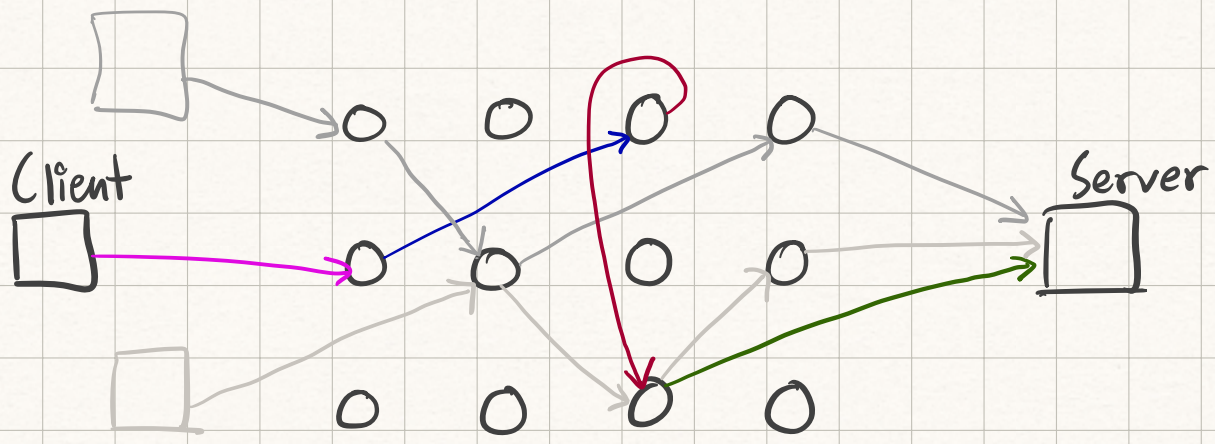
Tor Circuits

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:

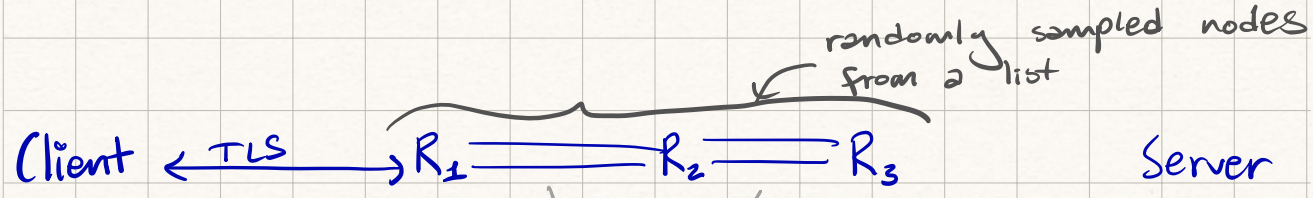
"Cells" ← like TLS has packets, Tor has cells. Its just a name to call commu-nication units

Types of "Cells":

→ Command Cells - Help to build/destroy circuits

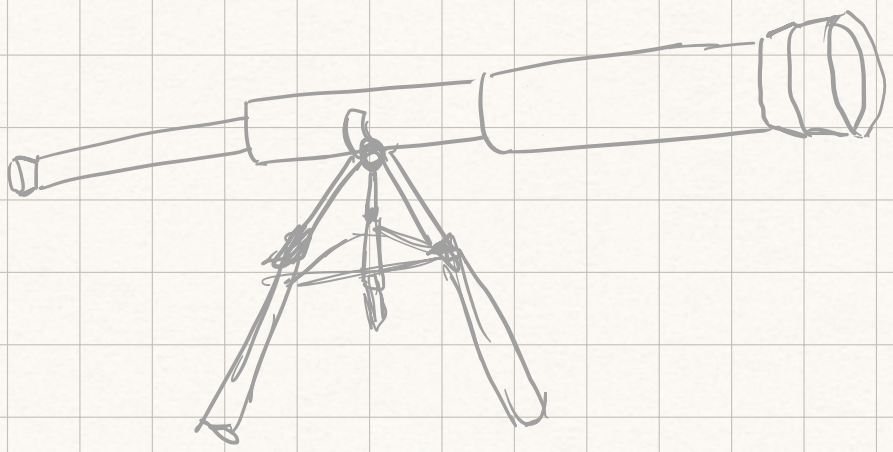
→ Relay Cells - carry data

→ ⋮

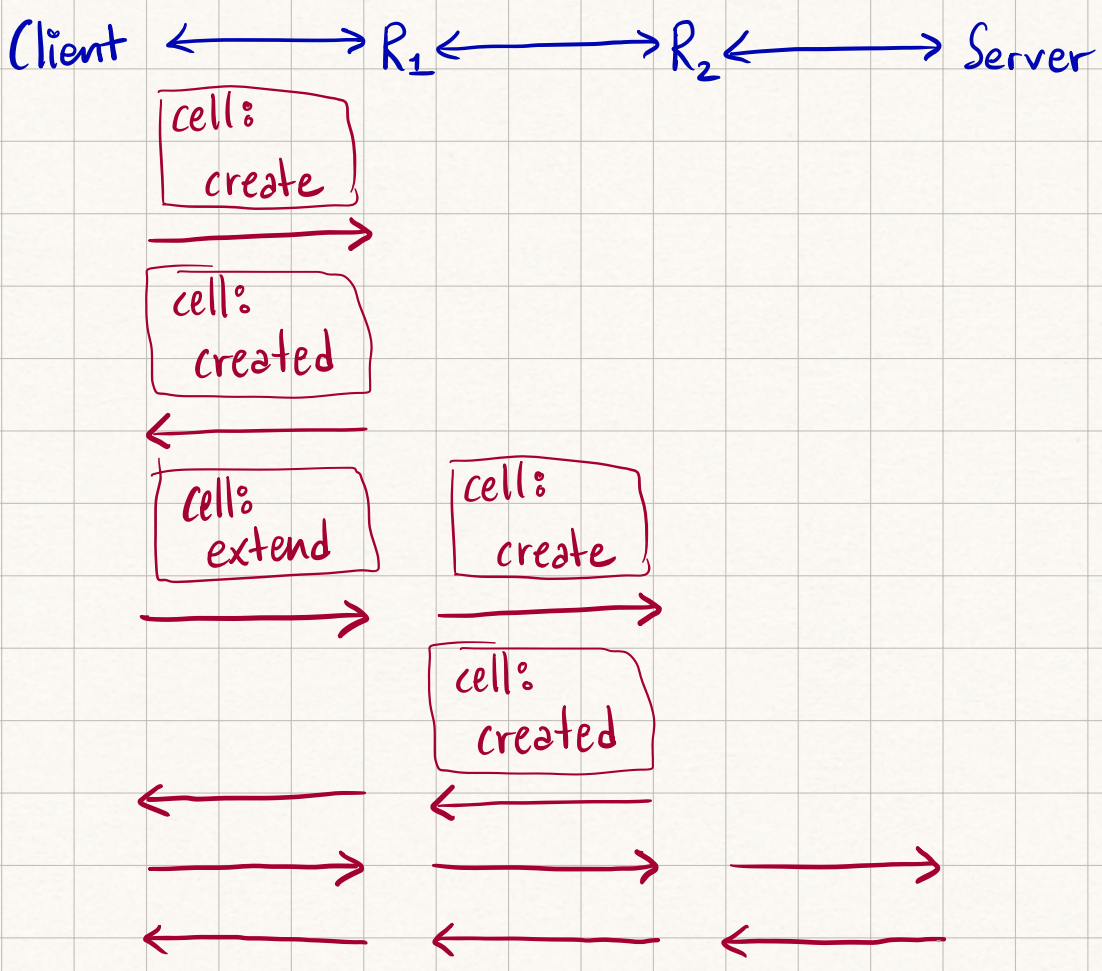


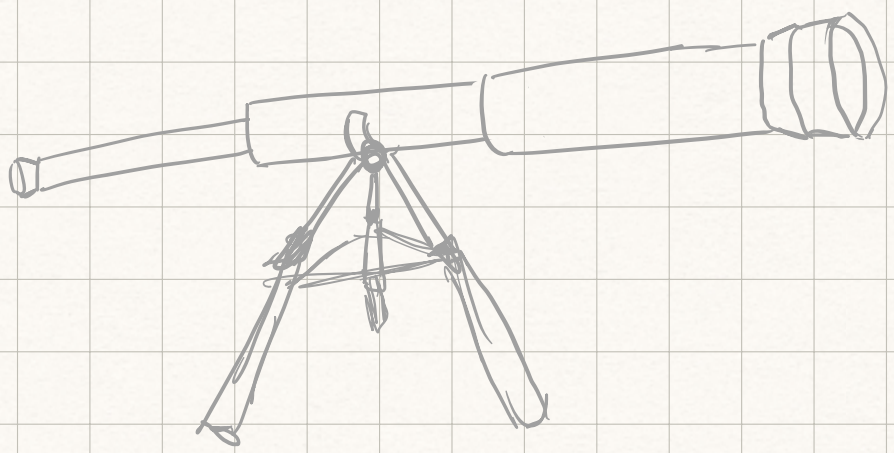
All relays R have a public key pk_R

relays have existing TLS connections between them.

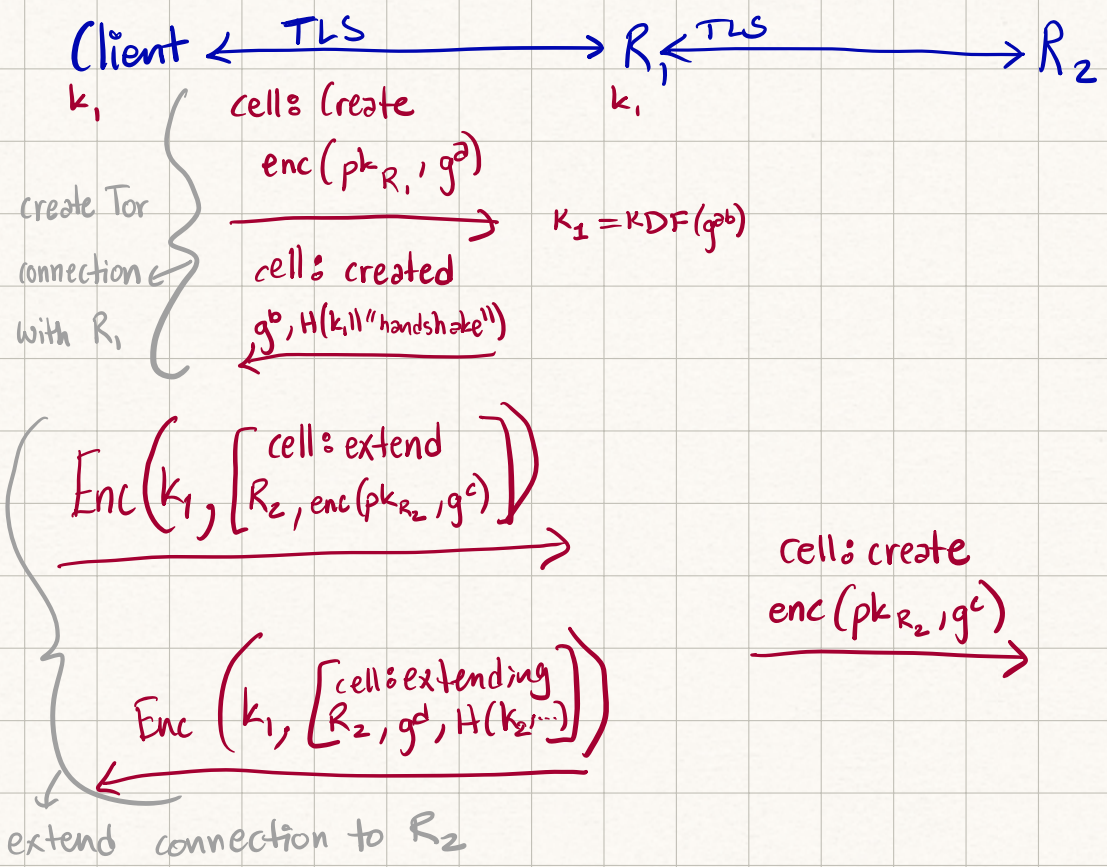


Telescoping Connection

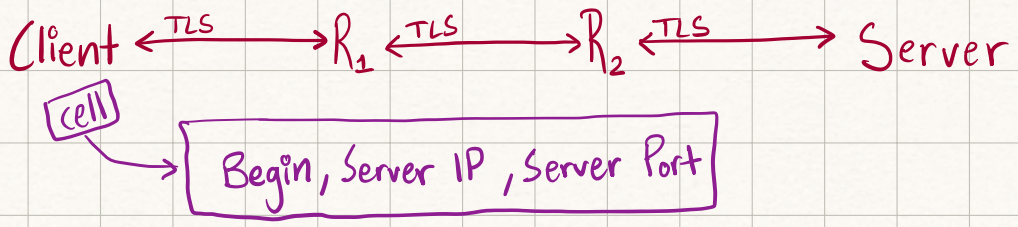




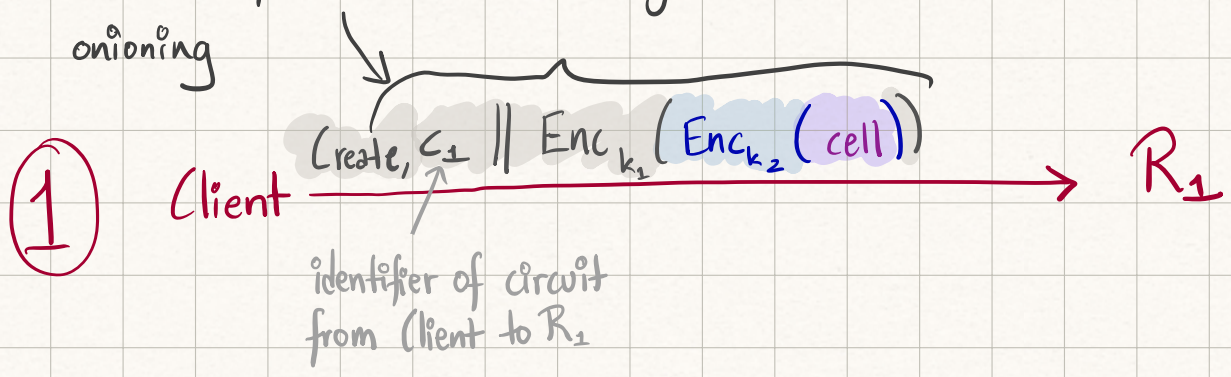
Telescoping Connection Continued



Onioning

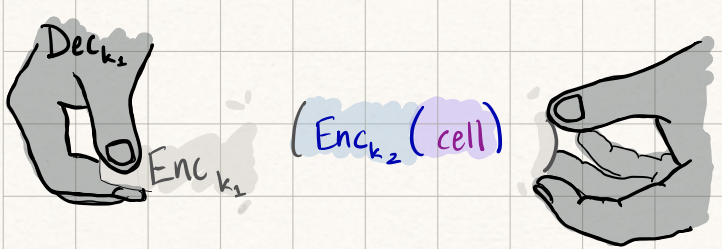


The Client will send the following encryption to R_1 that will be peeled back in layers. Hence the name onioning



① Look up c_1 to get k_1 & c_2

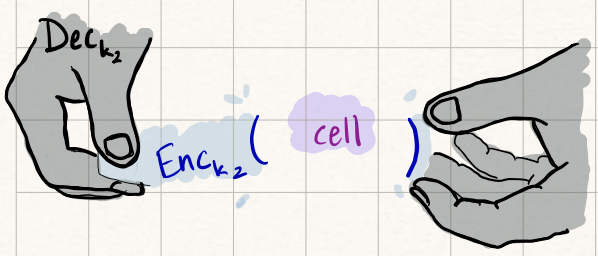
② decrypt using k_1



(2) R_2 ⟵ build TCP connection ⟶ Server

① Look up c_2 to get k_2

② decrypt using k_2



$c_1 \| Enc_{k_1}(Enc_{k_2}(cell)) \rightarrow c_2 \| Enc_{k_2}(cell) \rightarrow cell$