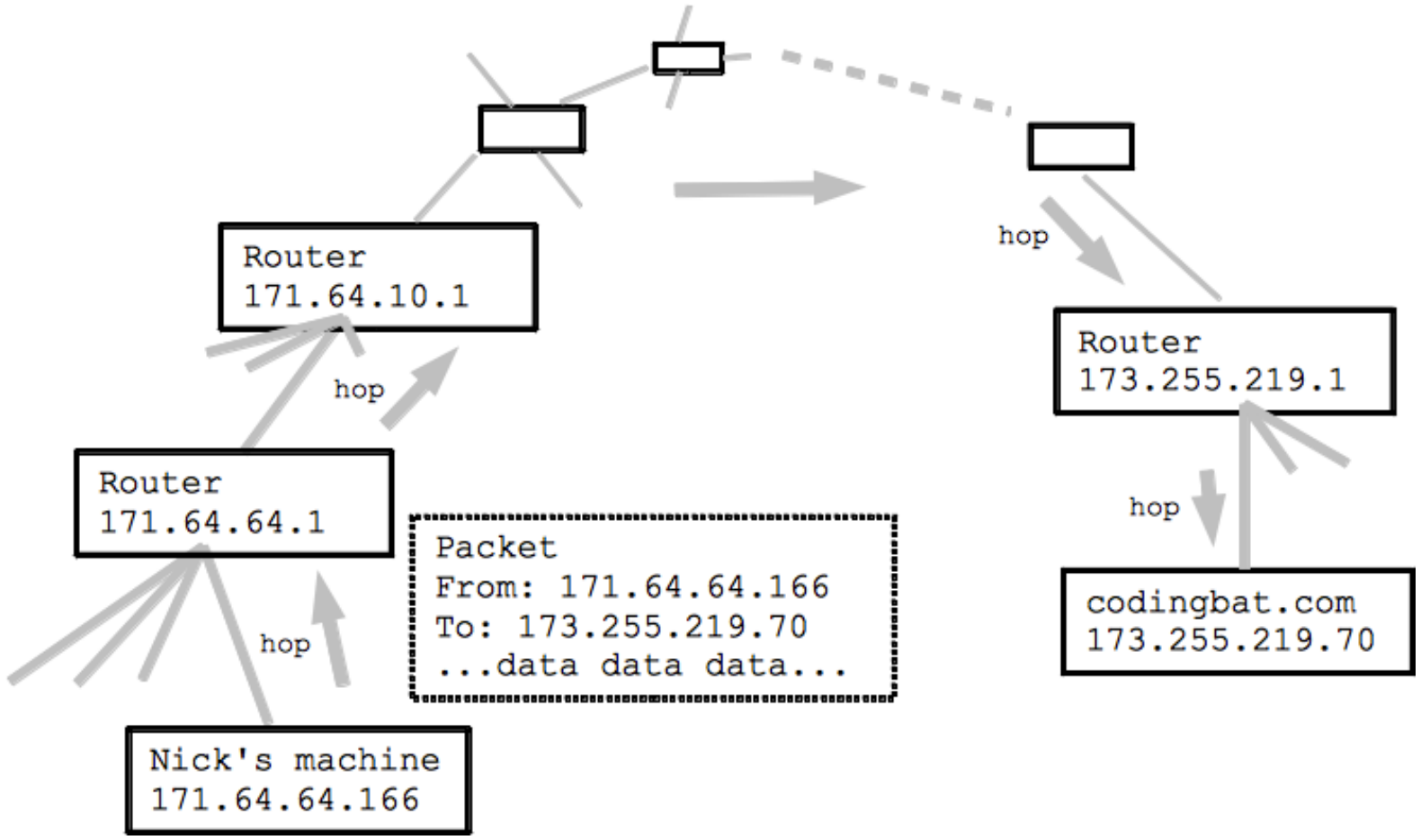
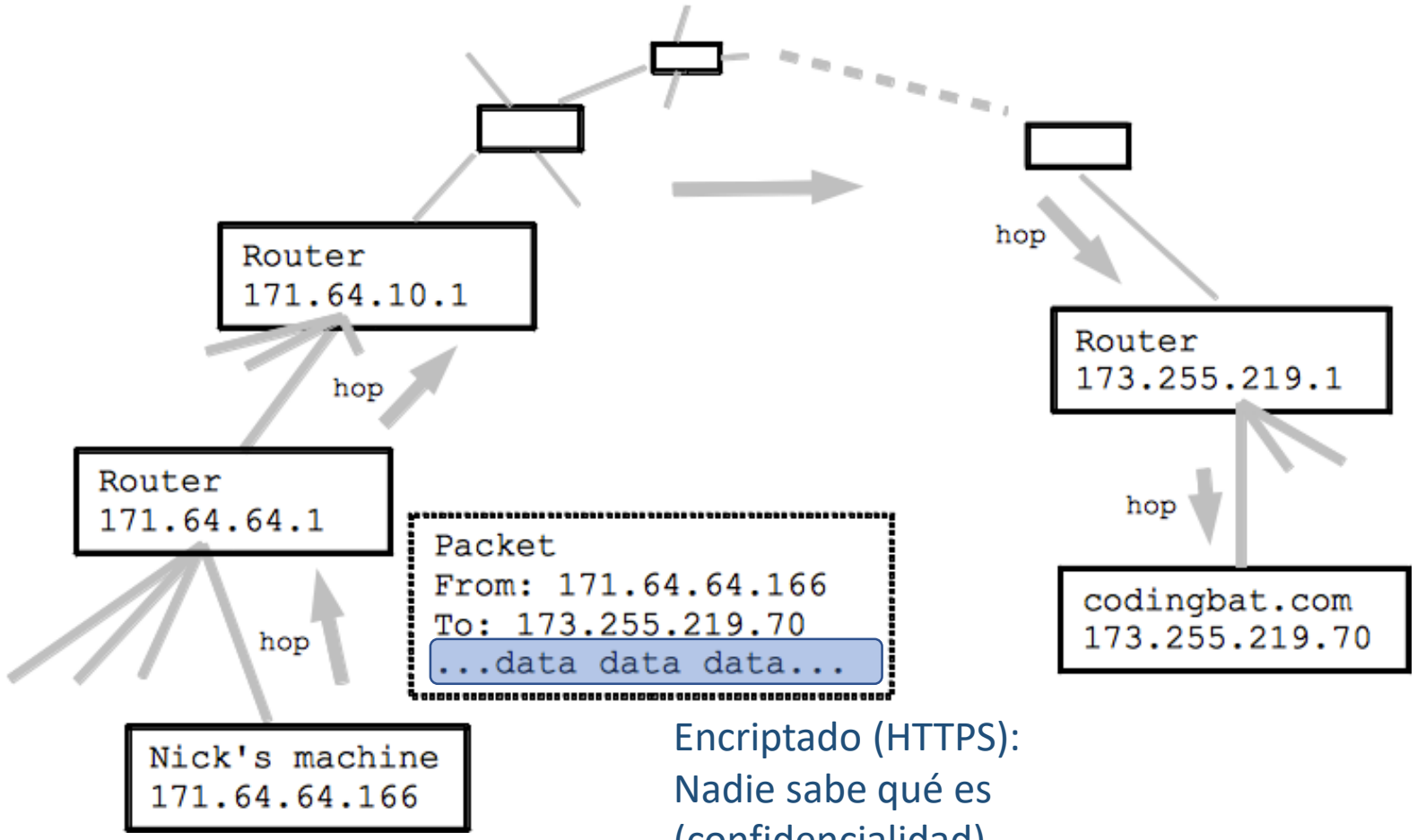
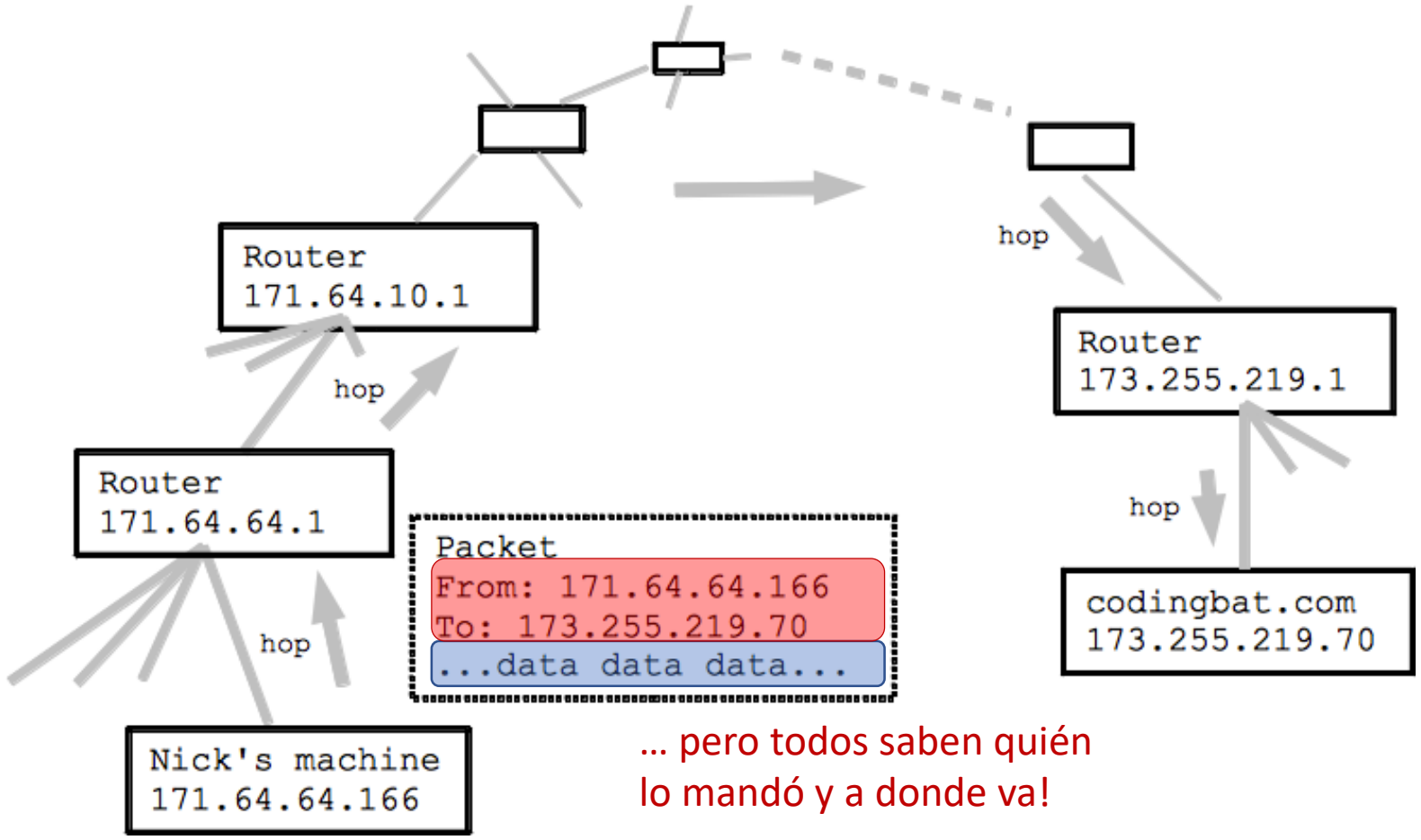

Router
171.64.10.1
hop
Router
171.64.64.1
hop
Nick's machine
171.64.64.166
Packet
From: 171.64.64.166
To: 173.255.219.70
...data data data...
hop
Router
173.255.219.1
hop
codingbat.com
173.255.219.70



Encriptado (HTTPS):
Nadie sabe qué es
(confidencialidad)…



… pero todos saben quién lo mandó y a donde va!

Consecuencias

- ISP pueden bloquear sitios (control de lo que uno ve)
- Monitoreo de actividad (control de lo que uno hace)

→ **Censura/Control de la información**

Onion Routing

Mauricio Ortiz

Contenido

- ¿Qué es?
- Cómo surgió
- Cómo funciona
- Beneficios y Desventajas

¿Qué es?

- “Enrutamiento cebolla” (o encaminamiento cebolla)
- *Infraestructura* para comunicación privada sobre una red pública que provee *anonimato* de los interlocutores
- Bidireccional y casi en tiempo real

- No confundir con Tor (implementación de esto)

Cómo surgió

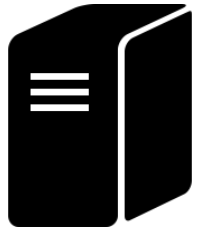
- Desarrollada en la ONR (Office of Naval Research) en 1995, para proteger la agencia de inteligencia (IC) del país.
- Posteriormente financiada también por el DARPA (Defense Advanced Research Projects Agency).
- Se libera el código al público en 2003
- The Tor Project (2006)

Cómo funciona

- Paquetes se envían a través de “onion routers”
- Paquete tiene capas de encriptación, los cuales deben ser desencriptados por estos routers
- “Los mensajes son como las cebollas, tienen capas”… de encriptación

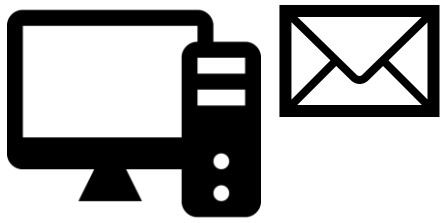
Cómo funciona

- Paquetes se envían a través de “onion routers”
- Paquete tiene capas de encriptación, los cuales deben ser desencriptados por estos routers
- “Los mensajes son como las cebollas, tienen capas”… de encriptación



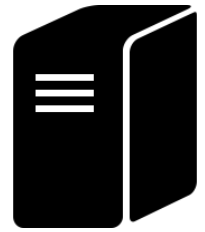
5.5.5.5

De: 1.1.1.1
Para: 5.5.5.5
Data: Buscar “Cebollas”

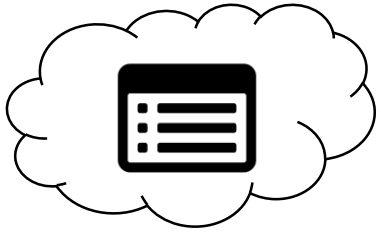


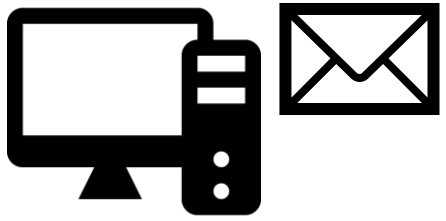
1.1.1.1

Armamos un recorrido mediante un directorio de *“onion routers”*



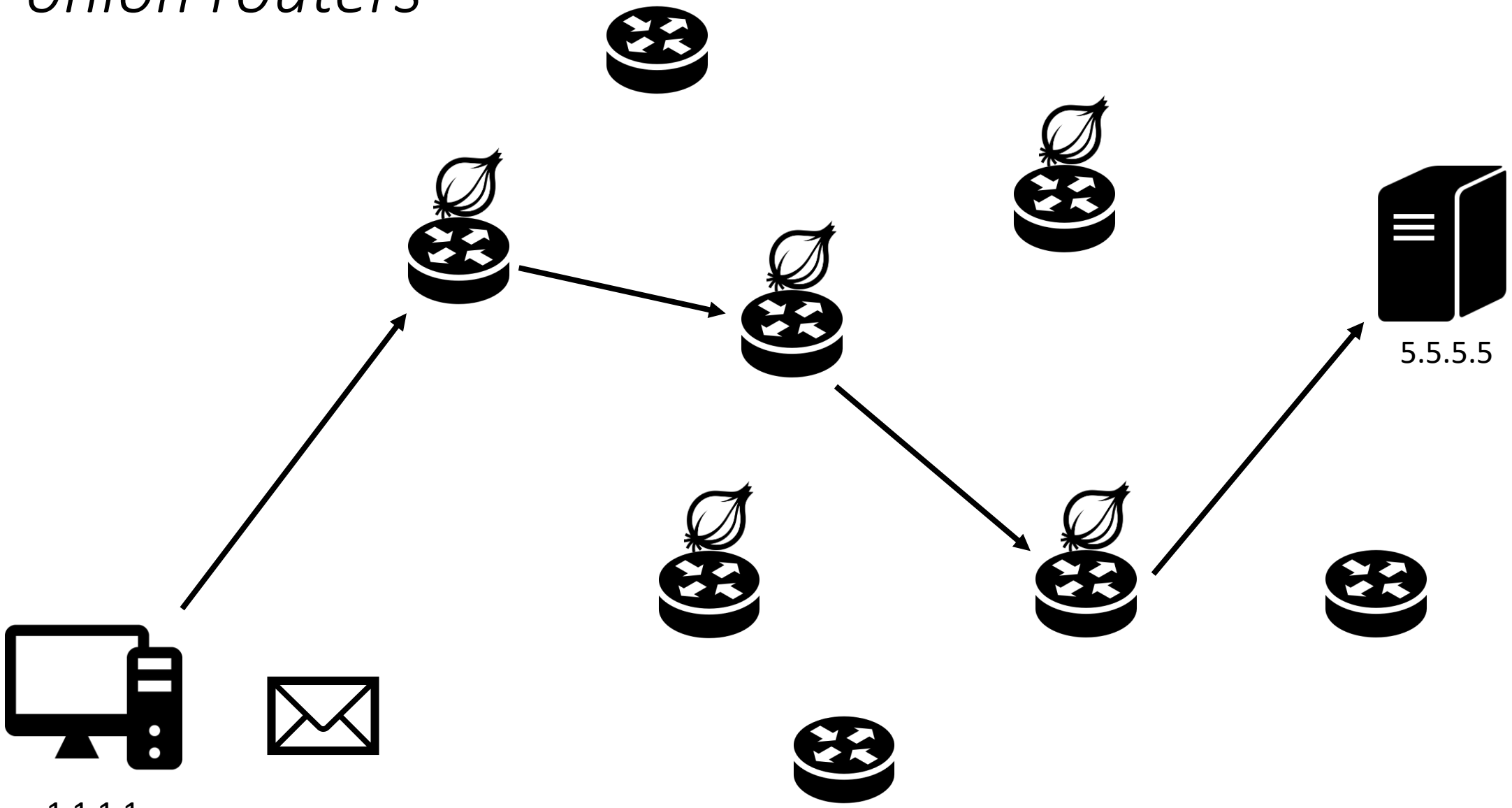
5.5.5.5



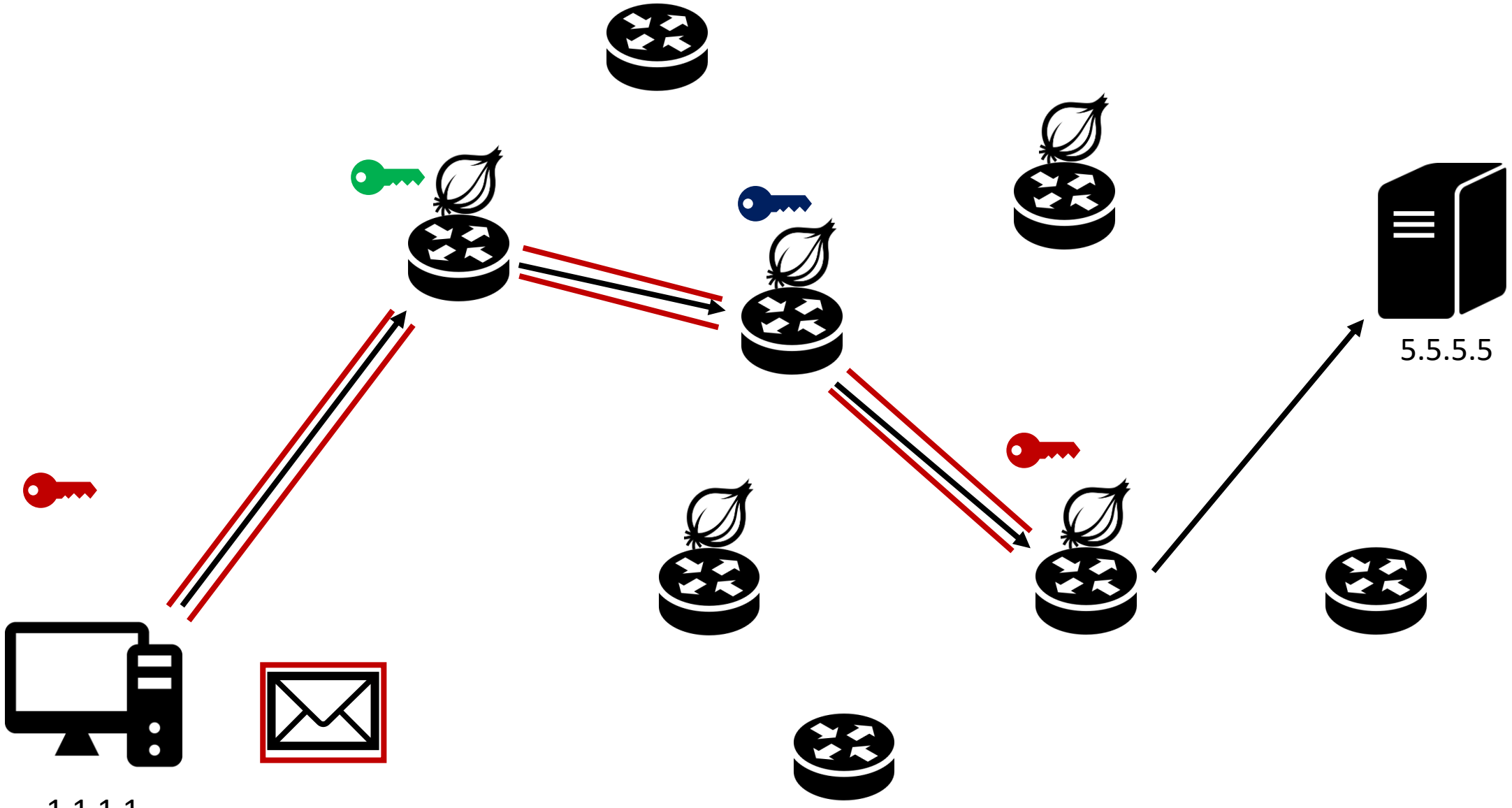


1.1.1.1

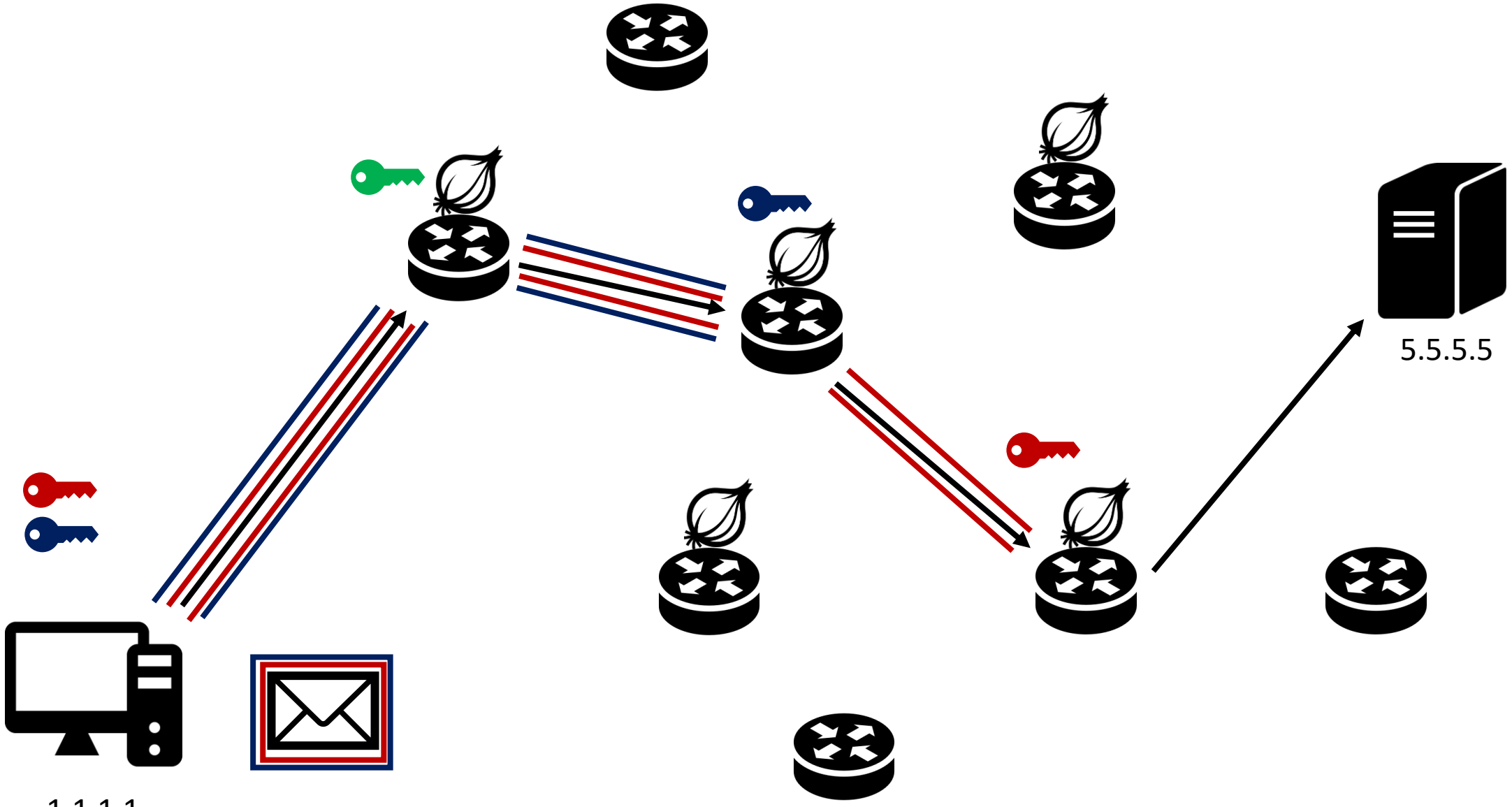
Armamos un recorrido mediante un directorio de *"onion routers"*



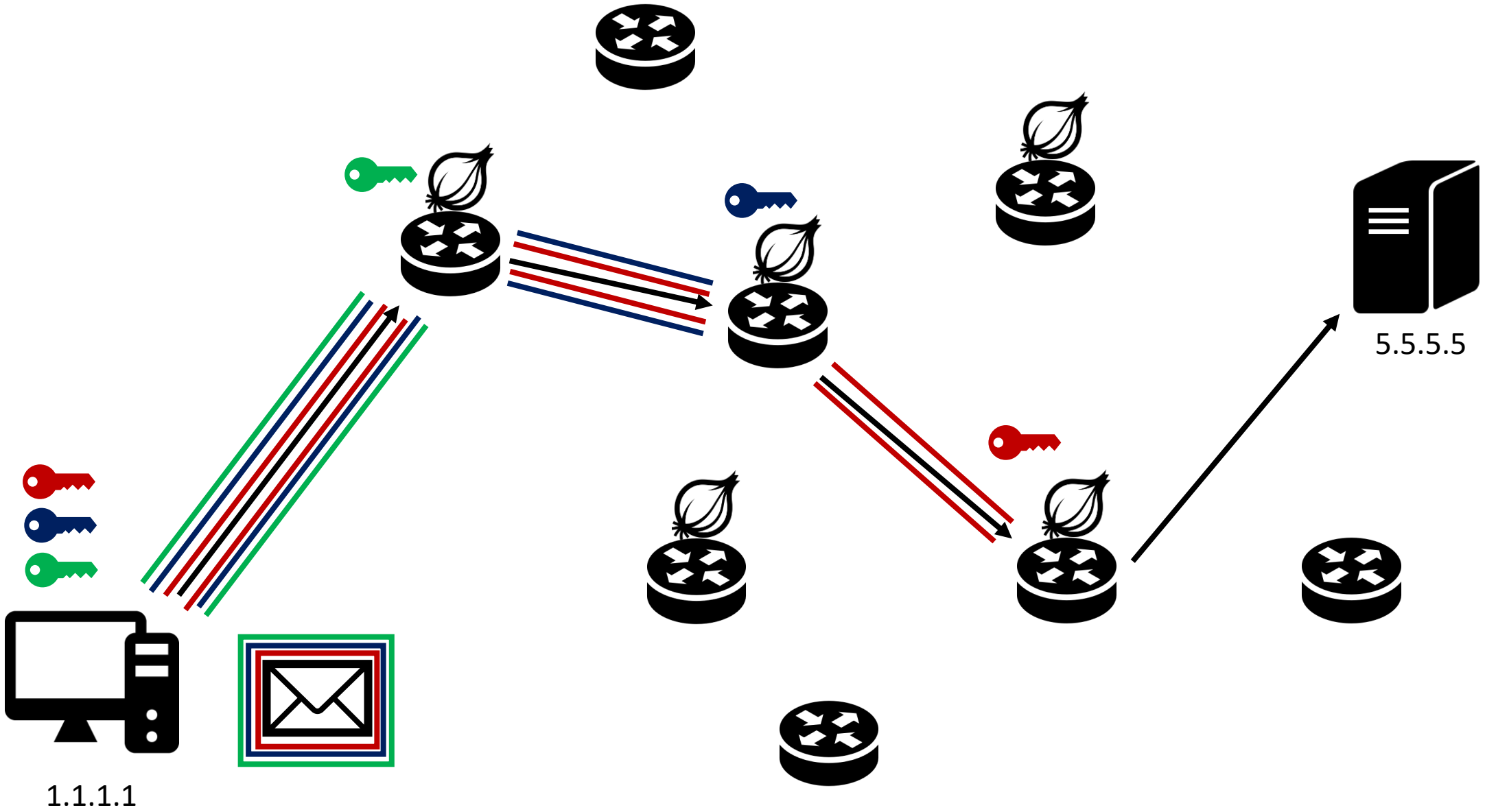
Armamos el “*onion packet*”



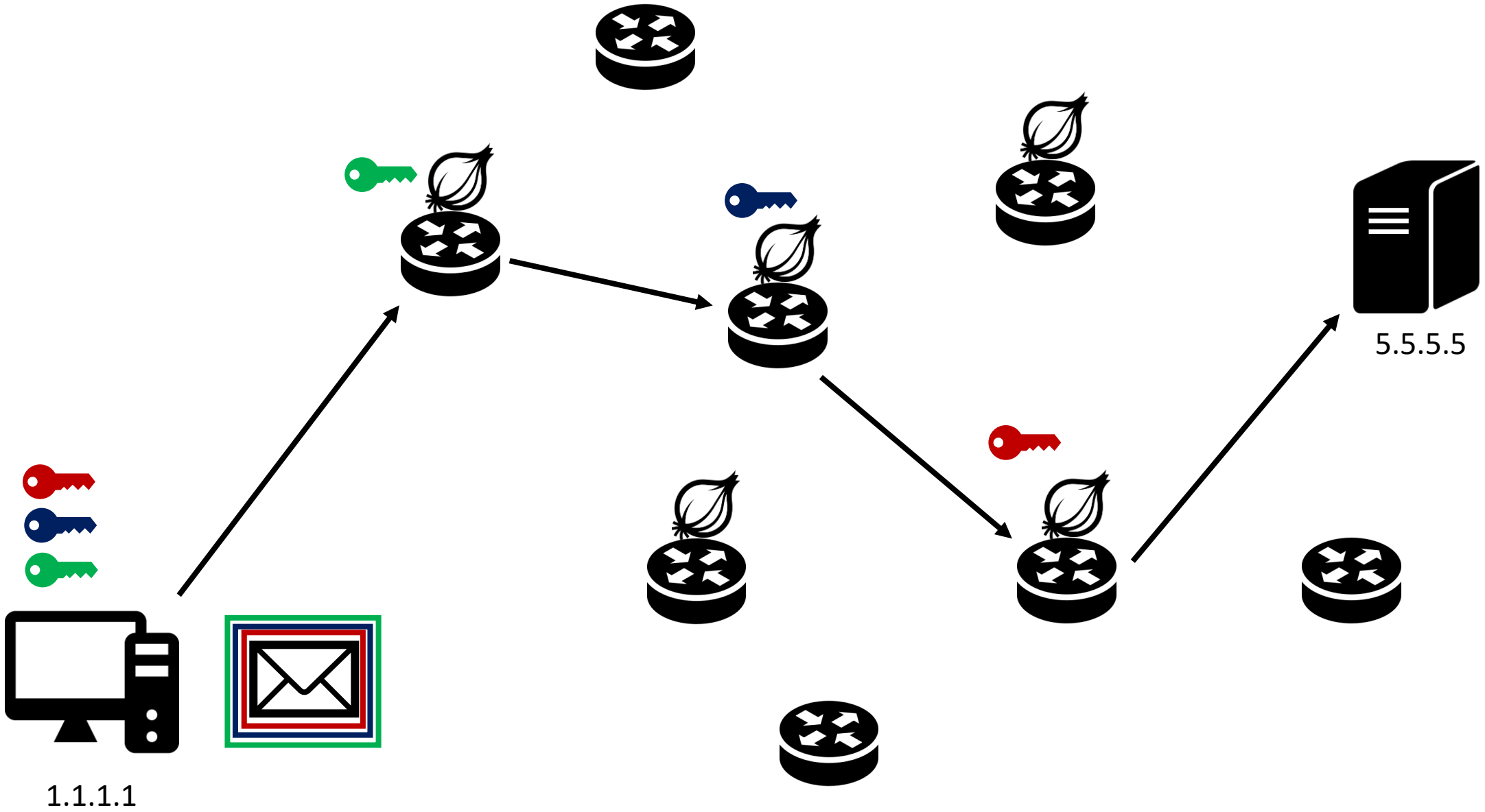
Armamos el “*onion packet*”



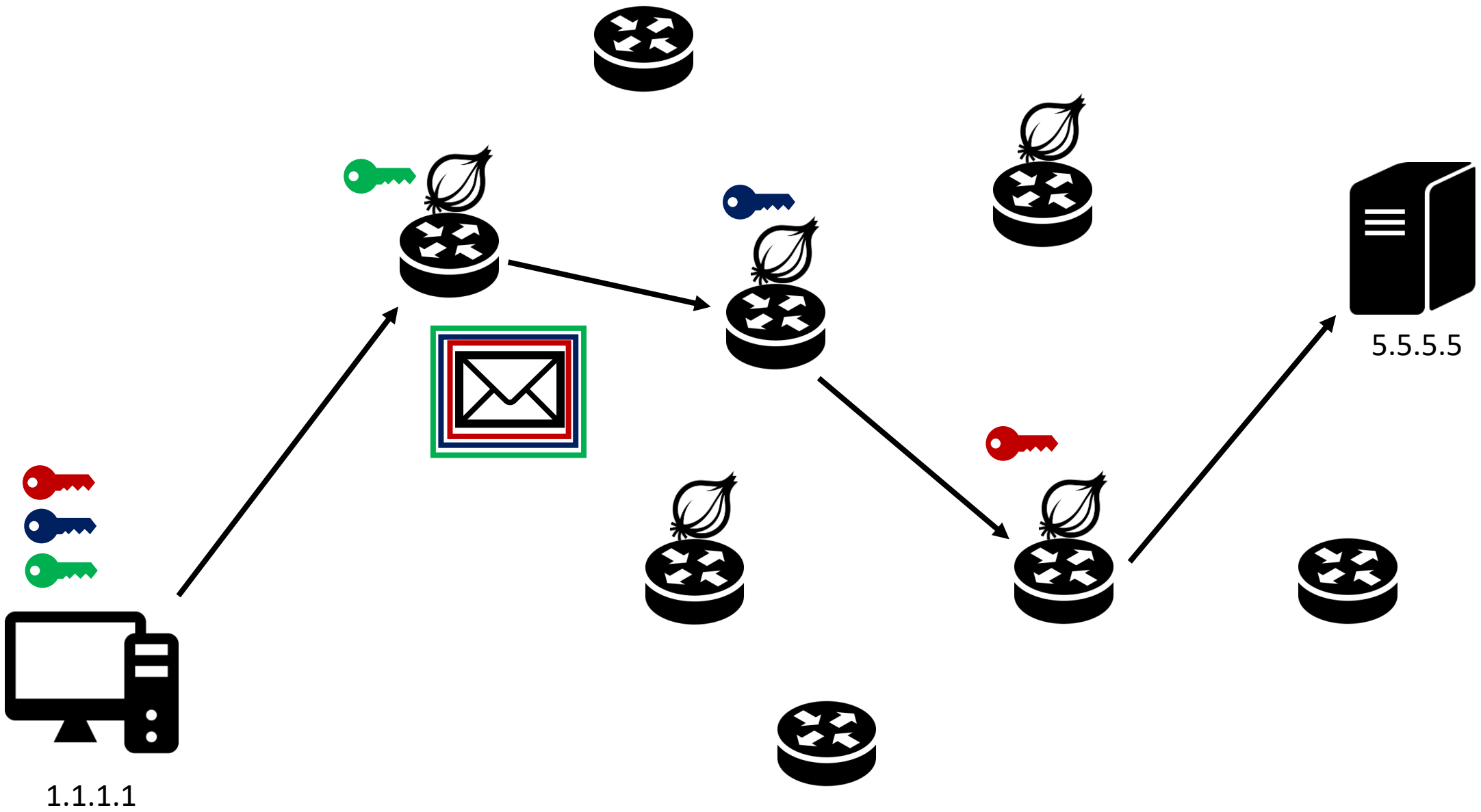
Armamos el “*onion packet*”



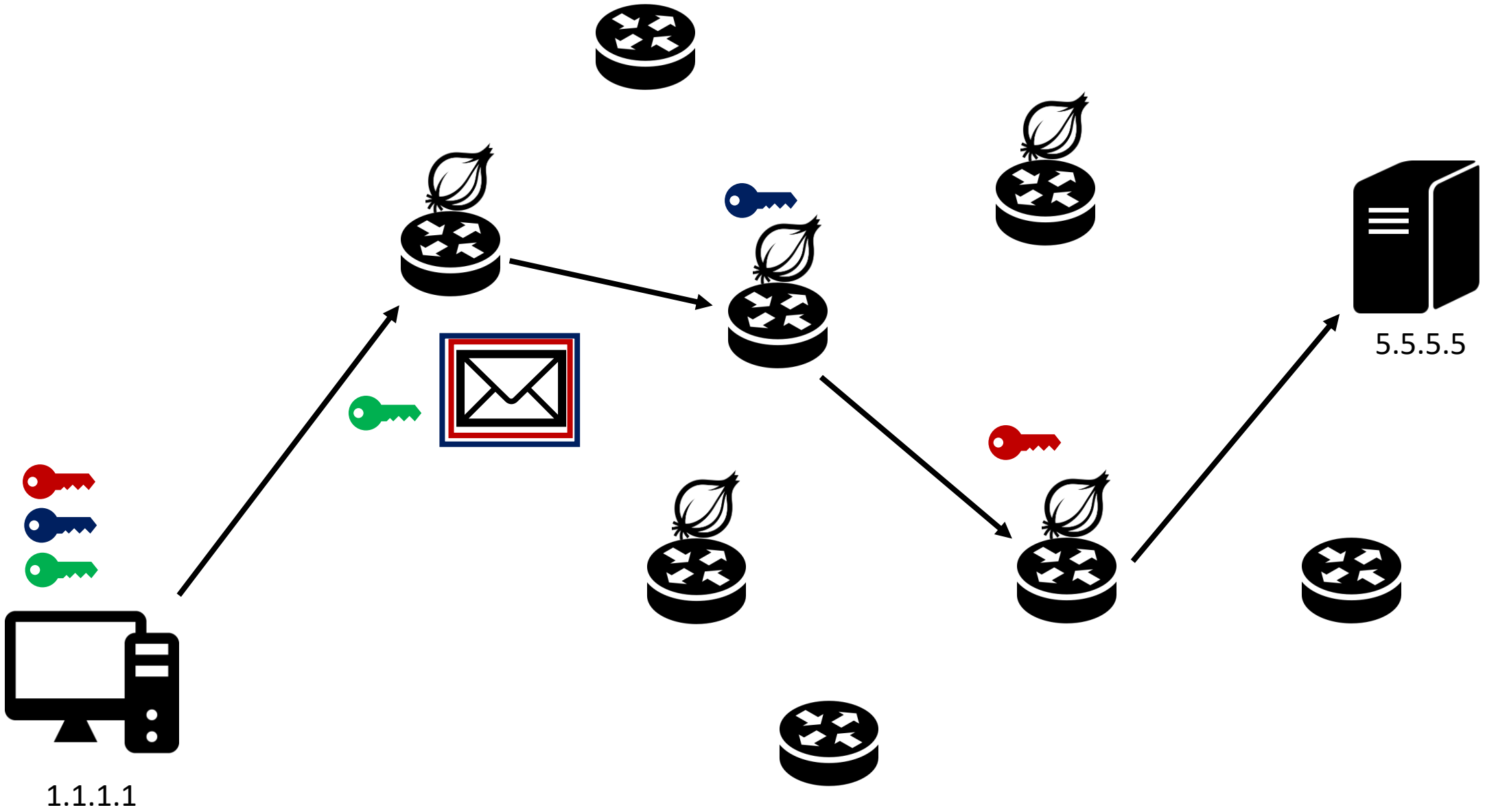
Y lo mandamos



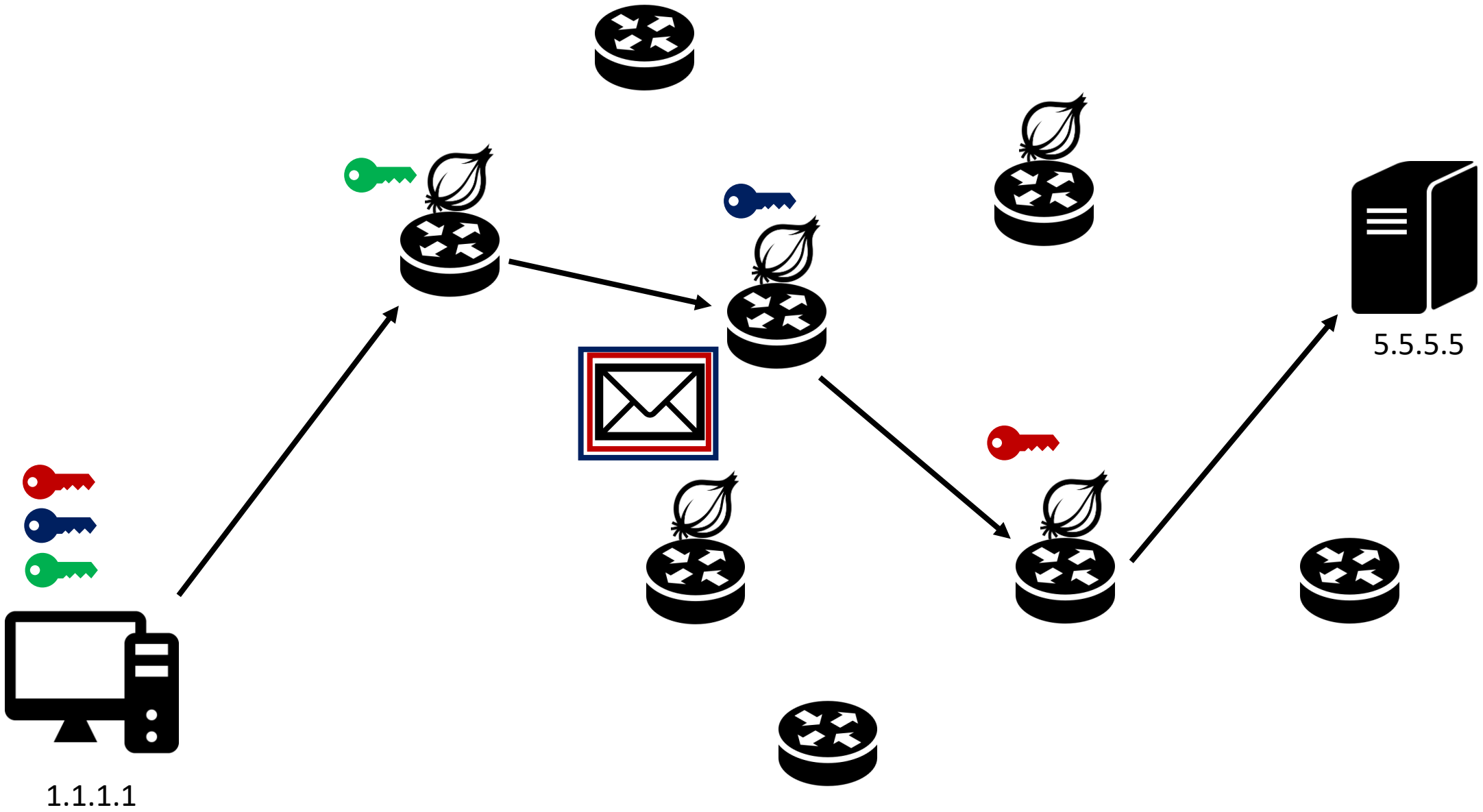
Y lo mandamos



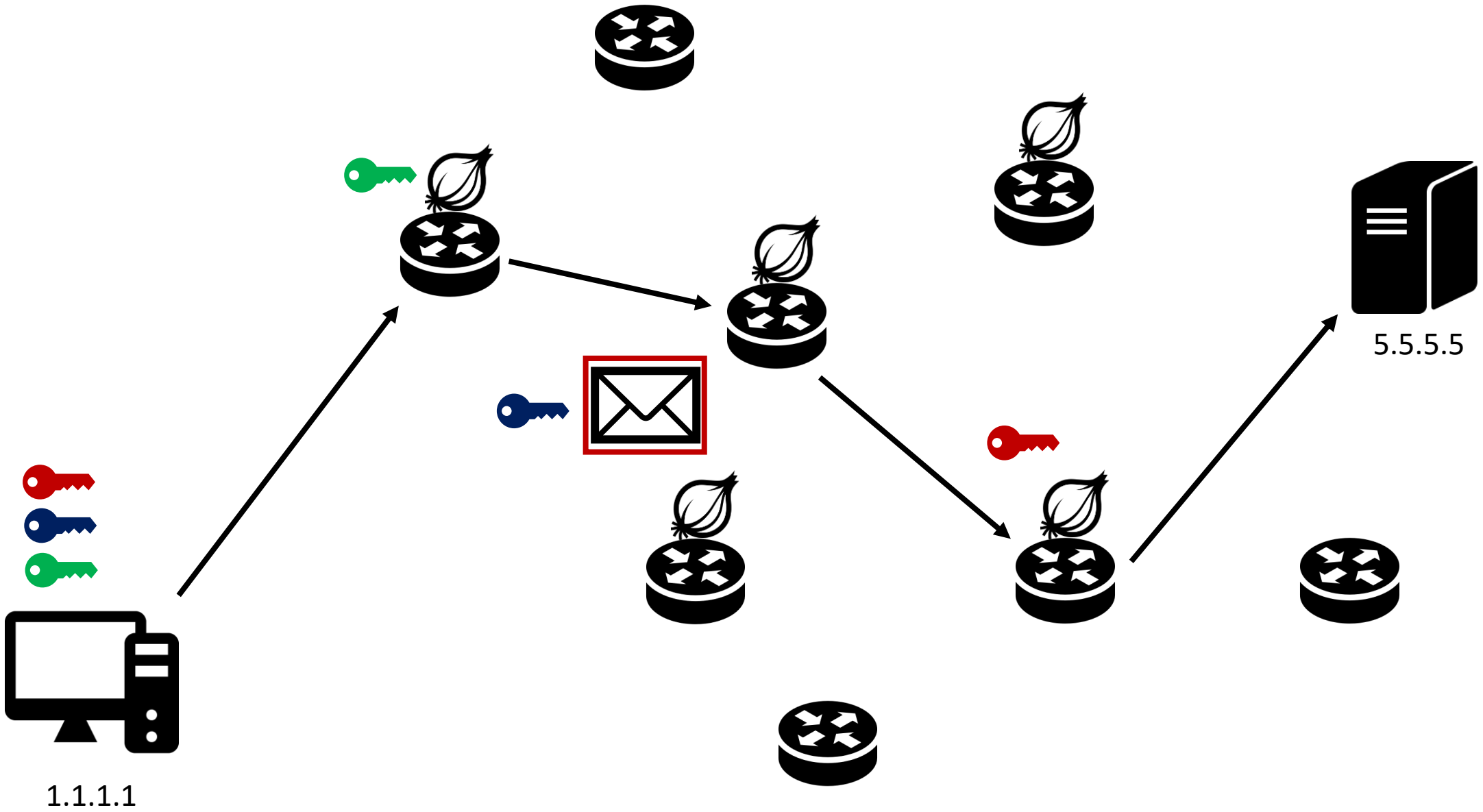
Y lo mandamos



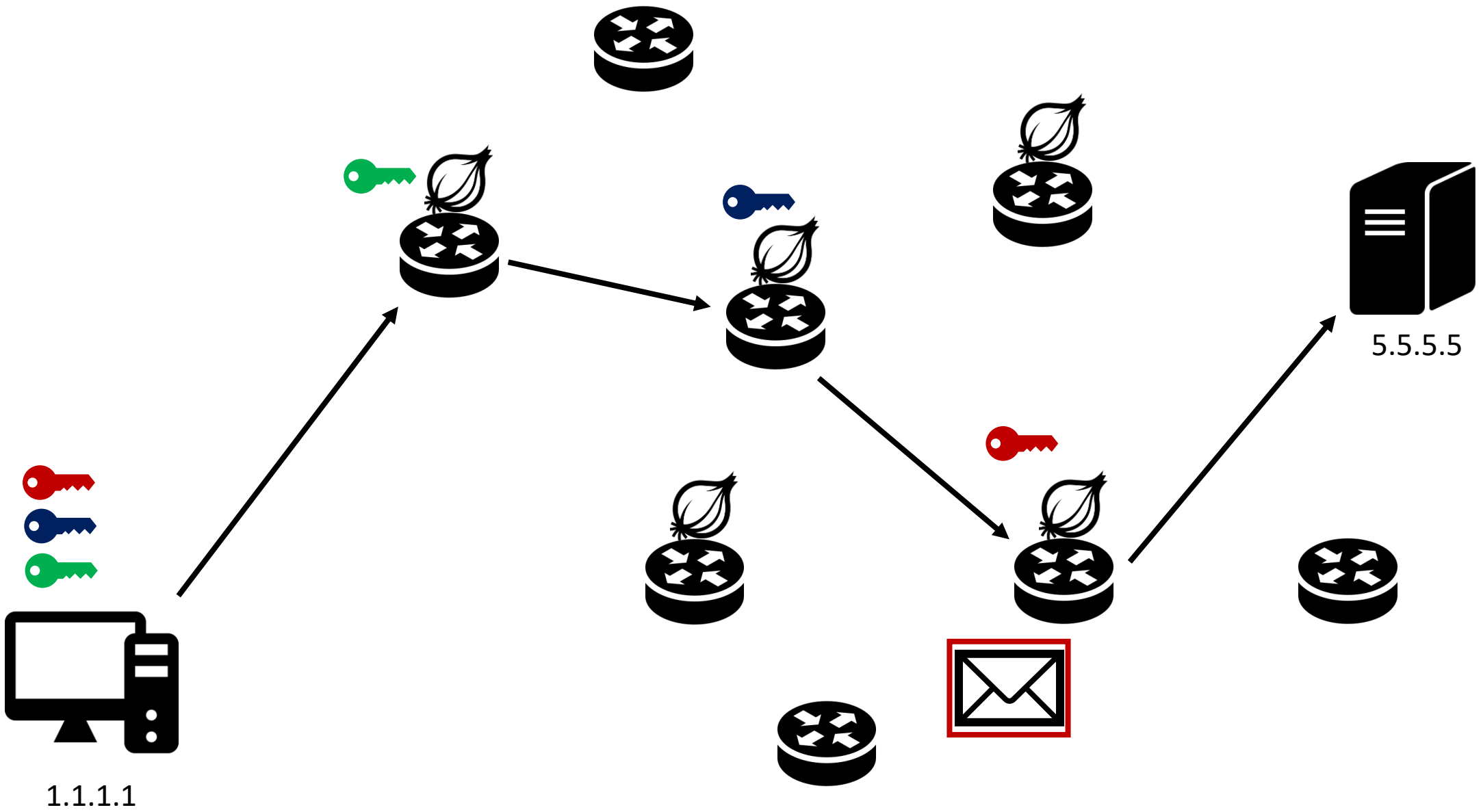
Y lo mandamos



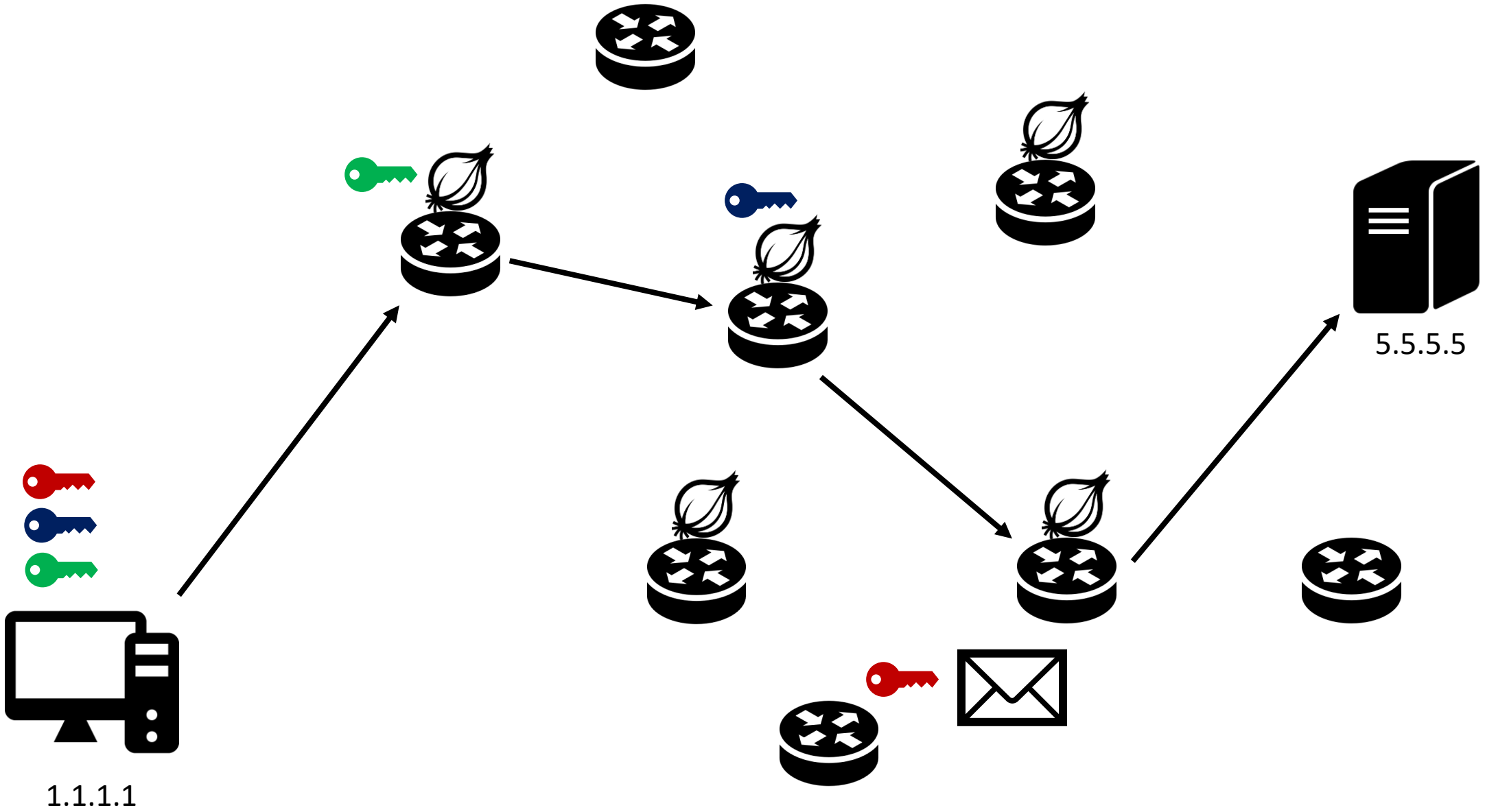
Y lo mandamos



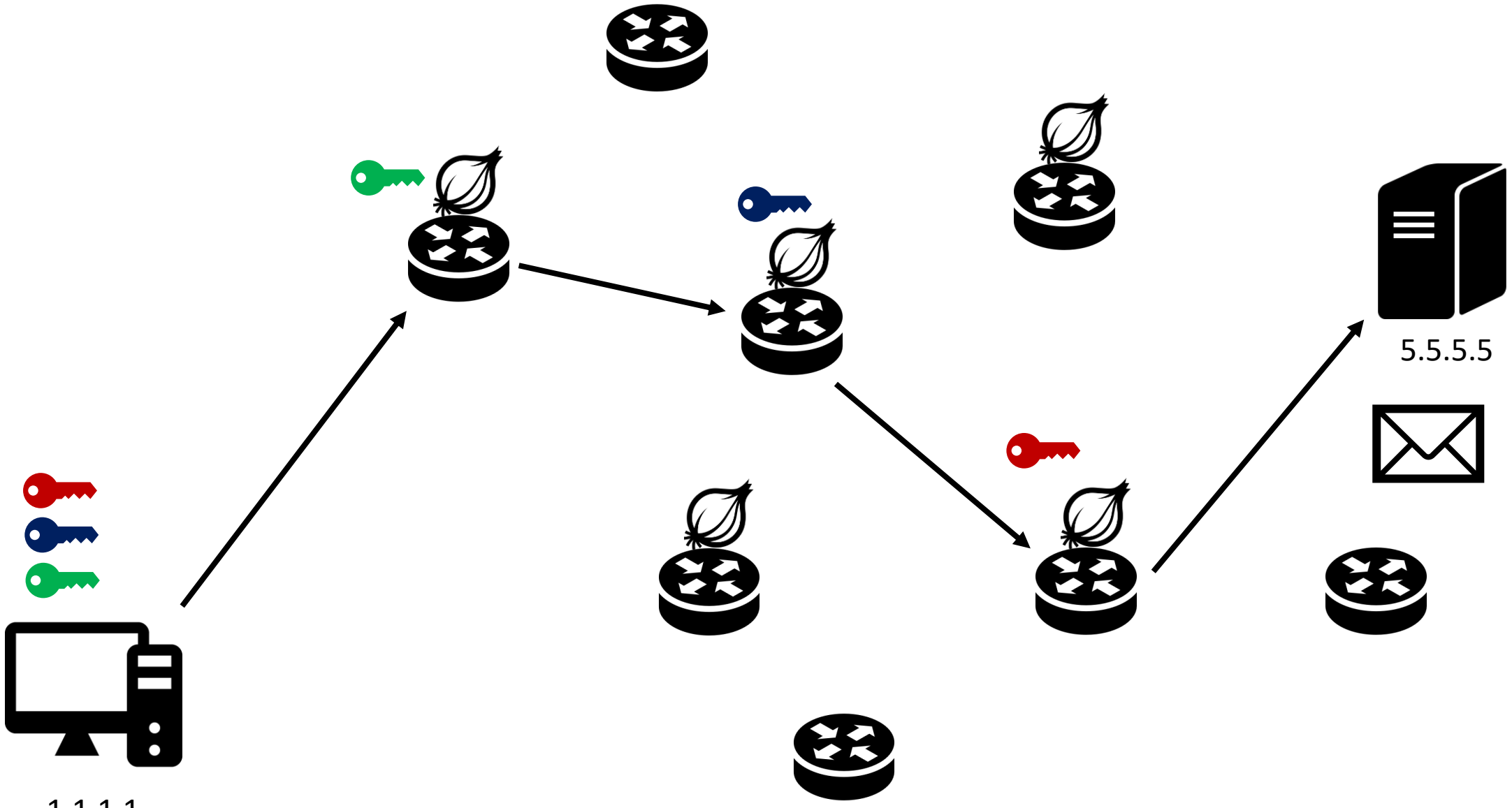
Y lo mandamos



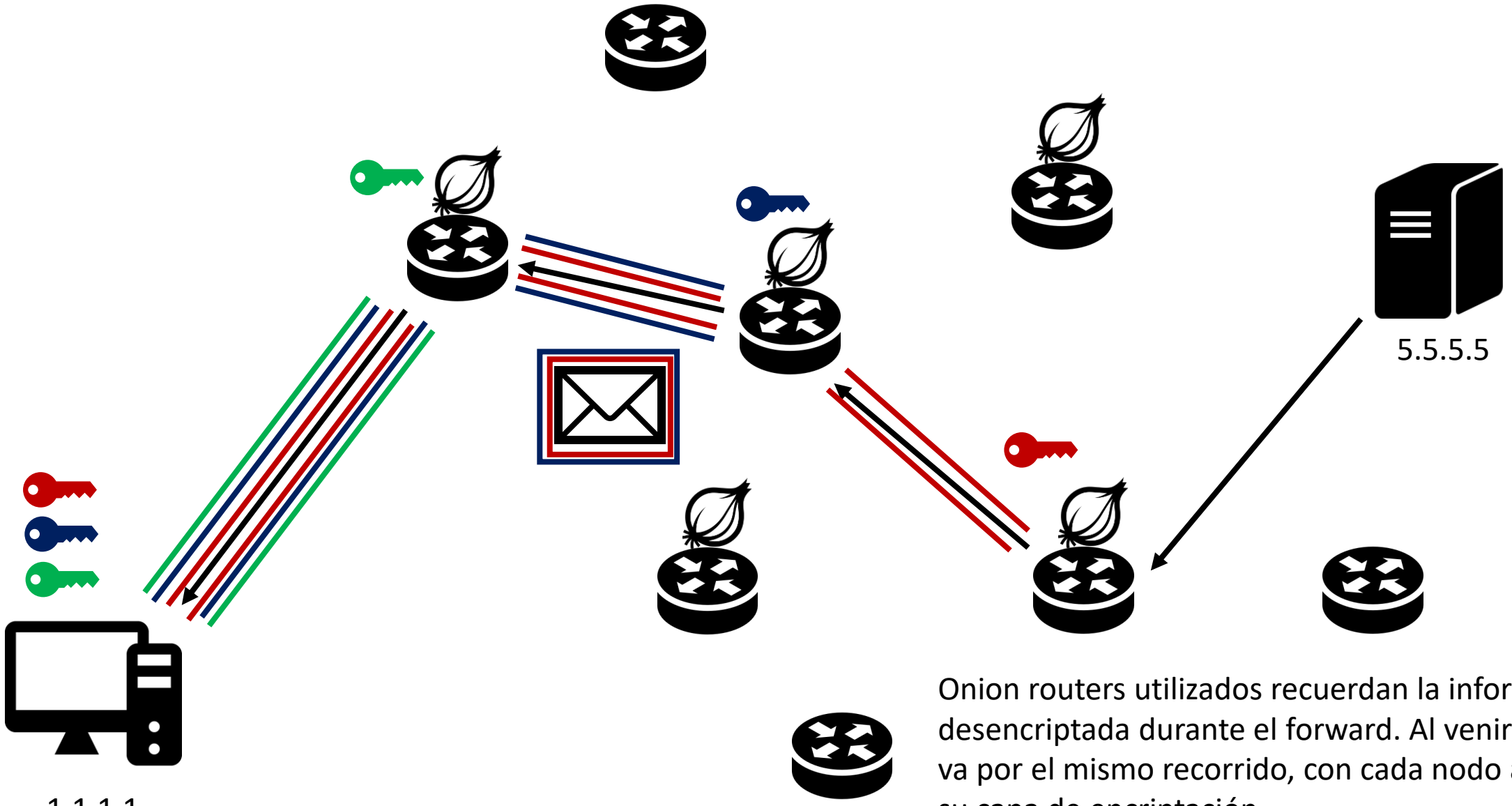
Y lo mandamos



Y ya está!

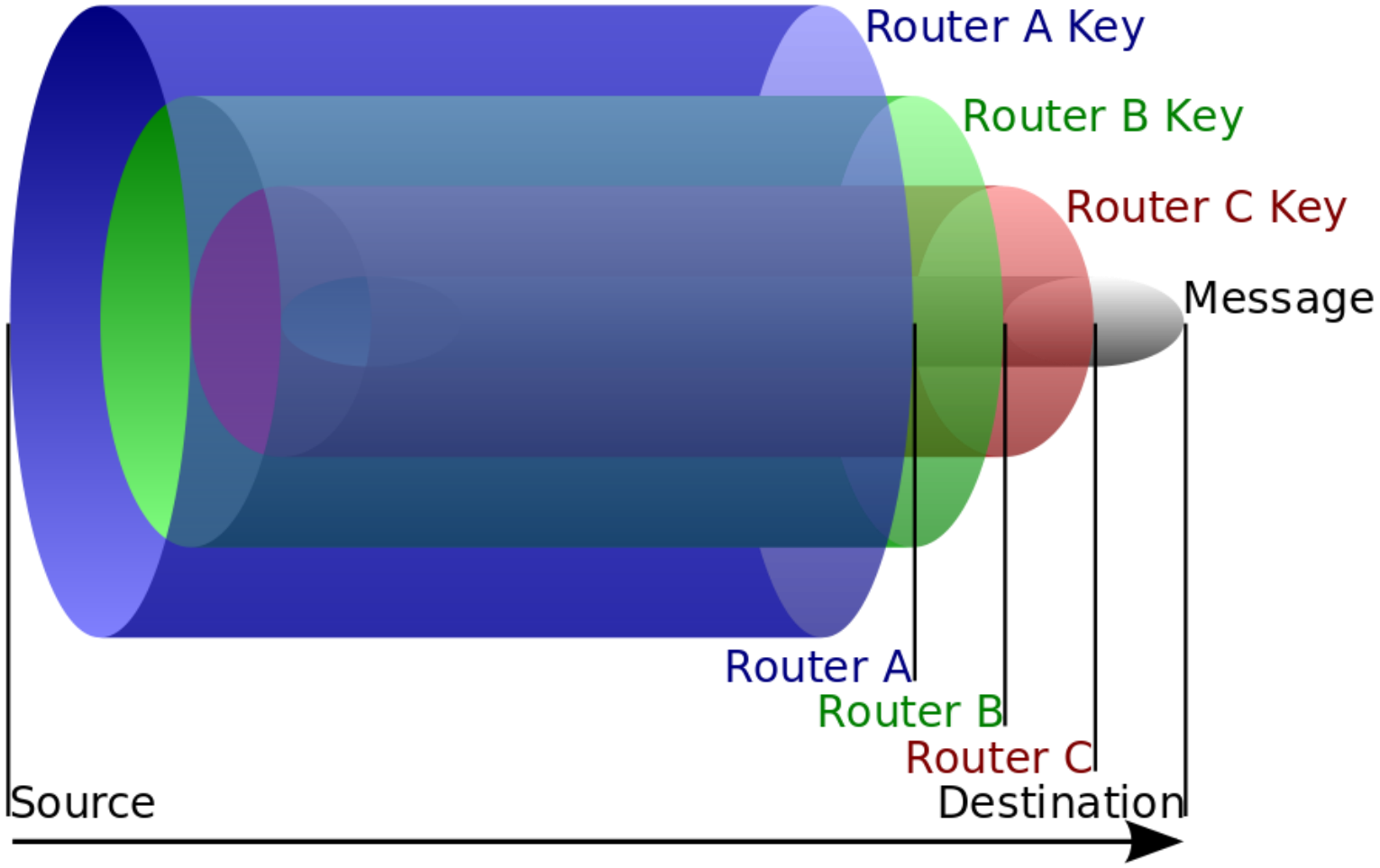


Y de vuelta es lo mismo



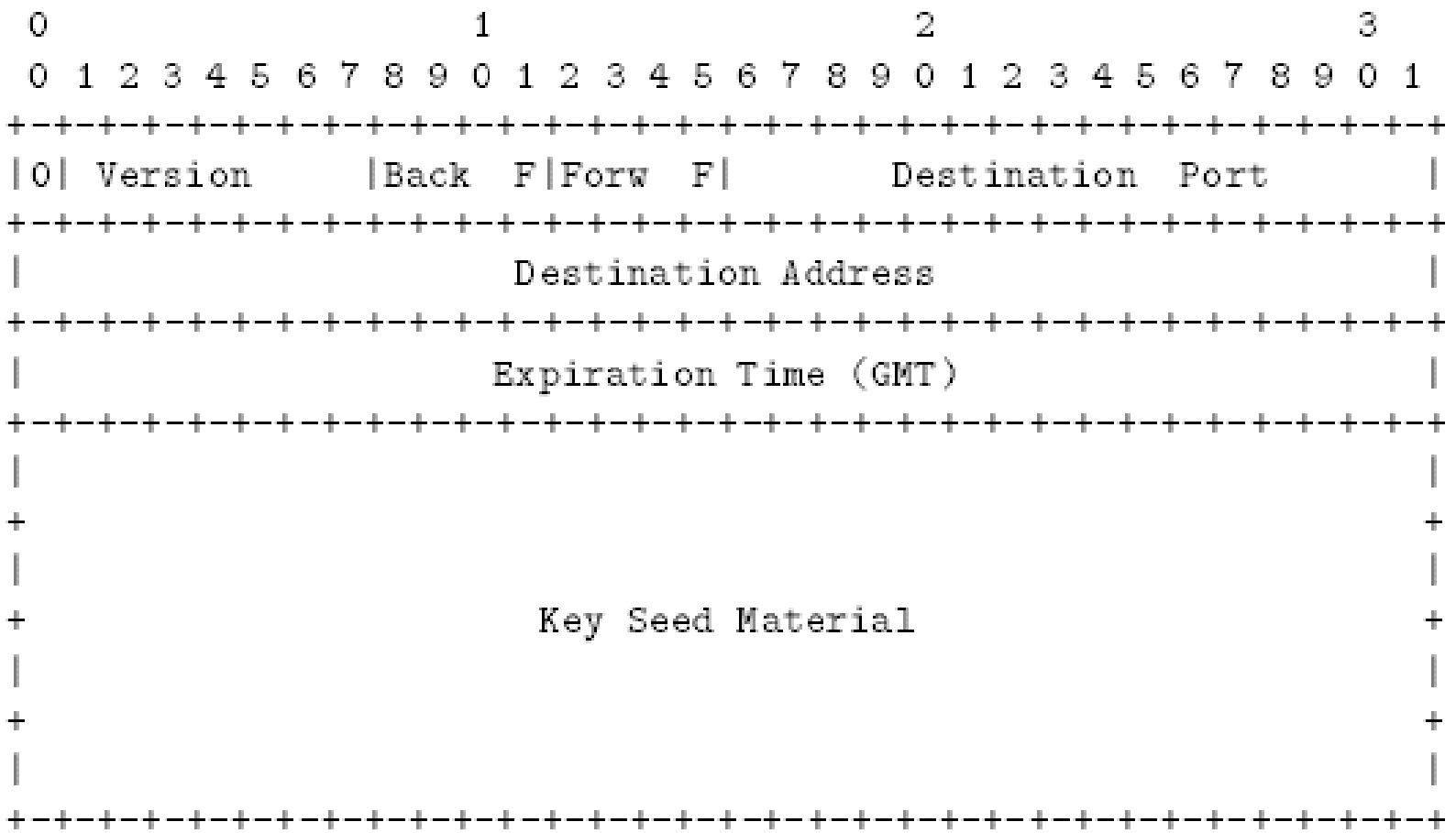
Onion routers utilizados recuerdan la información desencriptada durante el forward. Al venir de vuelta, va por el mismo recorrido, con cada nodo agregando su capa de encriptación.

Onion packet



Fuente: https://en.wikipedia.org/wiki/Onion_routing

Estructura de una capa (ver. 1)



Estructura de una capa (ver. 1)

- Back F y Forw F: funciones criptográficas a aplicar según el “sentido” del paquete (forward = hacia el destinatario).
  - 0: ninguna, 1: DES OFB, 2: RC4
- Destination Port y Address: del onion router siguiente (0 es el de salida).
- Key Seed Material: 128 bits, hasheado 3 veces con SHA para producir 3 llaves

Beneficios y desventajas

- Beneficios:
  - Anonimato: gente externa sólo sabe que “está usando onion routing”
  - Cada router solo sabe del router anterior que vino y al siguiente que debe enviar el paquete
  - Enrutamiento con al menos 3 routers dan un buen rendimiento
- Desventajas:
  - Más lento que comunicación normal
  - Interacción entre el último “onion router” con el servidor destino es común y corriente
  - No protección contra “timing analysis”: encontrar frecuencias de transmisión/tamaño de paquetes similares entre nodos → deducir origen/destino

Referencias

- https://www.onion-router.net/Publications/JSAC-1998.pdf (publicación original)
- https://en.wikipedia.org/wiki/Onion_routing (artículo Wikipedia)
- https://www.torproject.org/docs/faq (FAQ, Tor Project)
- http://sacworkshop.org/SAC15/S3-onion-part1.pdf (Basic Course on Onion Routing, Selected Areas in Cryptography)
- https://www.youtube.com/watch?v=QRYzre4bf7I (Onion Routing, Computerphile)
- https://pando.com/2014/07/16/tor-spooks/ (“*Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government*”, Pando)