS connections between them.
Telescoping Connection

Client ← R₁ ← R₂ ← Server

- cell: create
- cell: created
- cell: extend
- cell: create
- cell: created
Telescoping Connection Continued

\[
\text{Client} \xleftarrow{\text{TLS}} k_1 \xrightarrow{\text{cell: create}} R_1 \xleftarrow{\text{TLS}} R_2
\]

create Tor connection with \( R_1 \) \( k_1 \)
cell: created
\( g^b, H(k_1 || "handshake") \)

\[
\text{Enc} \left( k_1, \left[ \text{cell: extend} \right] \right)
\]

extend connection to \( R_2 \)

\[
\text{Enc} \left( k_1, \left[ \text{cell: extending} \right] \right)
\]

\( k_1 = \text{KDF}(g^b) \)

\[
\text{enc} \left( pk_{R_2}, g^b \right)
\]
**Onioning**

The client will send the following encryption to \( R_1 \) that will be peeled back in layers. Hence the name onioning.

1. **Client**
   - Create, \( C_1 \parallel \text{Enc}_{k_1}(\text{Enc}_{k_2}(\text{cell})) \)
   - Identifier of circuit from Client to \( R_1 \)

2. **\( R_1 \)**
   - Create, \( C_2 \parallel \text{Enc}_{k_2}(\text{cell}) \)

3. Look up \( C_1 \) to get \( k_1 \) and \( C_2 \)
4. Decrypt using \( k_1 \)
2) $R_2 \xleftarrow{\text{build TCP connection}} \text{Server}$

3) look up $c_2$ to get $k_2$

4) decrypt using $k_2$

$$c_1 \| \text{Enc}_{k_1}(\text{Enc}_{k_2}(\text{cell})) \rightarrow c_2 \| \text{Enc}_{k_2}(\text{cell}) \rightarrow \text{cell}$$