Tor

Cenni storici

Tor nasce da un progetto dagli U.S. Naval Research Laboratory, come strumento dedicato alla mirina militare.

Era un servizio primario per la protezione delle comunicazioni governative.

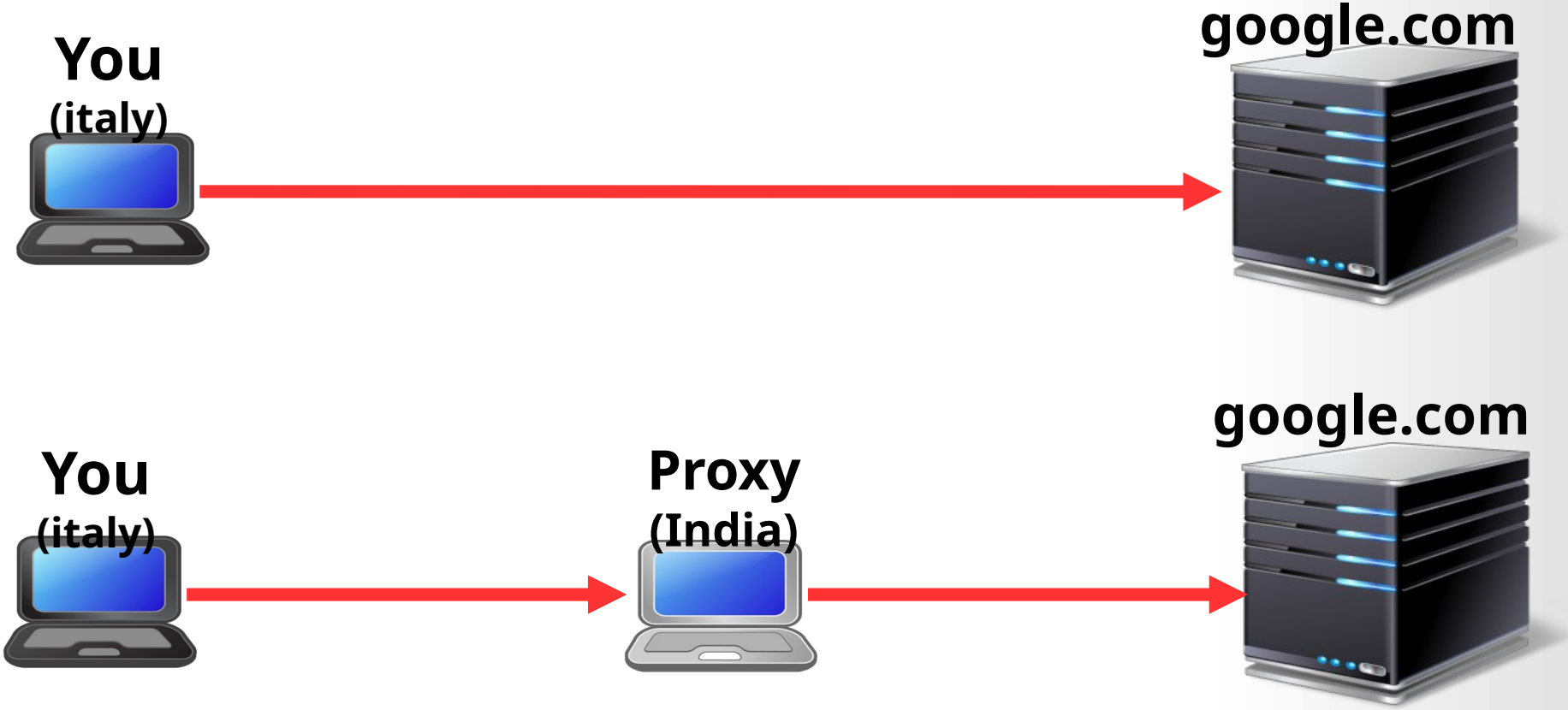
Oggi è un progetto open-source disponibile per chiunque, sviluppato dalla The Tor Project, un' associazione senza scopo di lucro. Viene utilizzato da giornalisti, militari, forze dell'ordine, whistleblower, infiltrati e sopratutto dagli hacktivisti.

Concetti Di Base

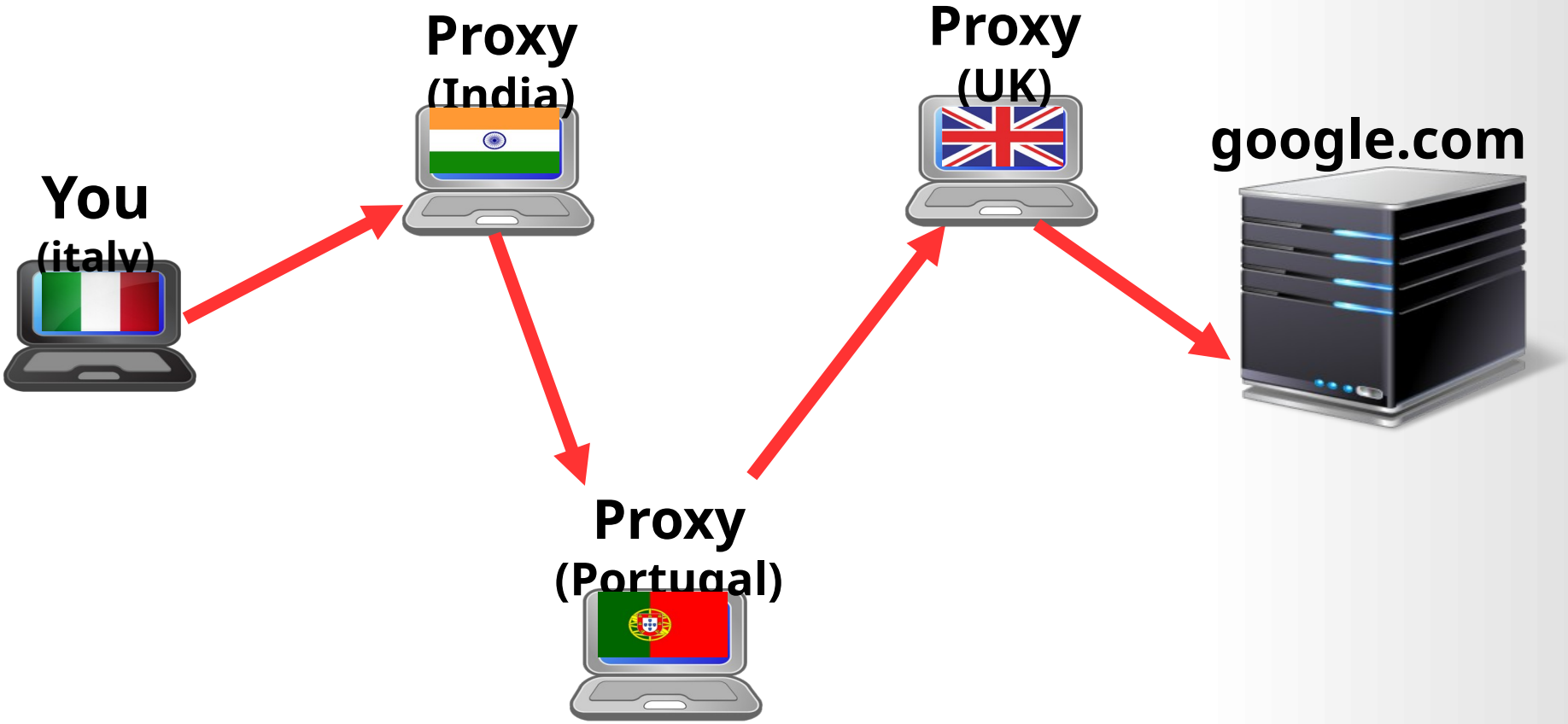
- Proxy
- Crittografia Asimmetrica
- Crittografia Asimmetrica su più livelli

Proxy

Proxy



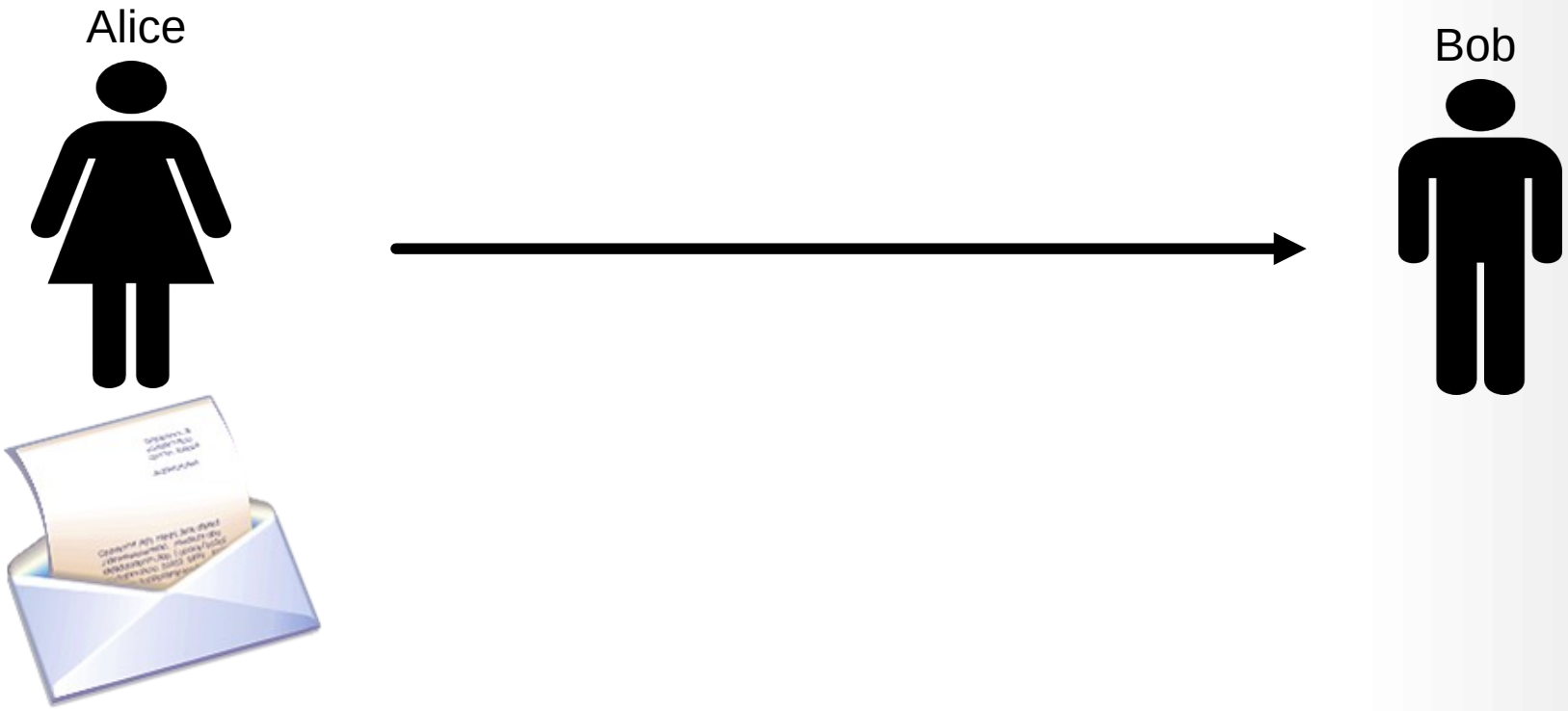
Proxy



Concetti Di Base

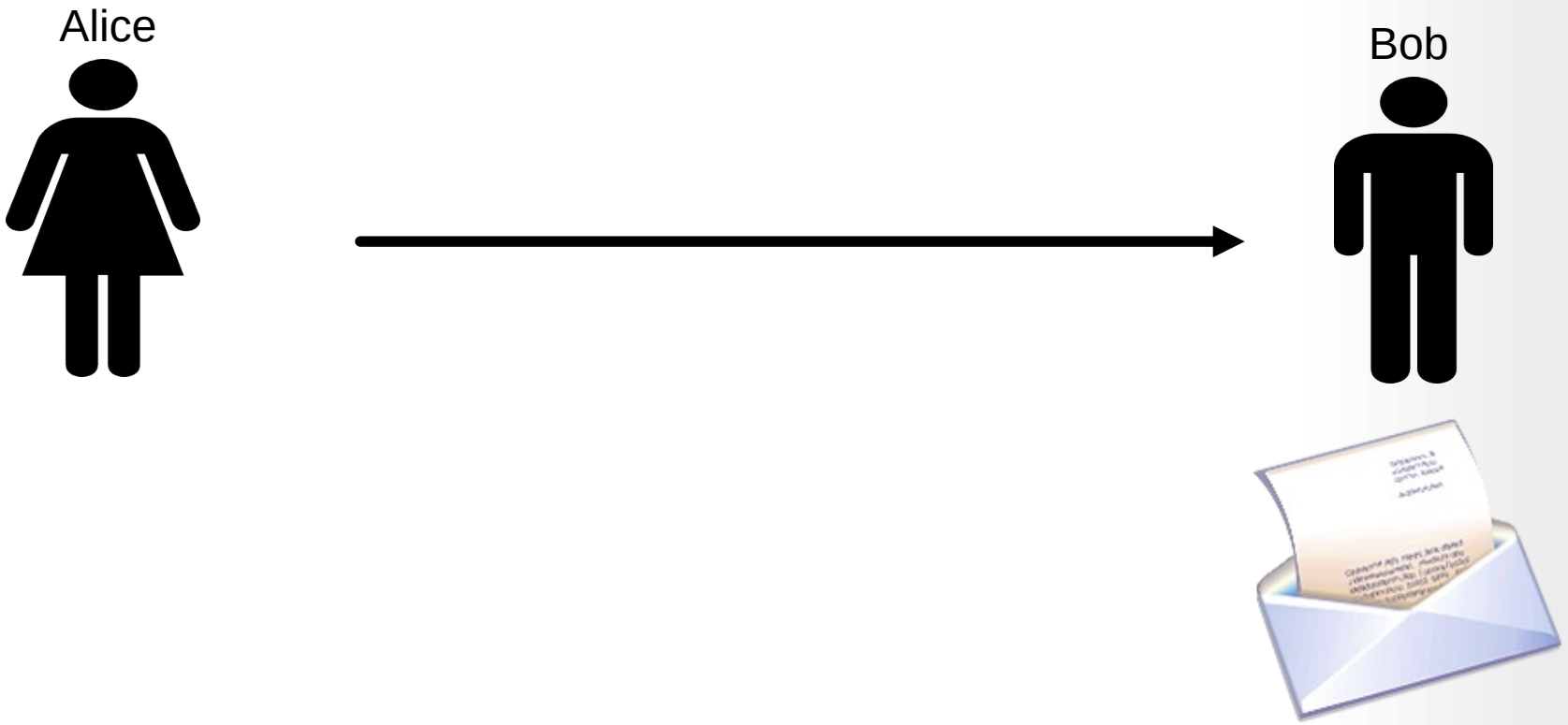
- ~~Proxy~~
- Crittografia Asimmetrica
- Crittografia Asimmetrica su più livelli

Crittografia Asimmetrica

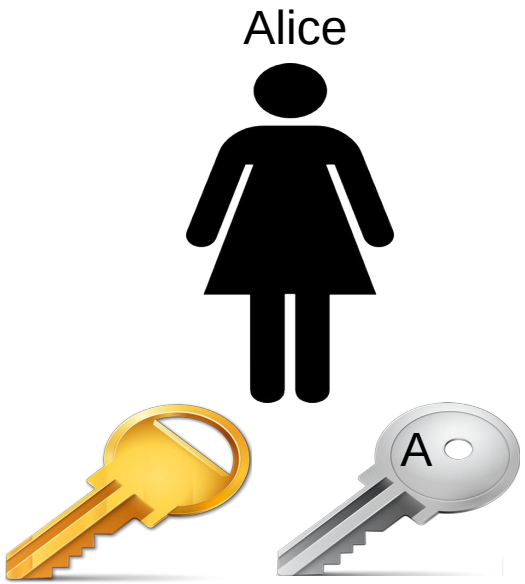


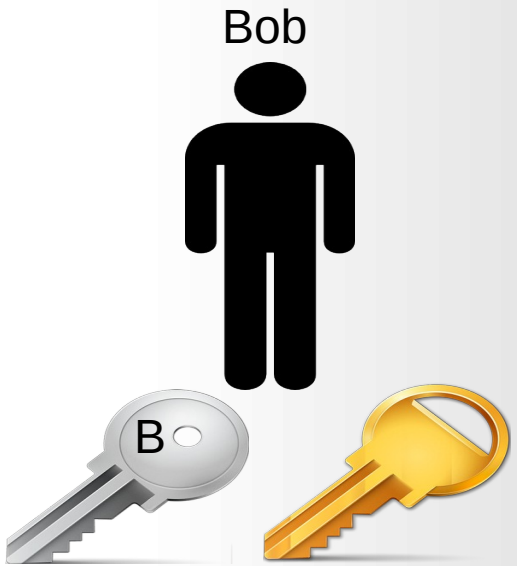
Crittografia Asimmetrica

Crittografia Asimmetrica

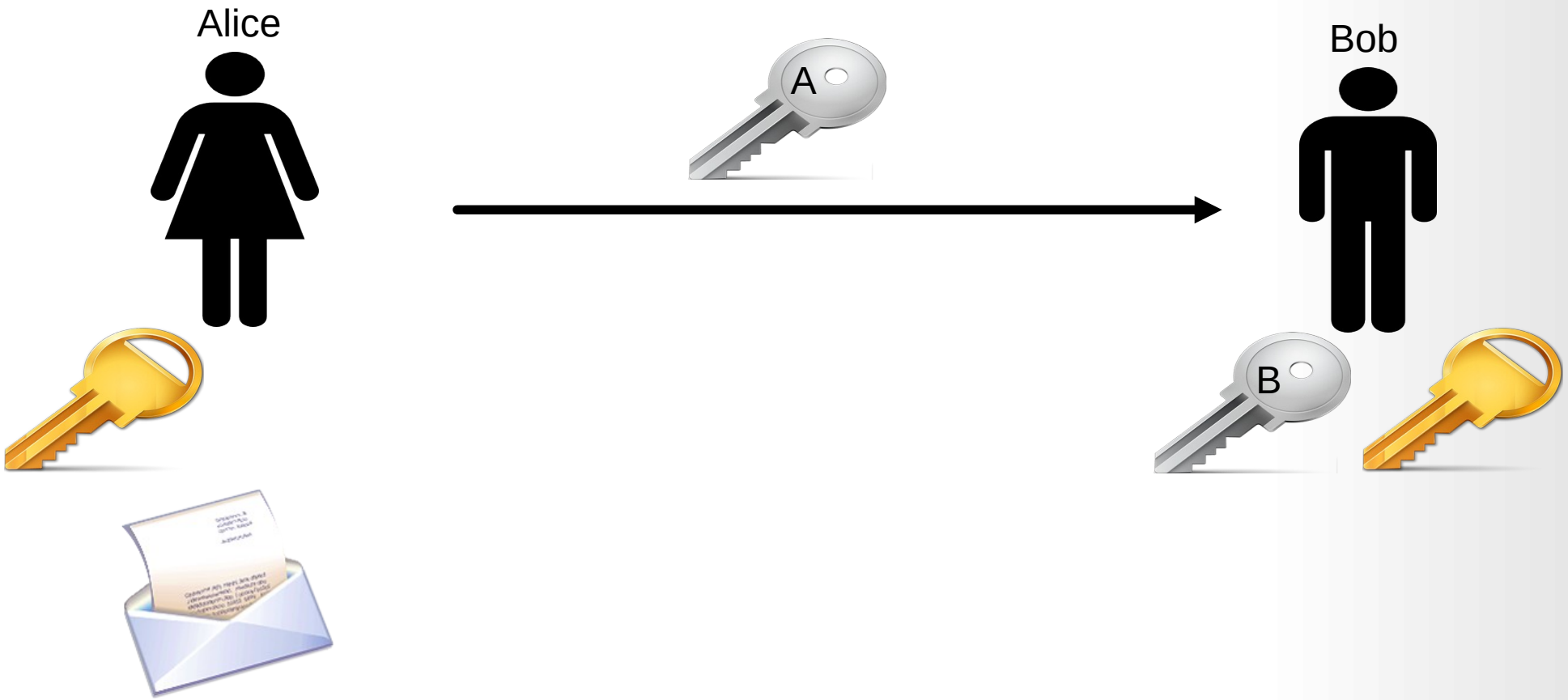


Crittografia Asimmetrica

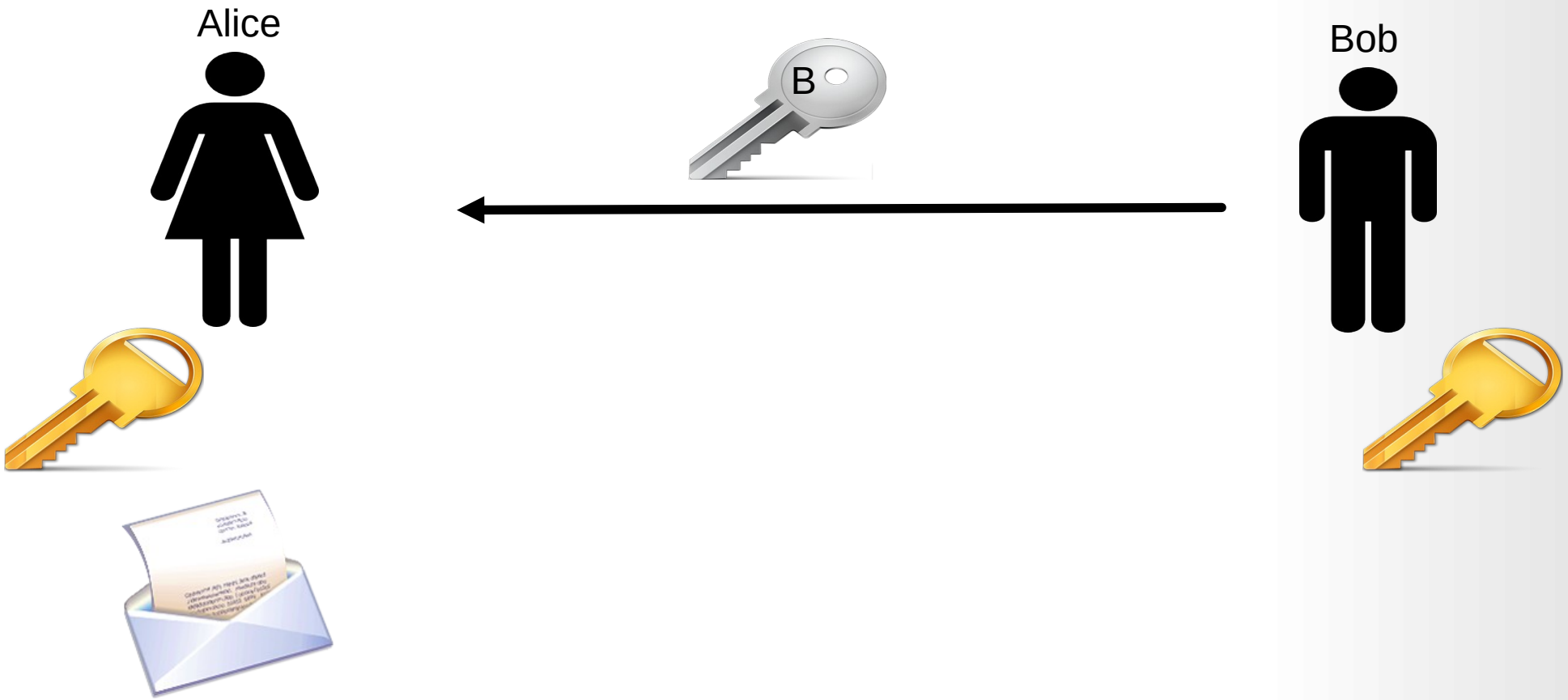




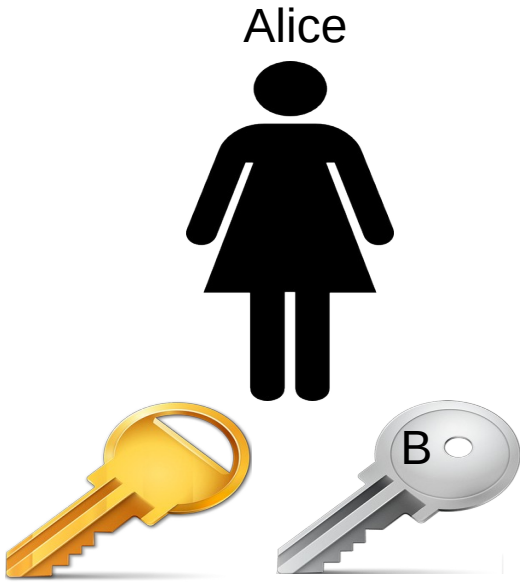
Crittografia Asimmetrica



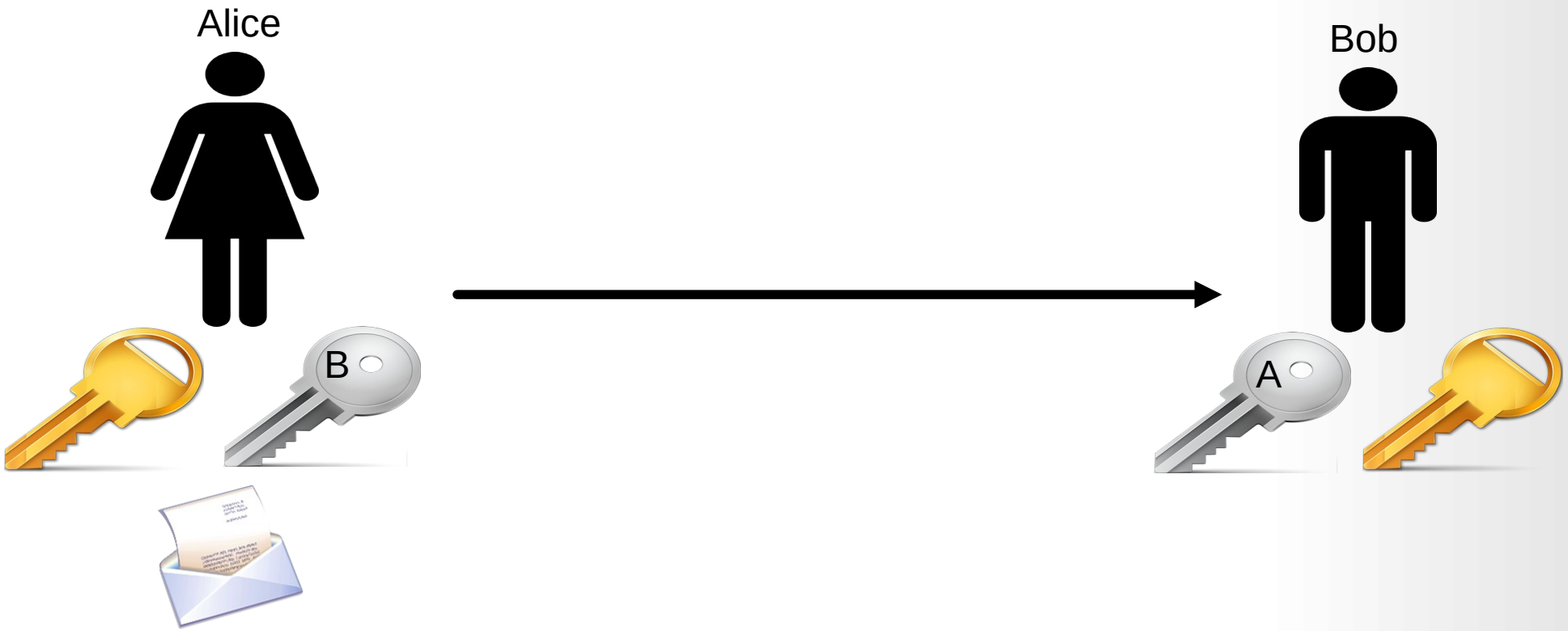
Crittografia Asimmetrica



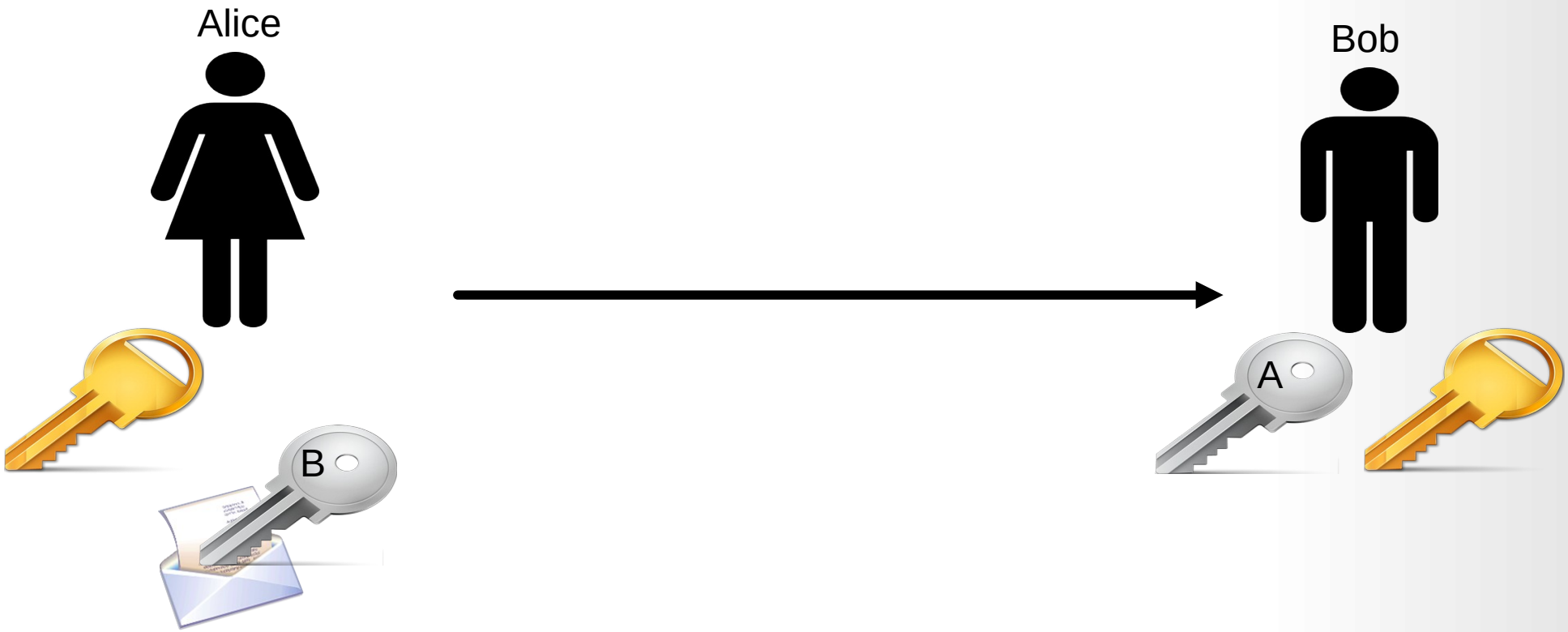
Crittografia Asimmetrica



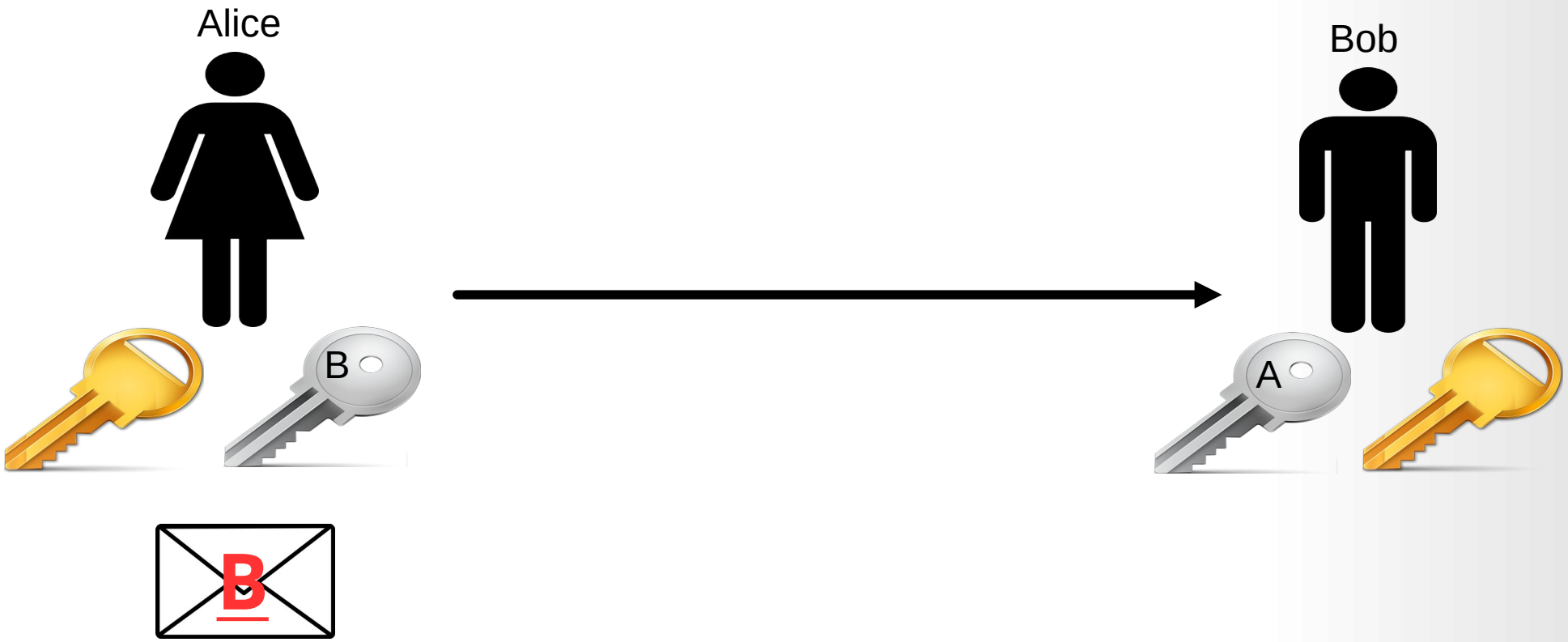
Crittografia Asimmetrica



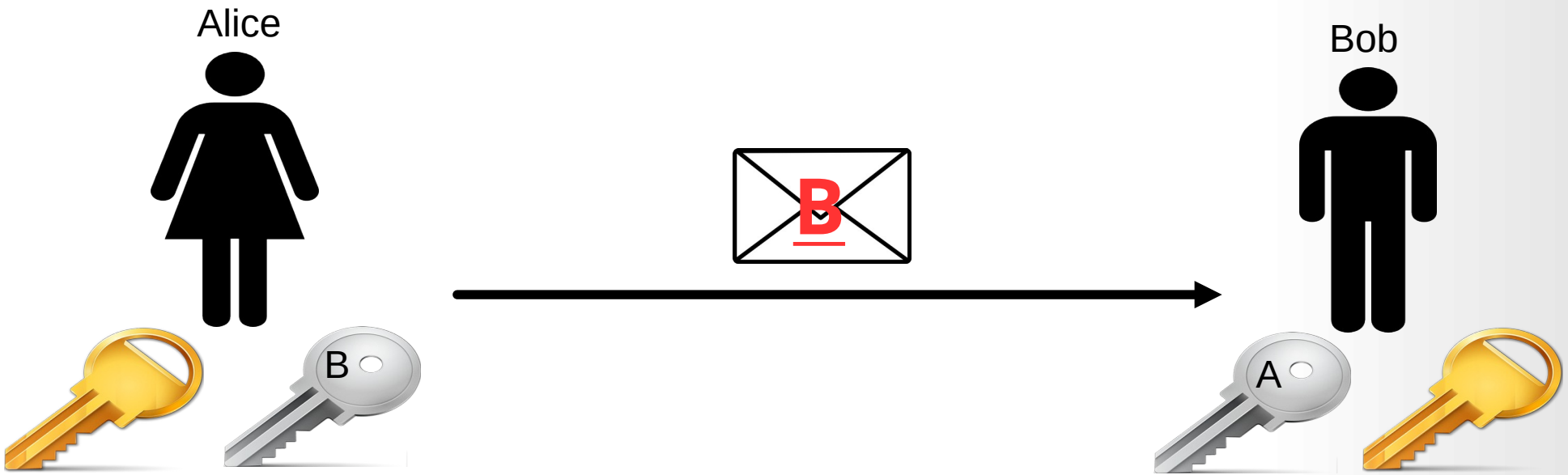
Crittografia Asimmetrica



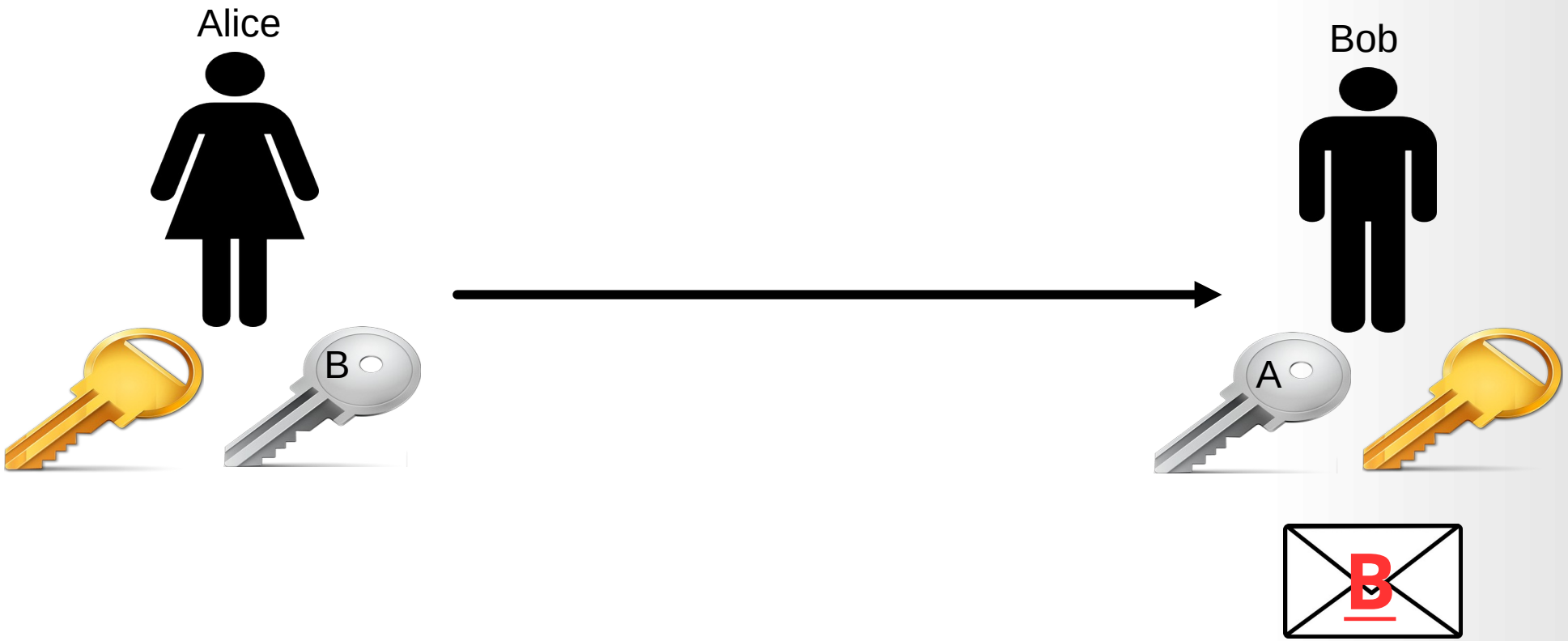
Crittografia Asimmetrica



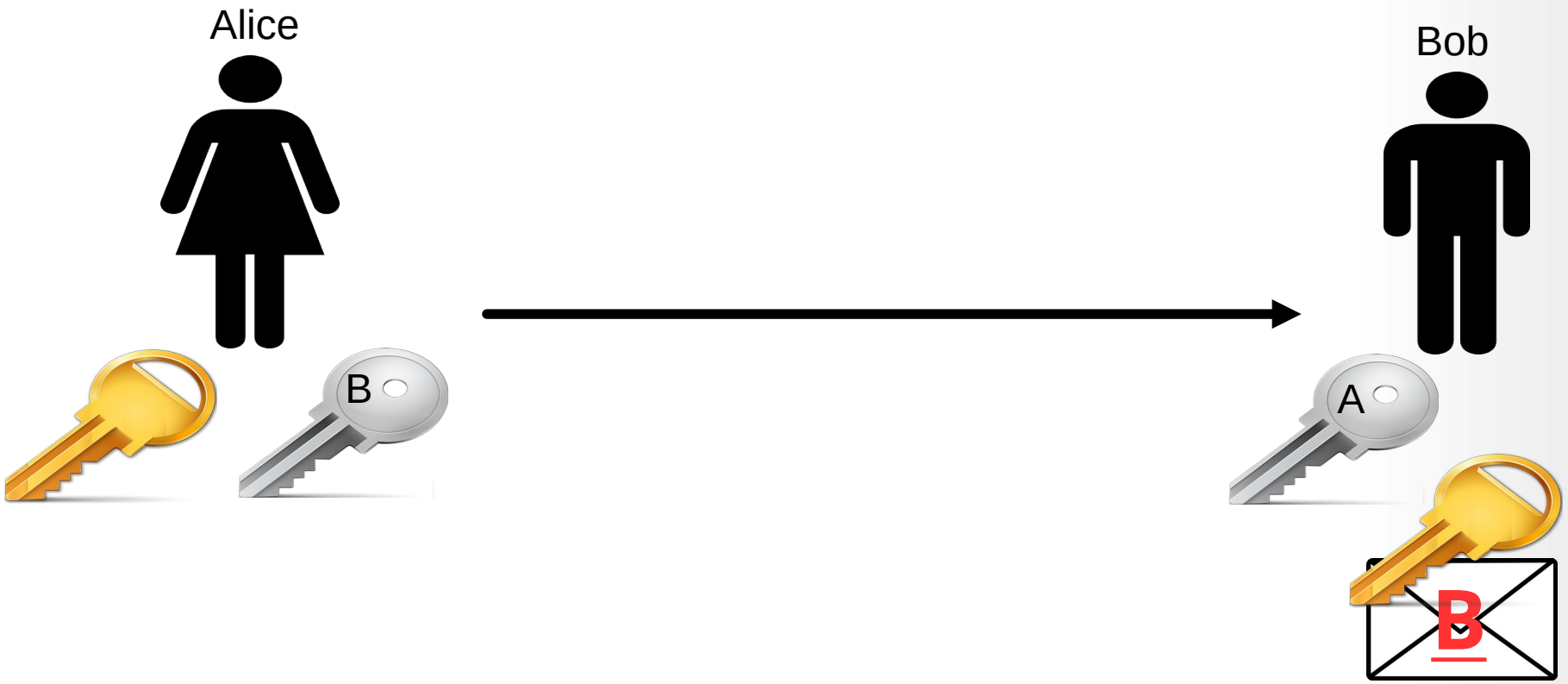
Crittografia Asimmetrica



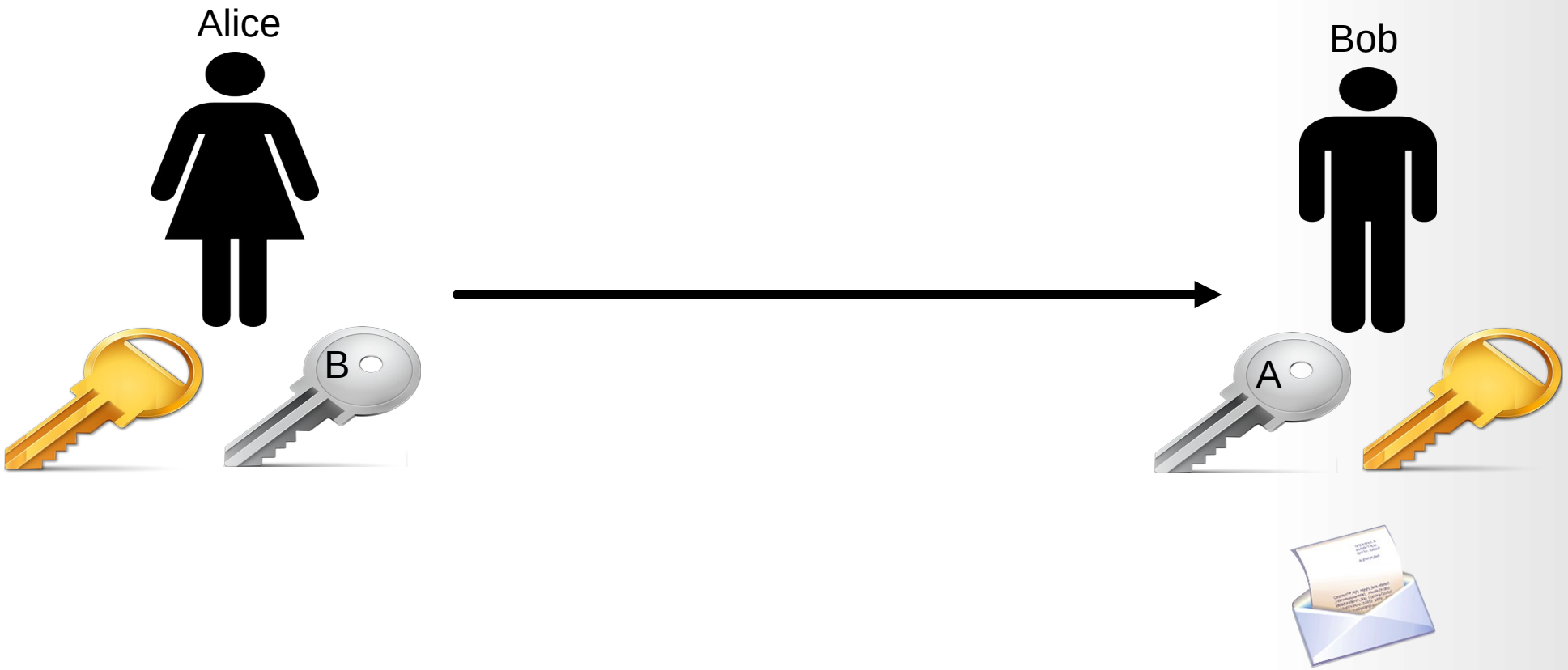
Crittografia Asimmetrica



Crittografia Asimmetrica



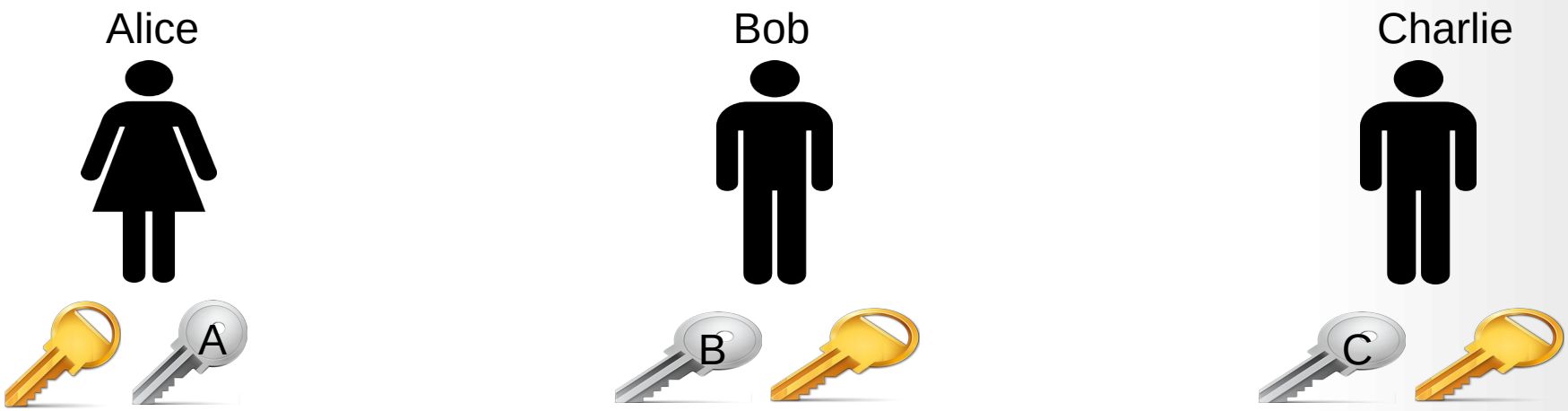
Crittografia Asimmetrica



Concetti Di Base

- ~~Proxy~~
- ~~Crittografia Asimmetrica~~
- Crittografia Asimmetrica su più livelli

Crittografia Asimmetrica++



Crittografia Asimmetrica++

Alice

Bob

Charlie

Crittografia Asimmetrica++

Alice

Bob

Charlie

Crittografia Asimmetrica++

Alice

Bob

Charlie

Crittografia Asimmetrica++

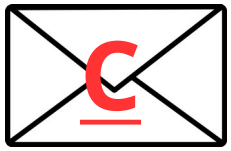
Alice

Bob

Charlie

Crittografia Asimmetrica++

Alice



Bob

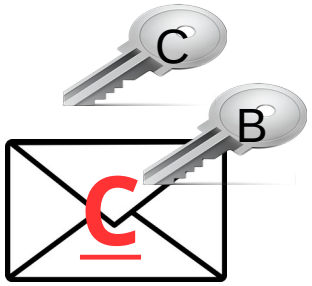
Charlie

Crittografia Asimmetrica++

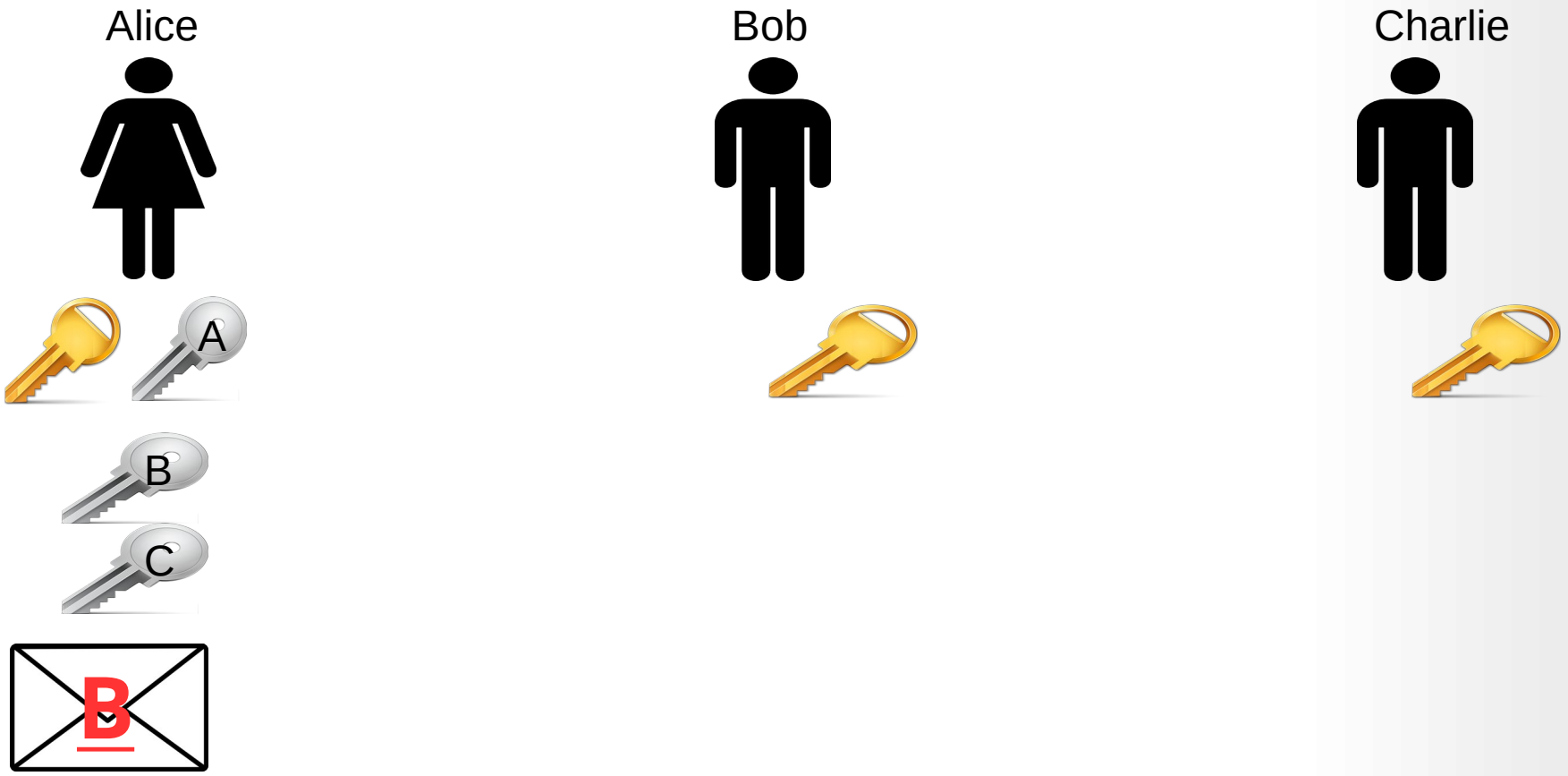
Alice

Bob

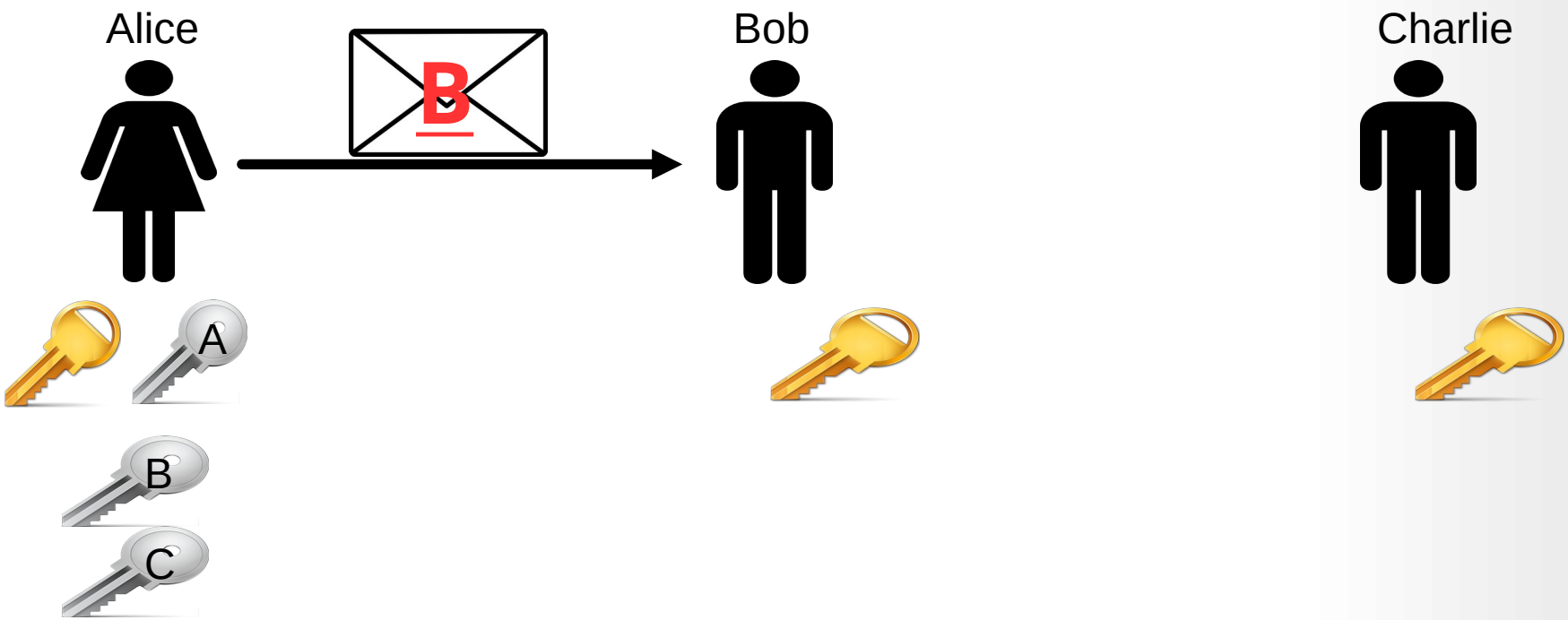
Charlie



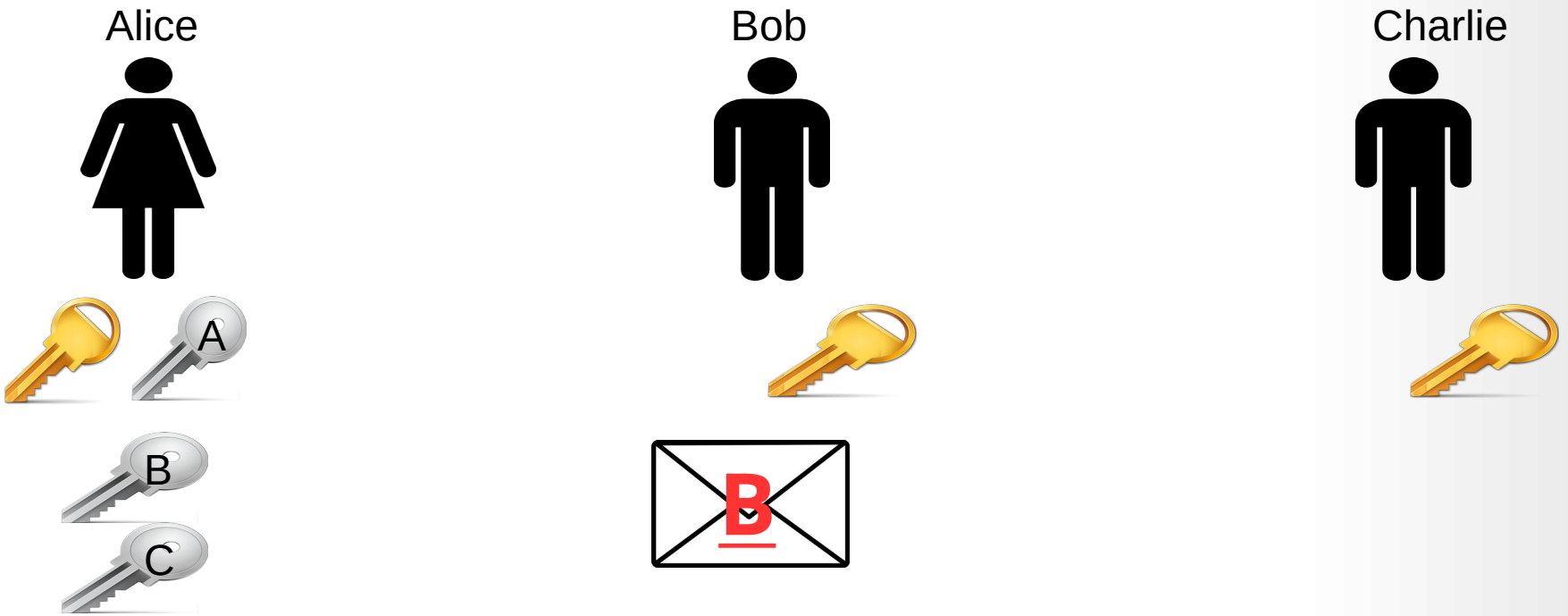
Crittografia Asimmetrica++



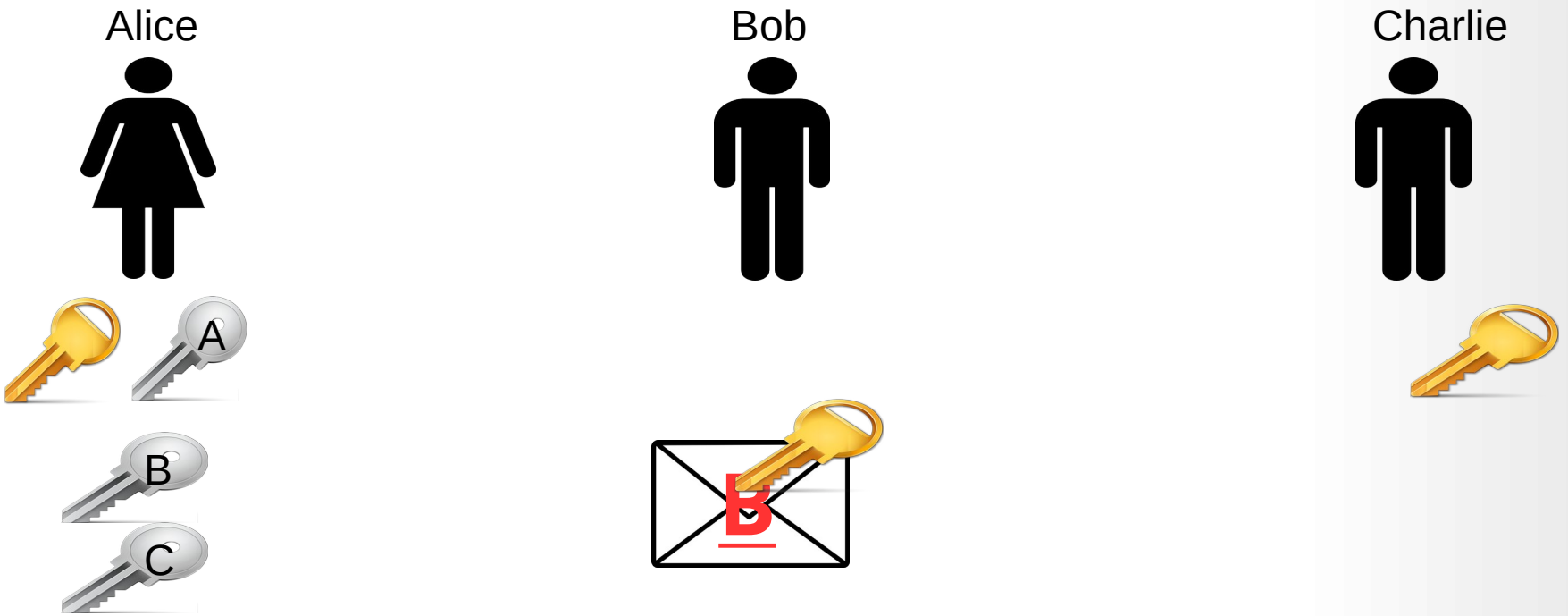
Crittografia Asimmetrica++



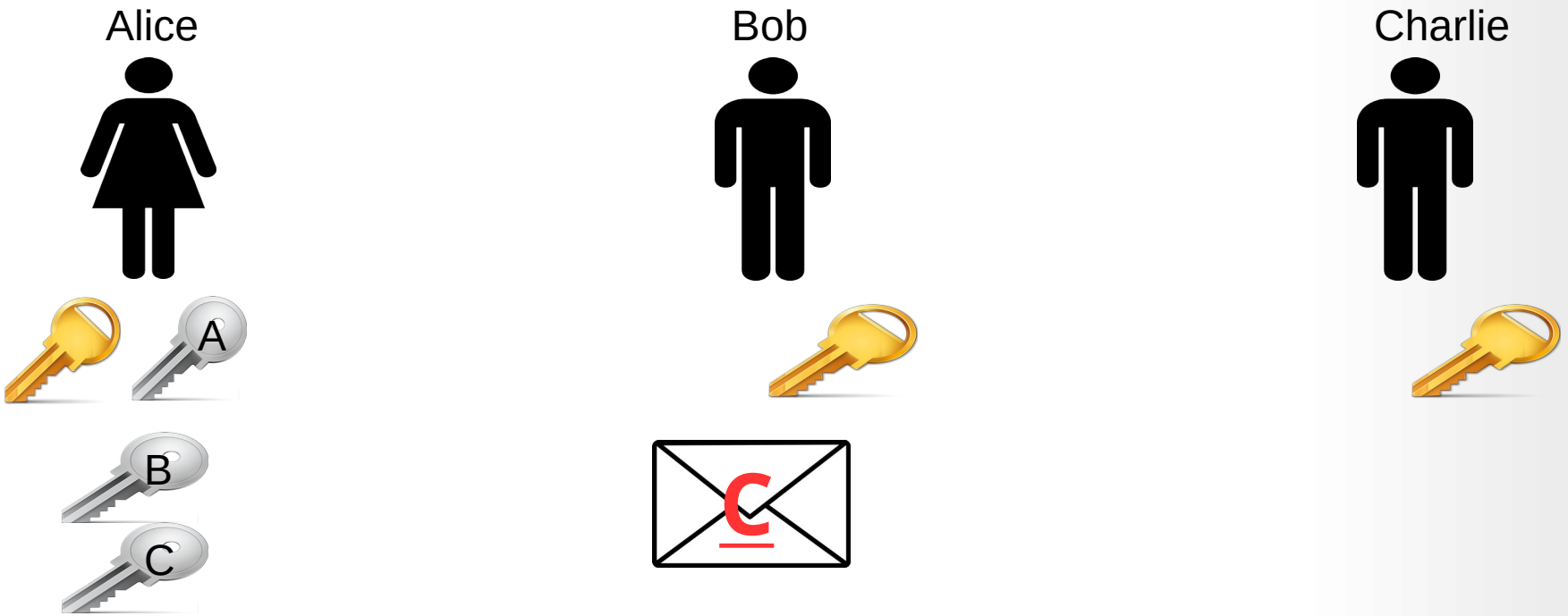
Crittografia Asimmetrica++



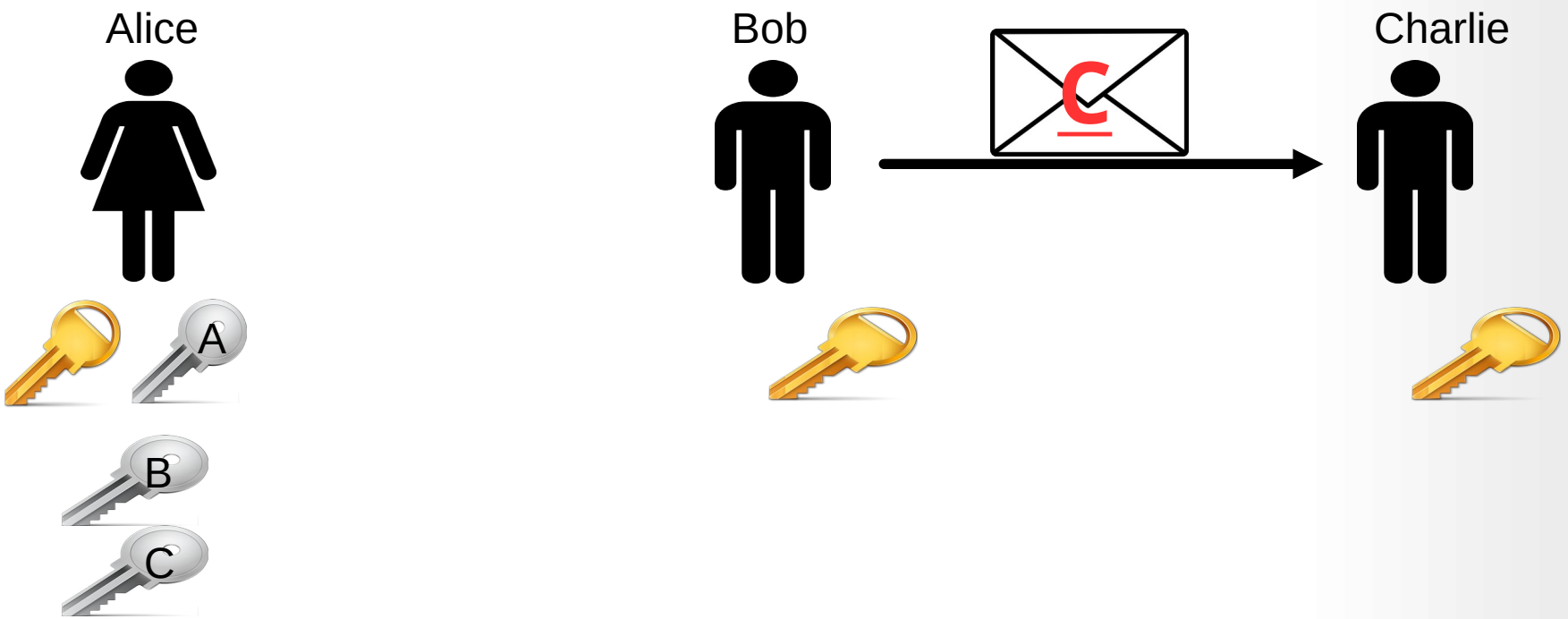
Crittografia Asimmetrica++



Crittografia Asimmetrica++

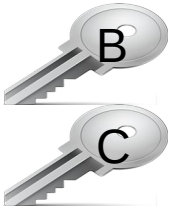


Crittografia Asimmetrica++



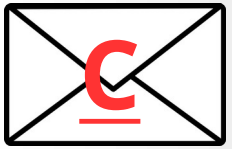
Crittografia Asimmetrica++

Alice

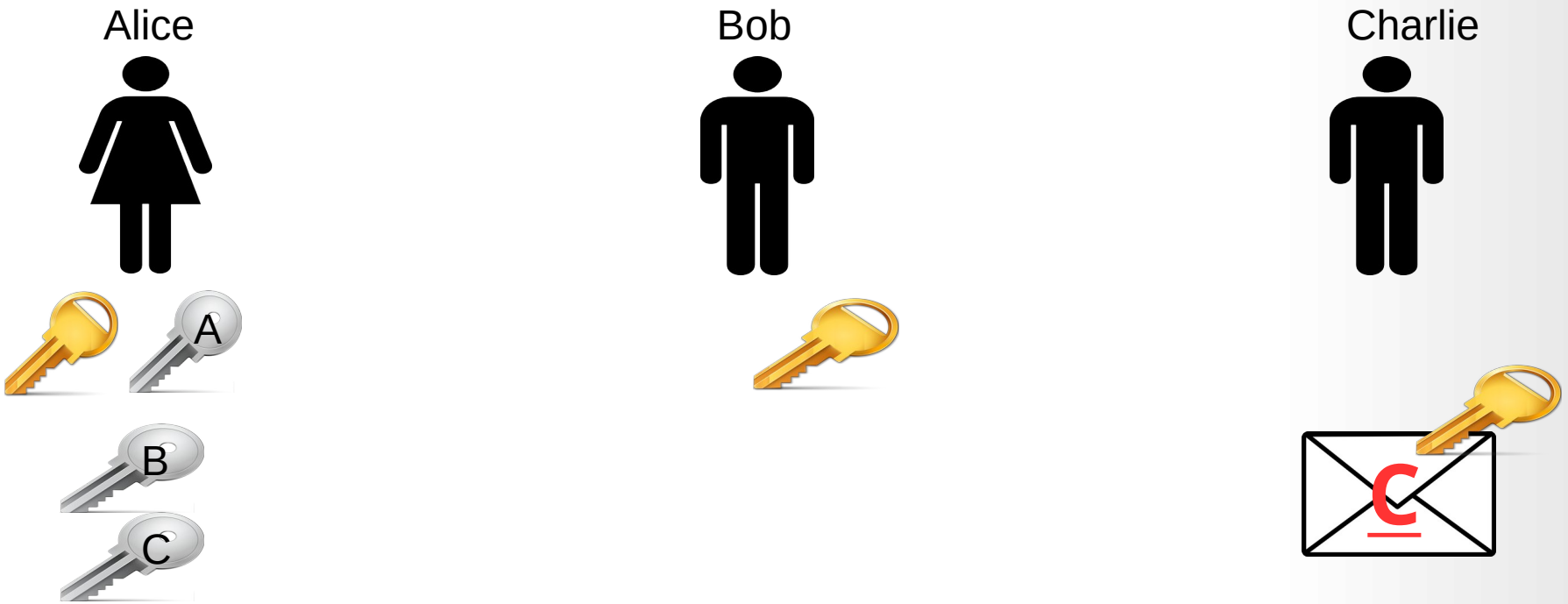


Bob

Charlie

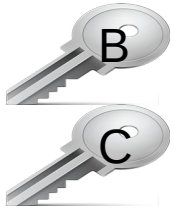


Crittografia Asimmetrica++



Crittografia Asimmetrica++

Alice



Bob

Charlie

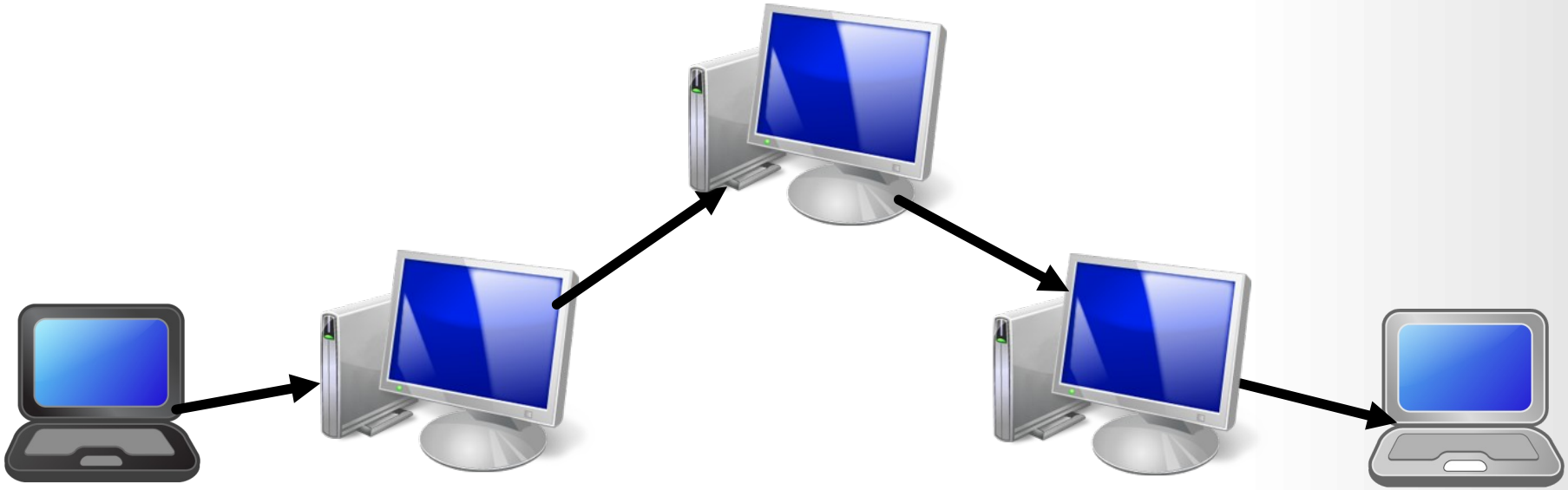
Concetti Di Base

- ~~Proxy~~
- ~~Crittografia Asimmetrica~~
- ~~Crittografia Asimmetrica su più livelli~~

Tor

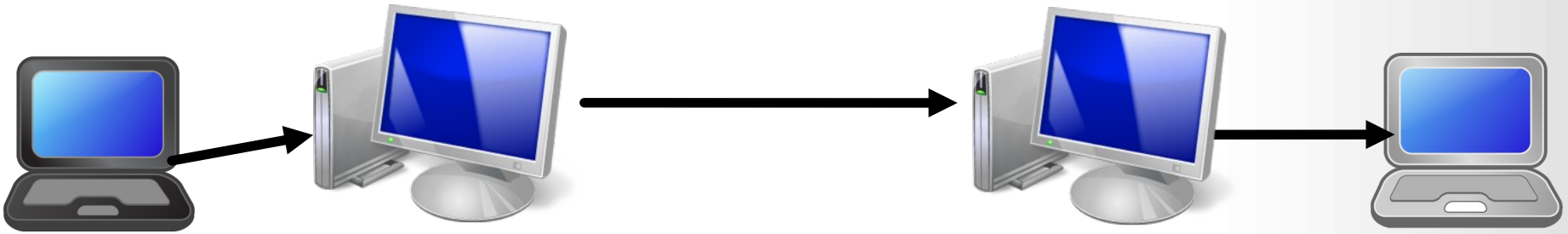
- Il circuito Tor
- Instaurazione di un Hidden Service
- Indirizzi .onion V3
- Connessione ad un Hidden Service
- Bridge
- Pericoli

Circuito Tor



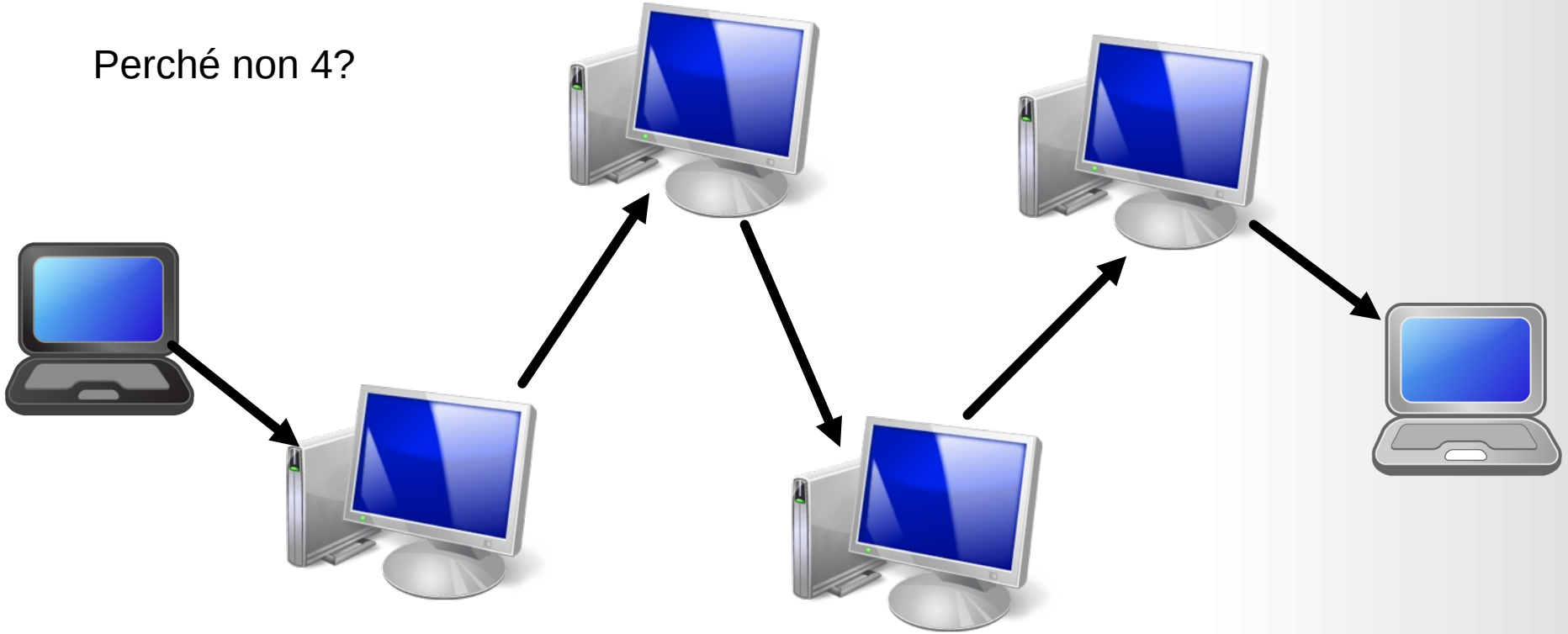
Circuito Tor

Perché non 2?

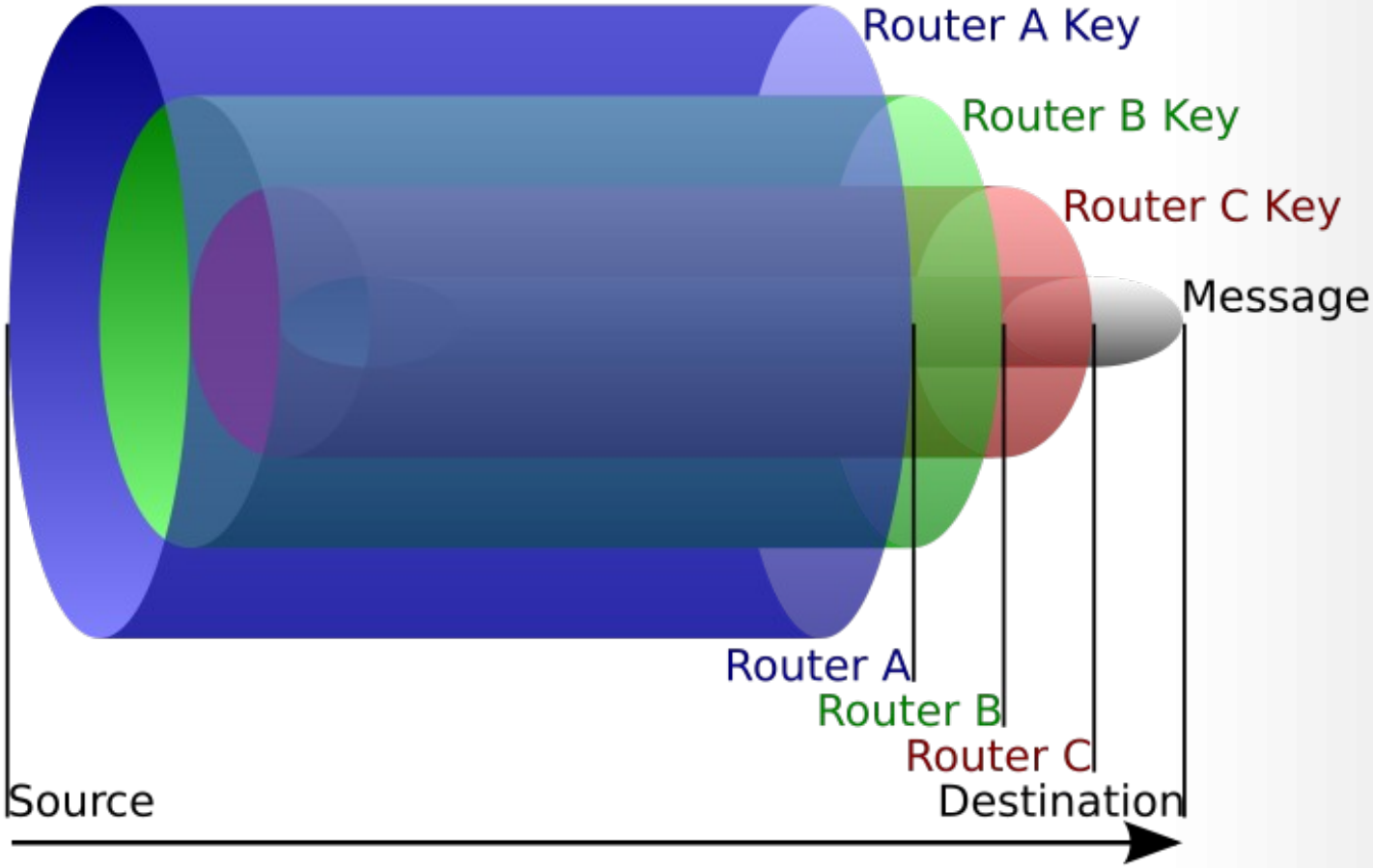


Circuito Tor

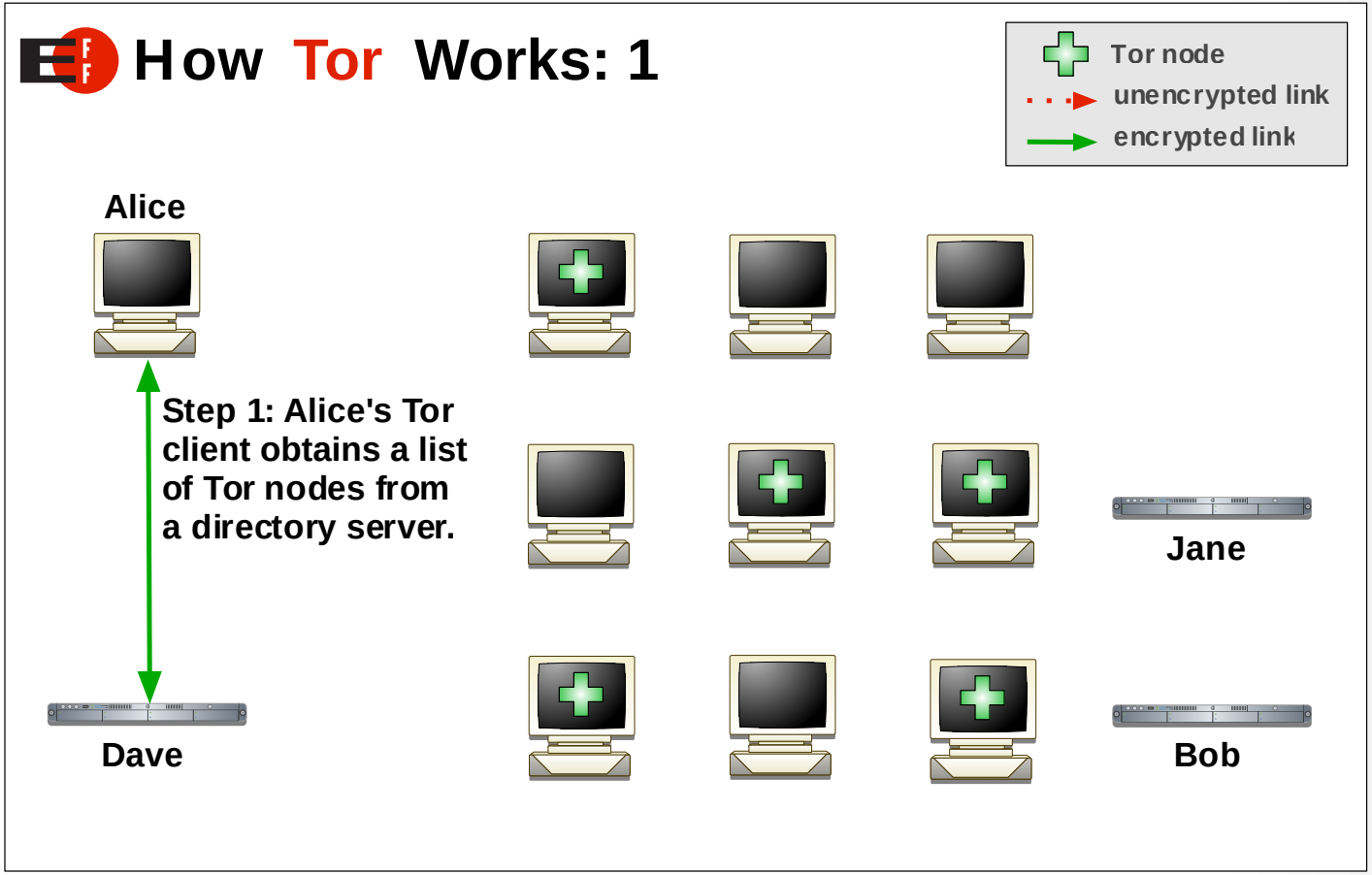
Perché non 4?



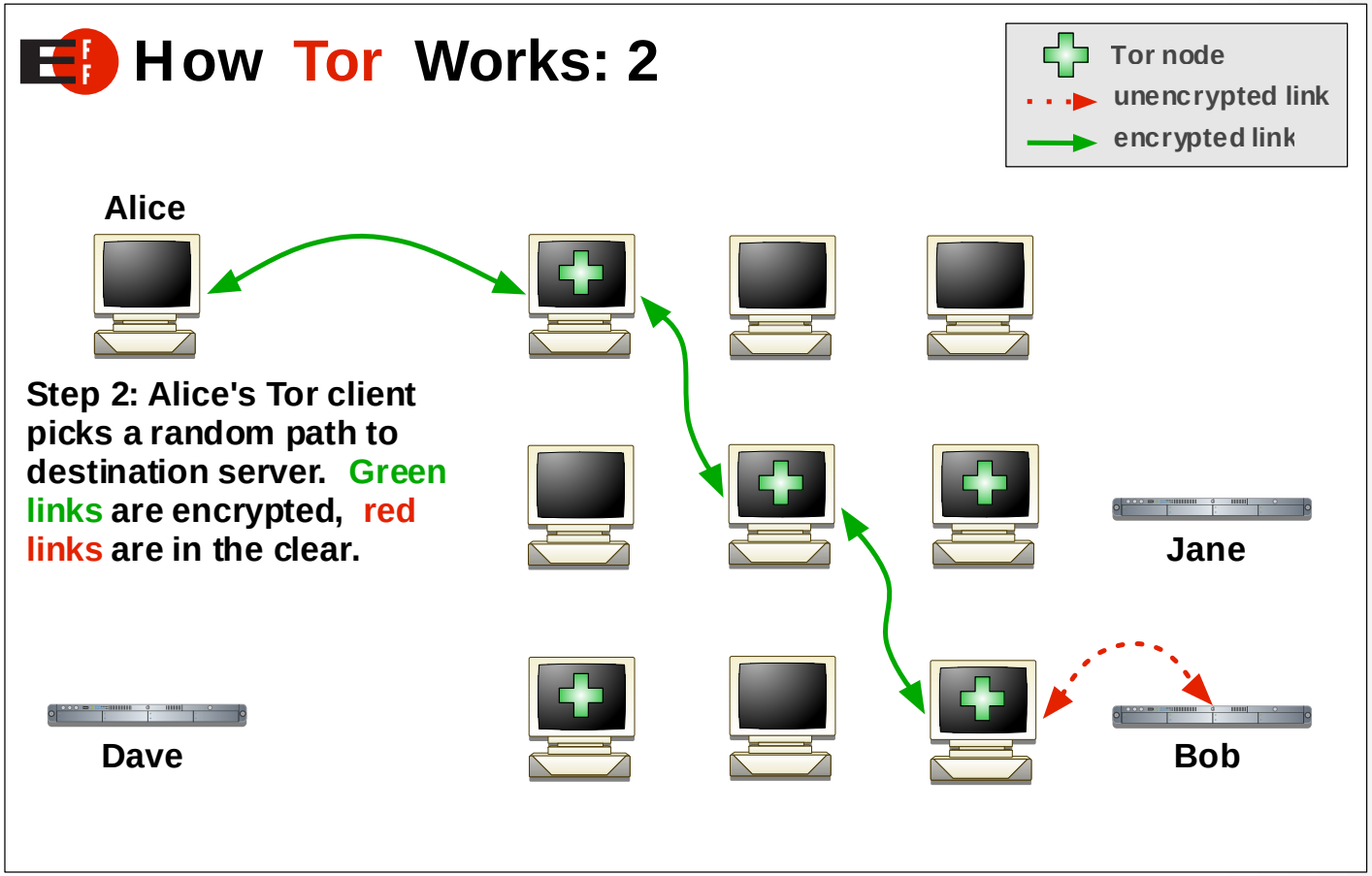
Circuito Tor



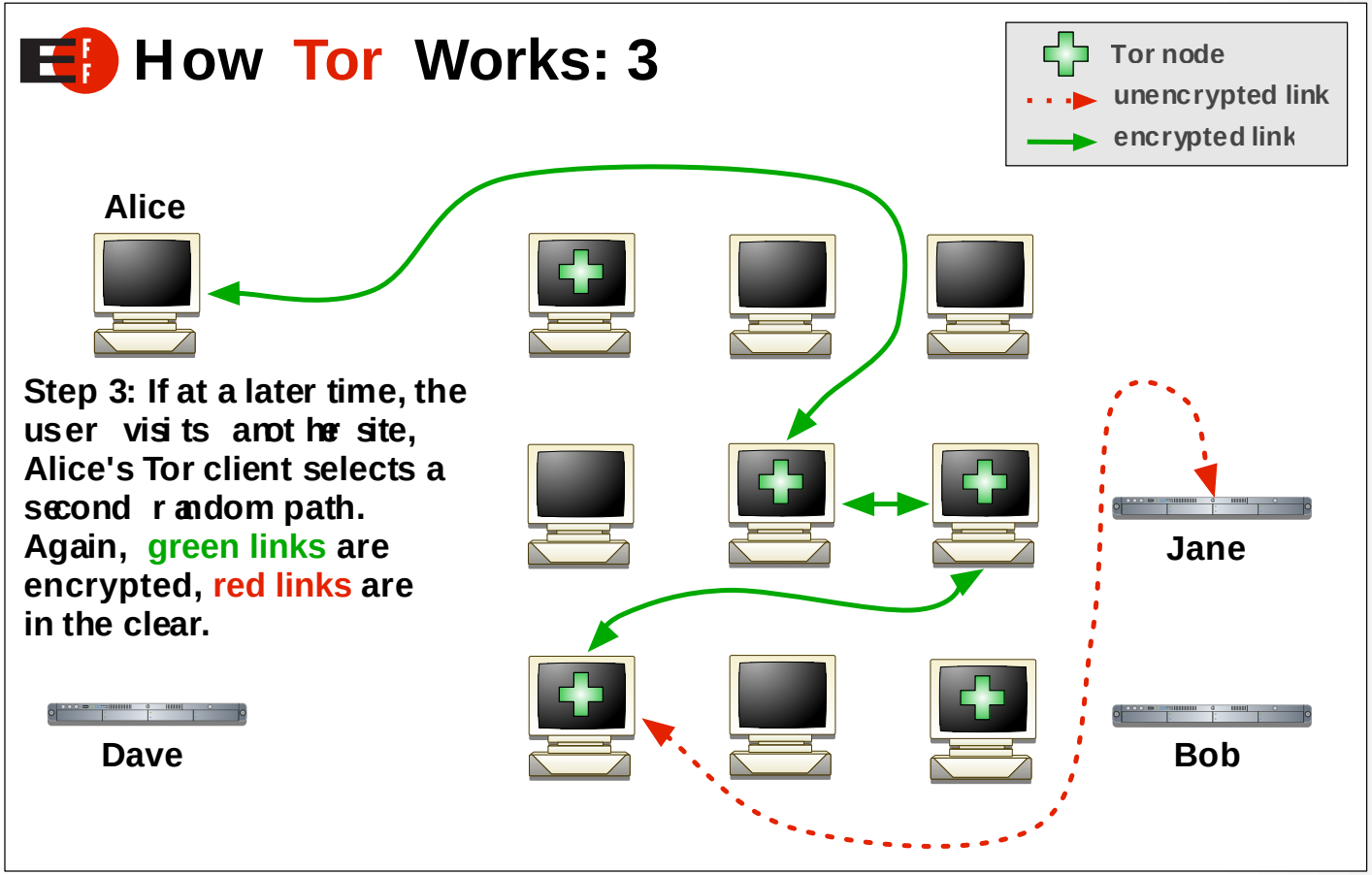
Circuito Tor



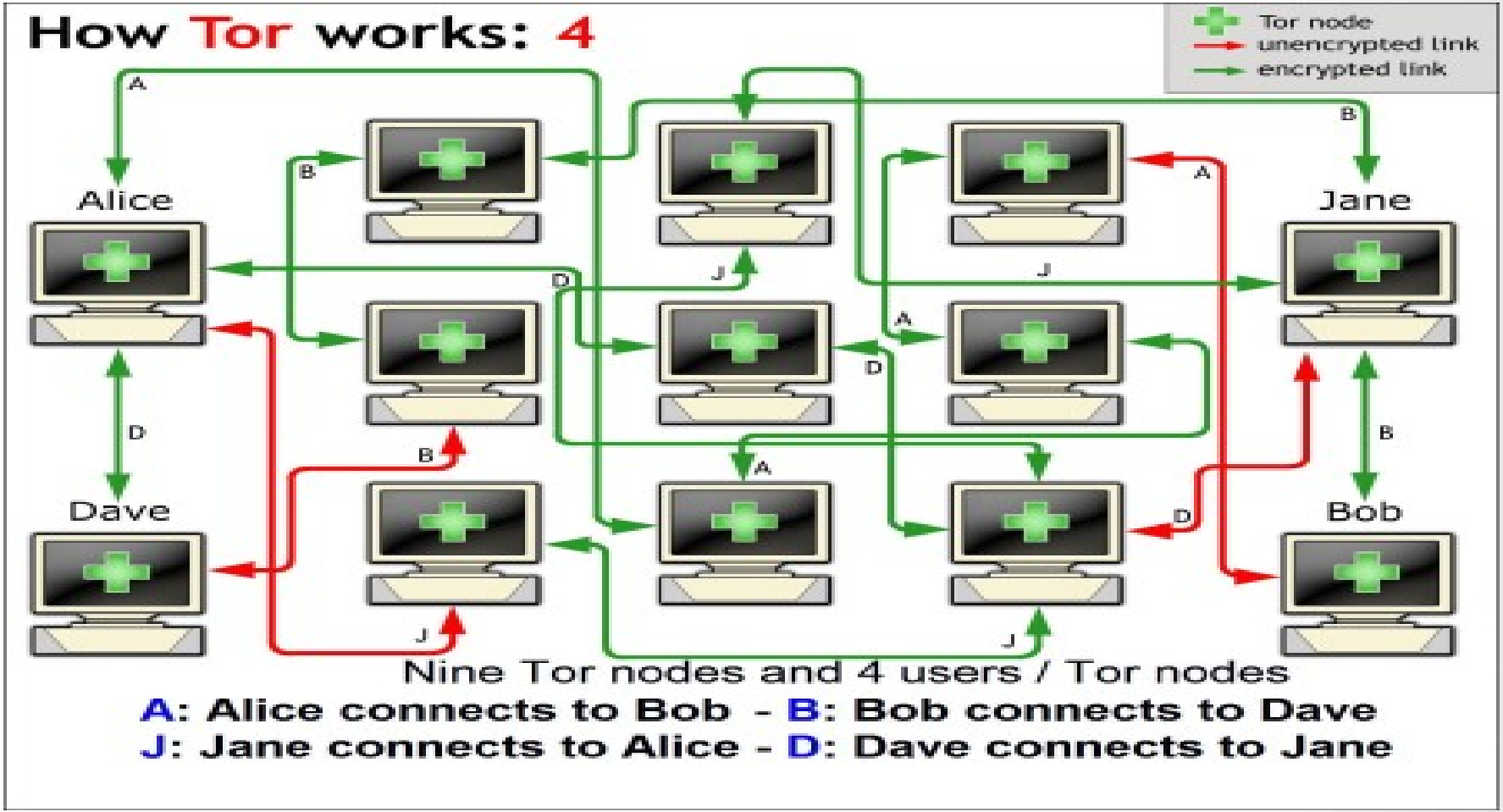
Circuito Tor



Circuito Tor



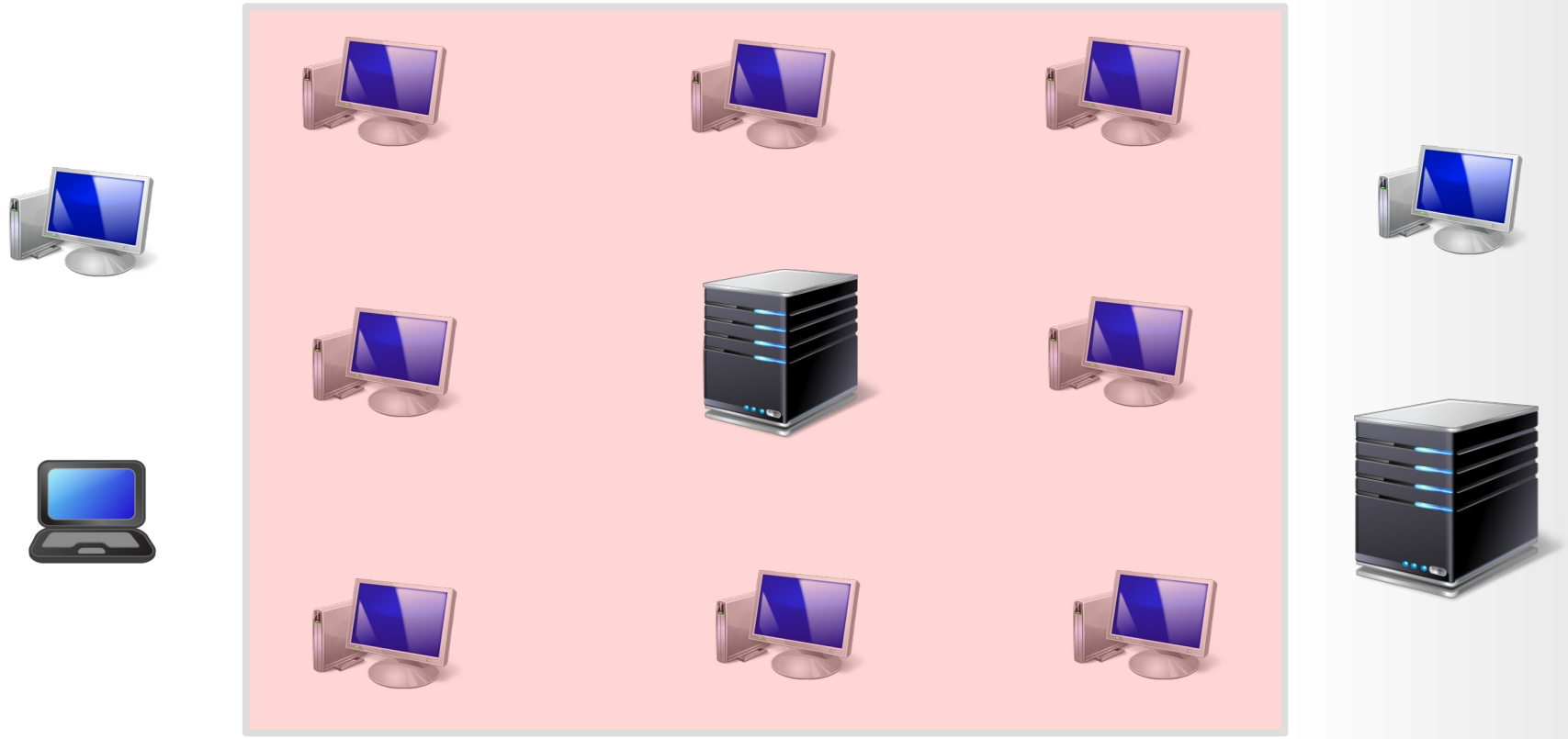
Circuito Tor



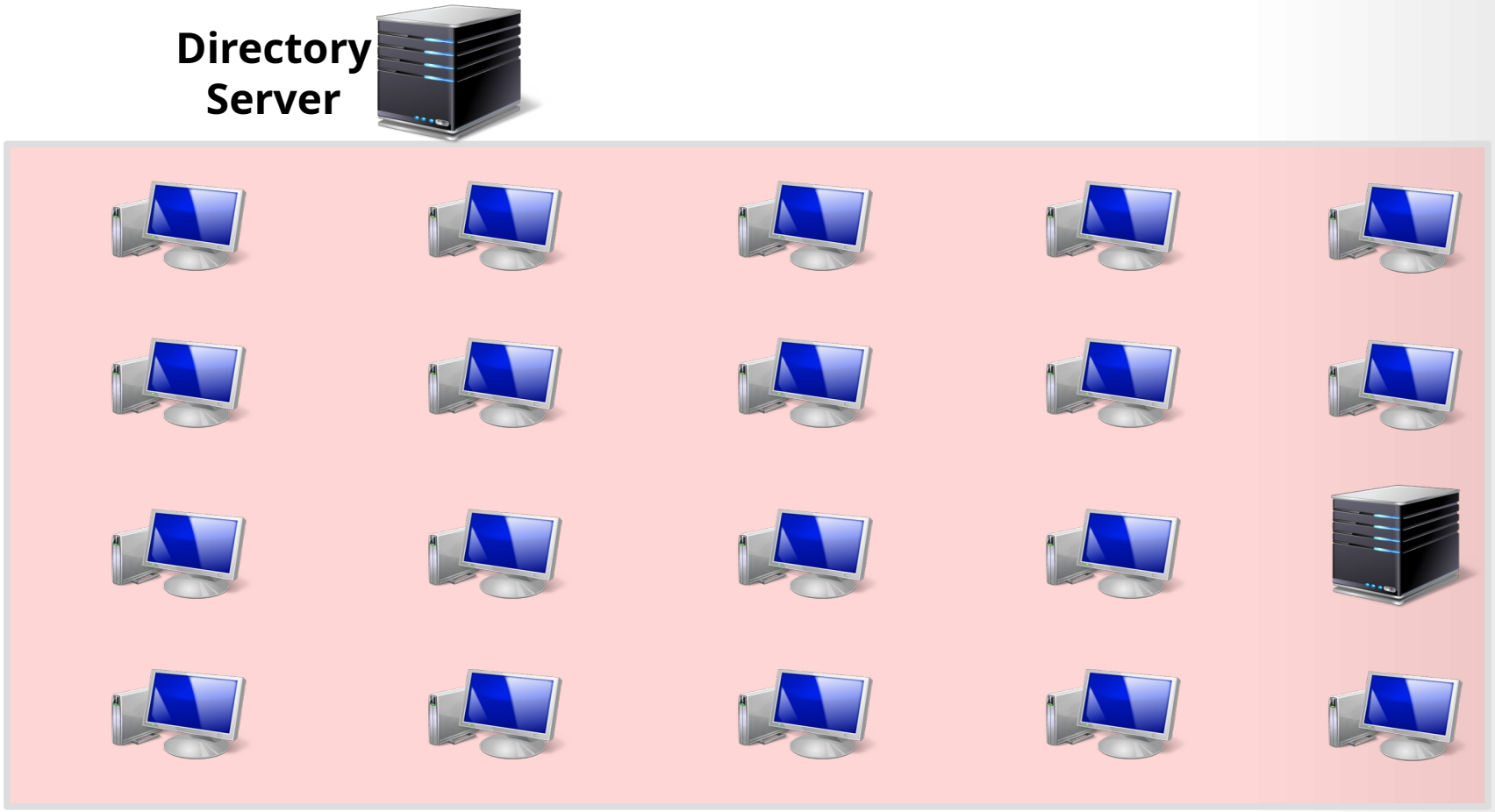
Tor

- ~~Il circuito Tor~~
- Instaurazione di un Hidden Service
- Indirizzi .onion V3
- Connessione ad un Hidden Service
- Bridge
- Pericoli

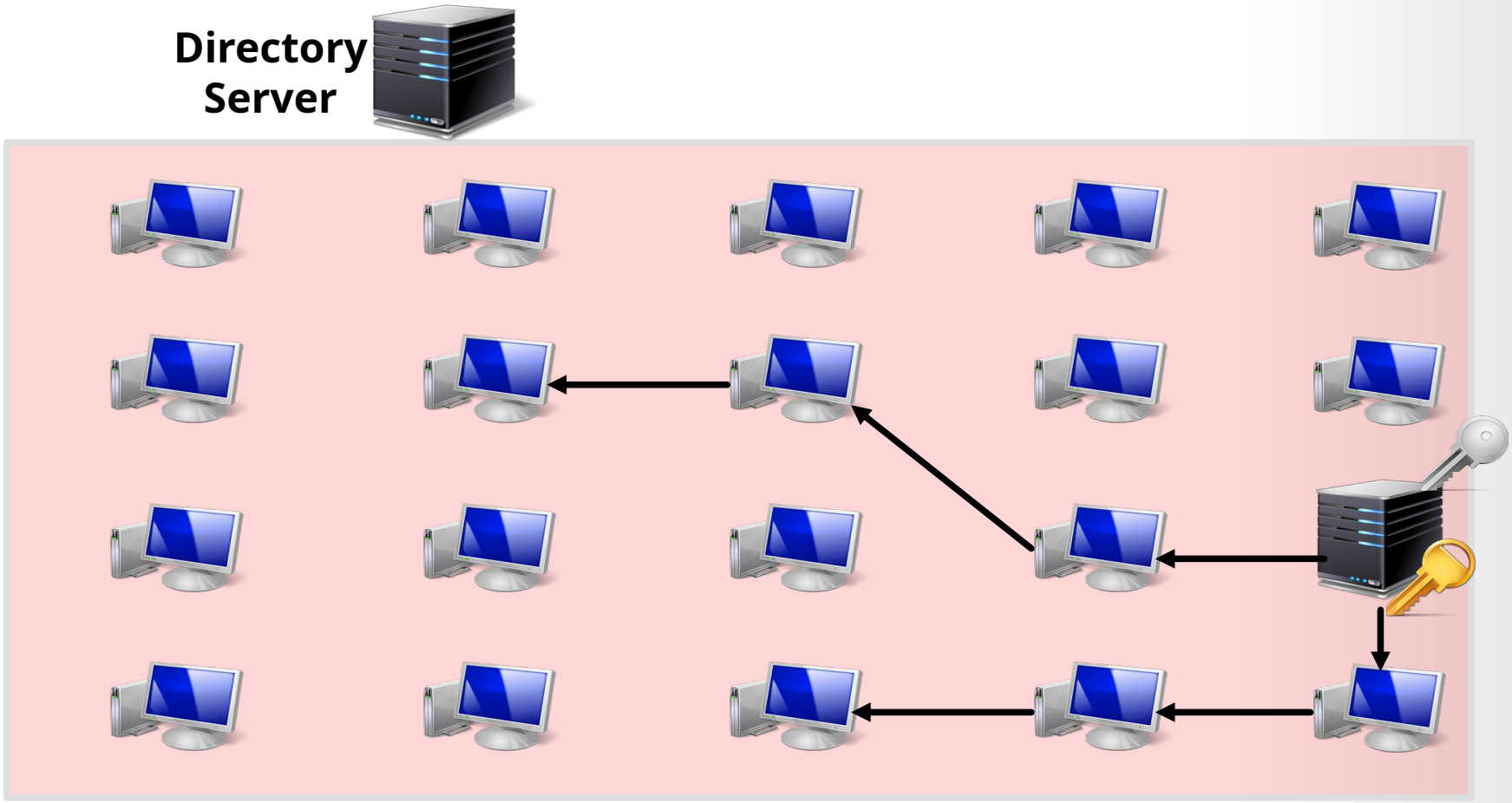
Hidden Services



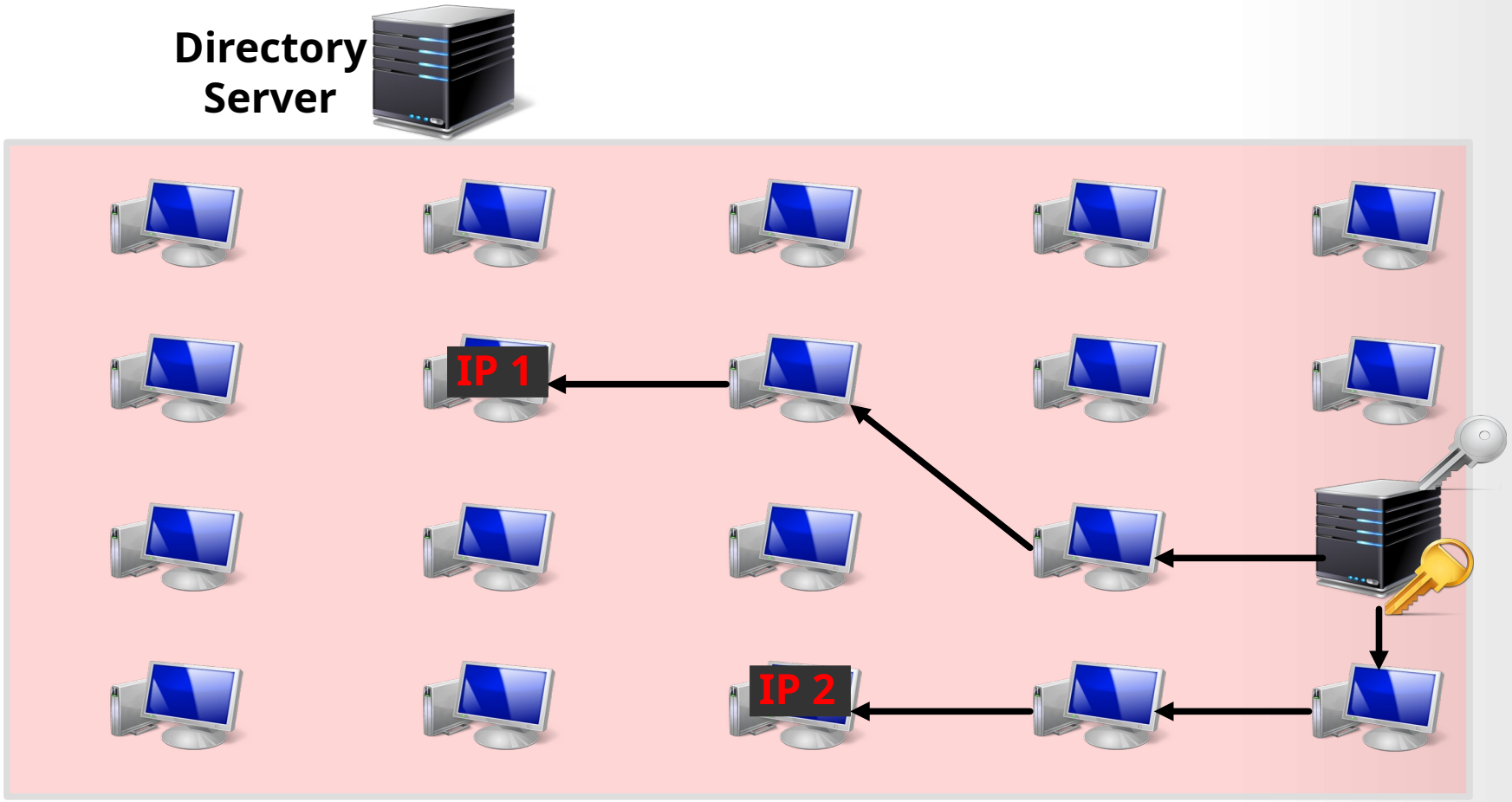
Hidden Services



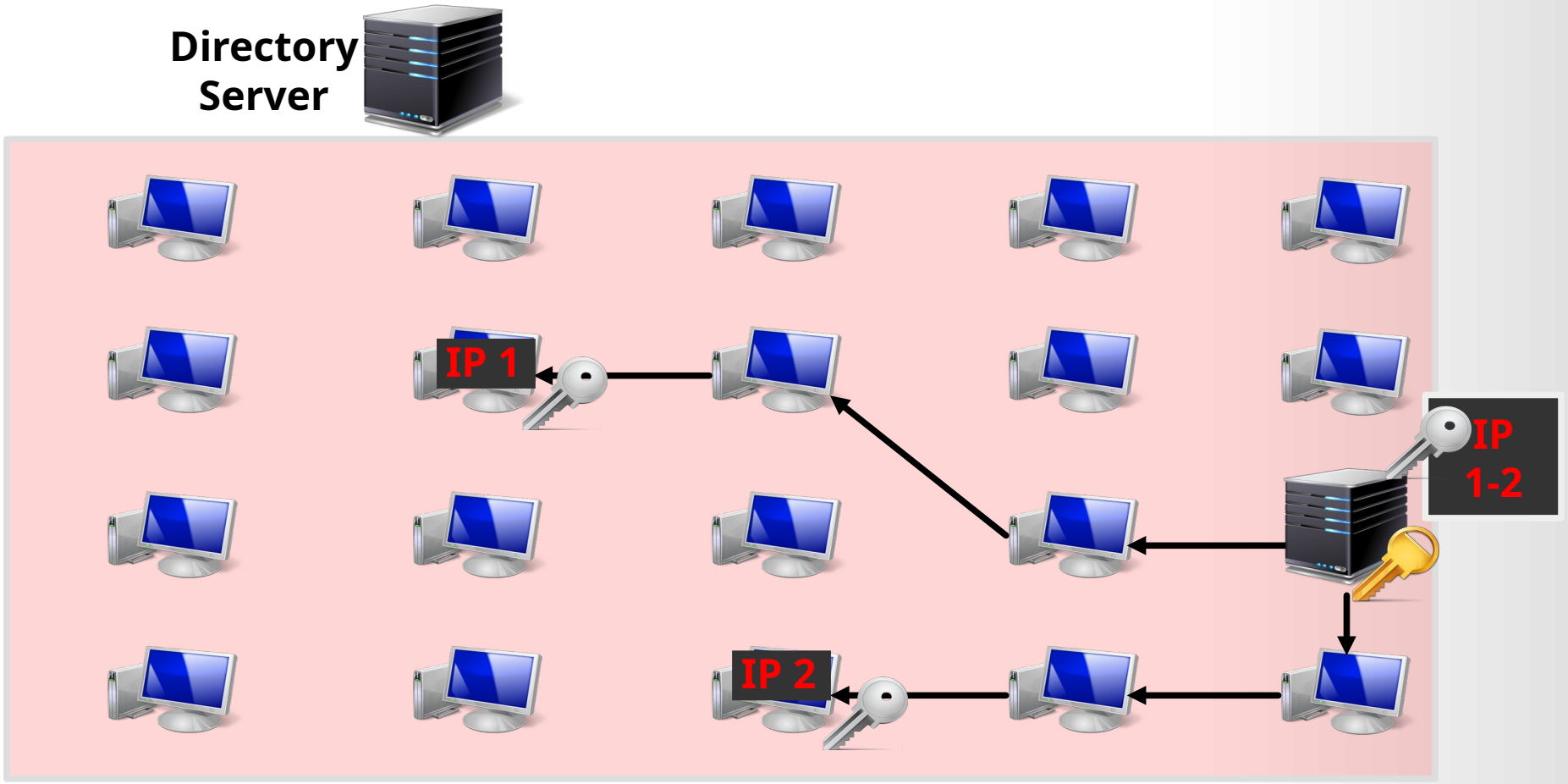
Hidden Services



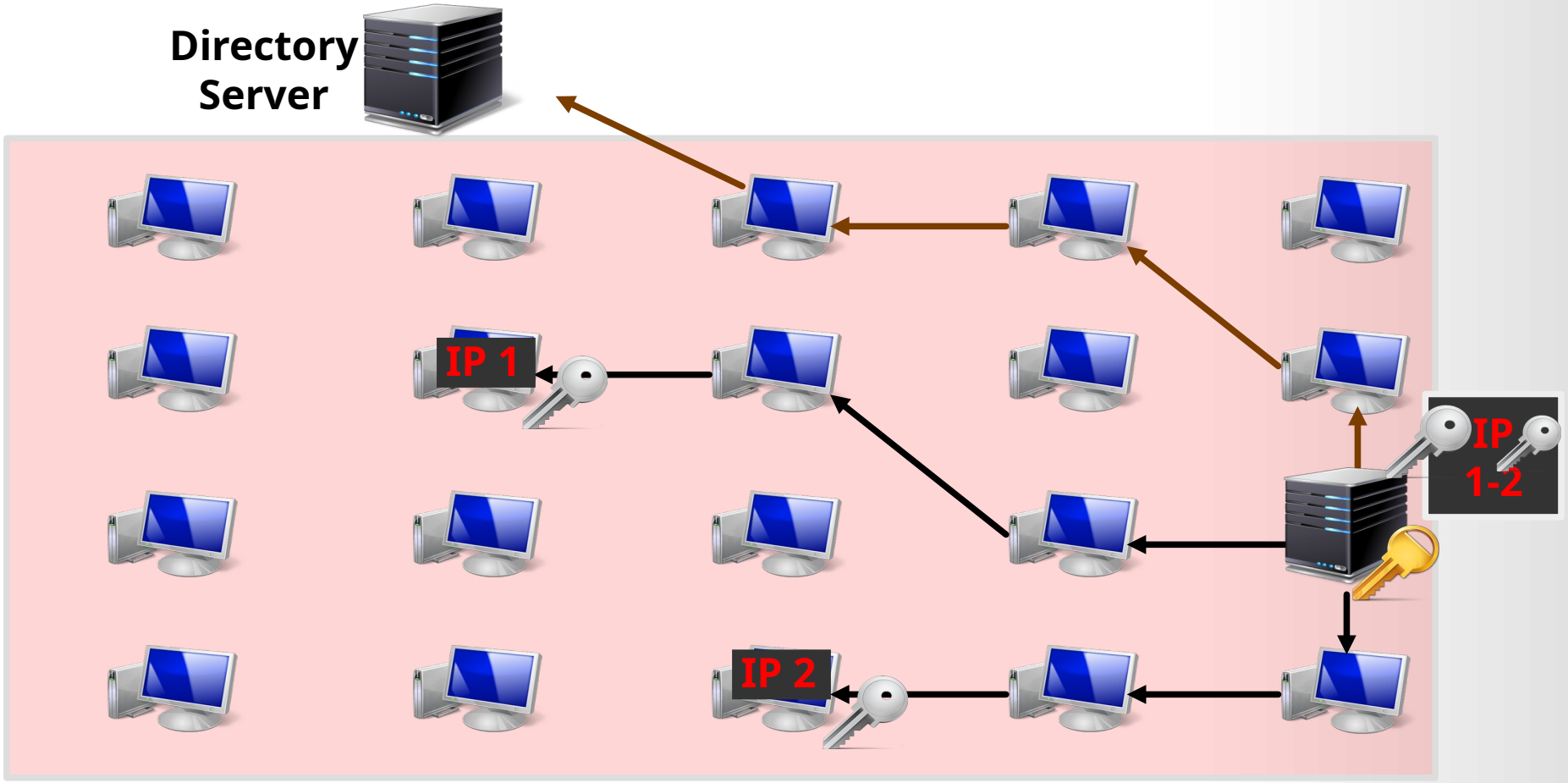
Hidden Services



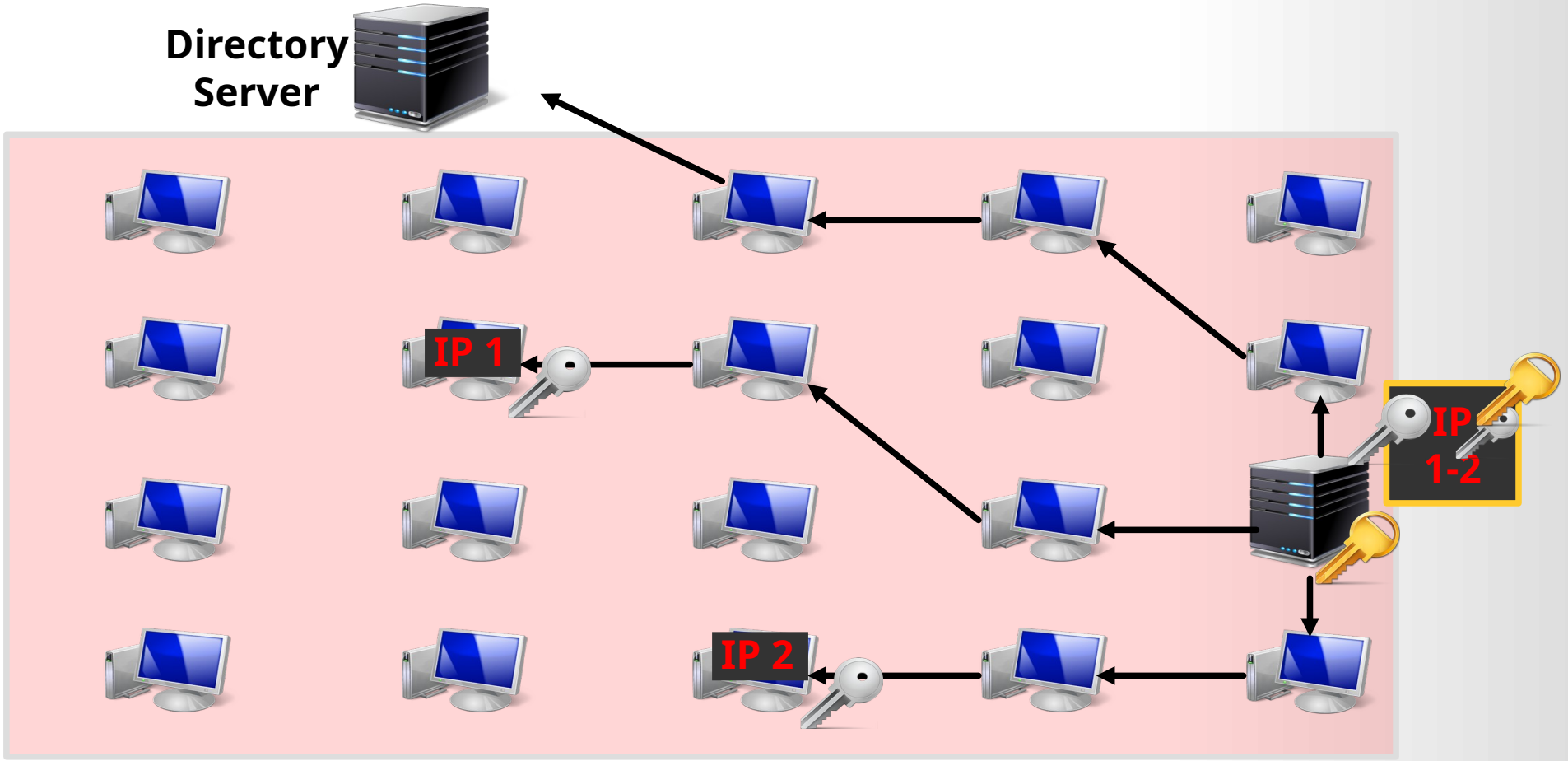
Hidden Services



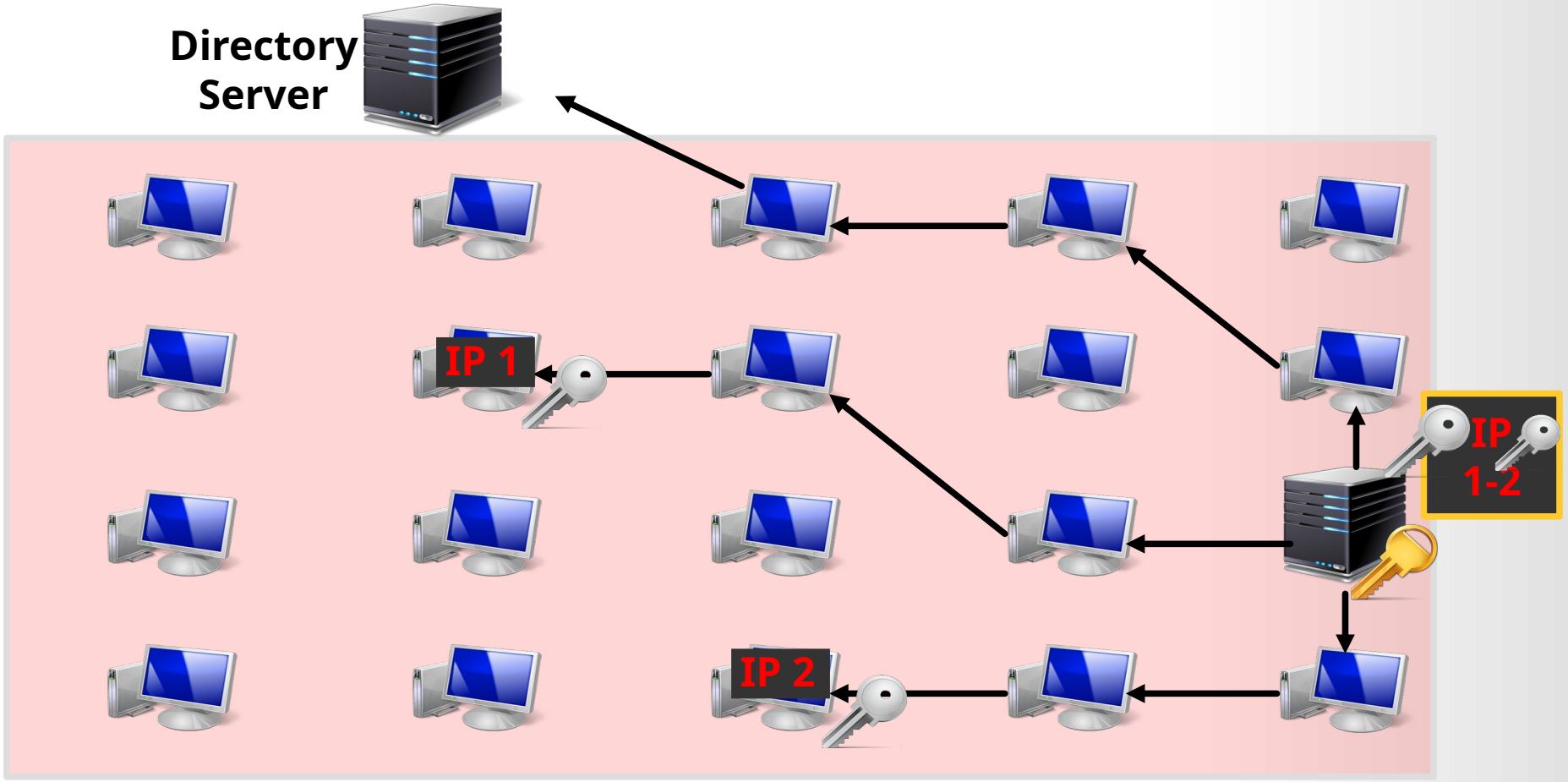
Hidden Services



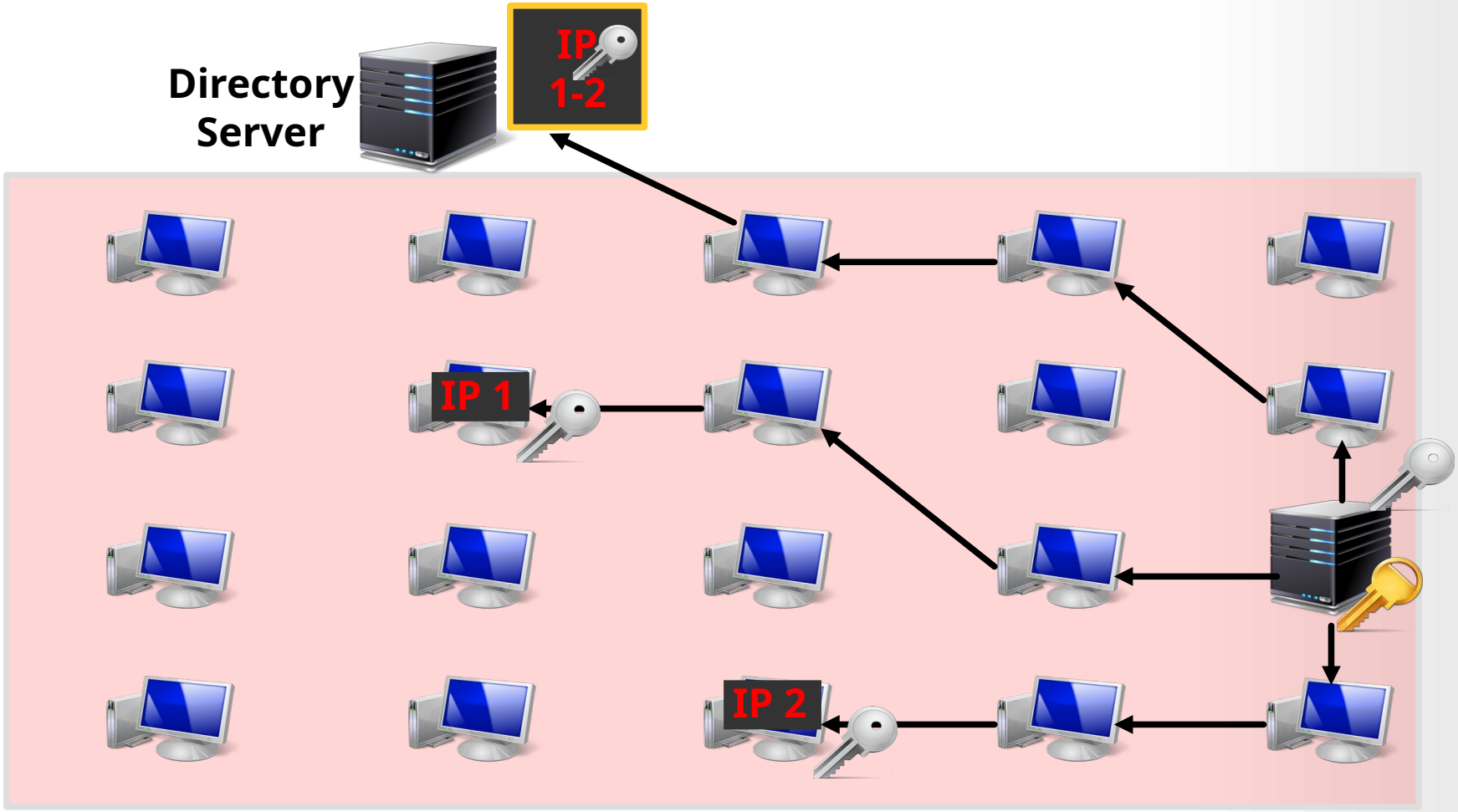
Hidden Services



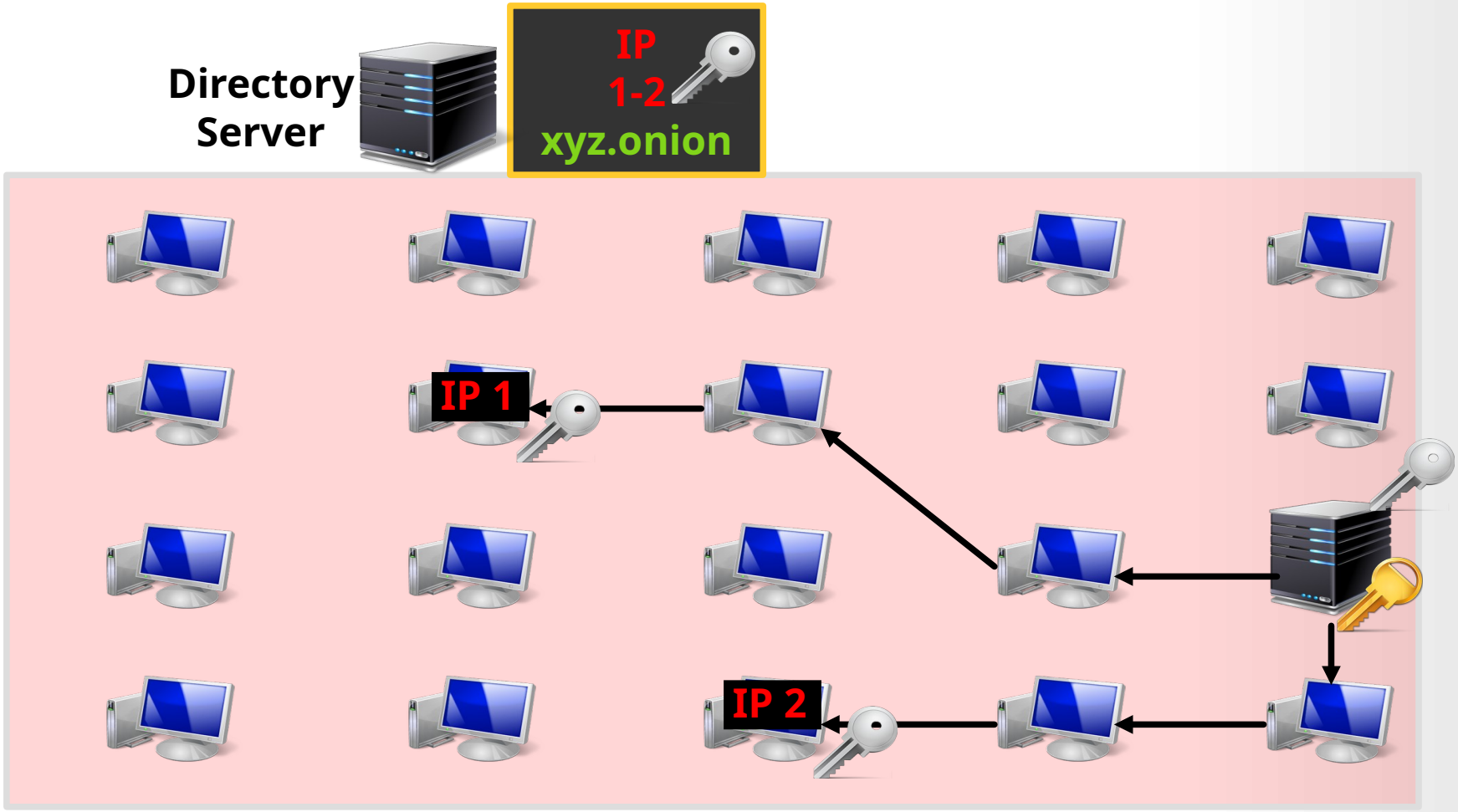
Hidden Services



Hidden Services



Hidden Services

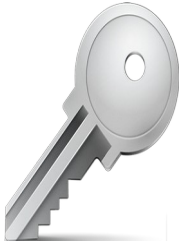


Tor

- ~~Il circuito Tor~~
- ~~Instaurazione di un Hidden Service~~
- Indirizzi .onion V3
- Connessione ad un Hidden Service
- Bridge

Indirizzi .onion V3

V2

HASH () = xyz.onion

V3

generate_ed25519_key() = abc.onion

Indirizzi .onion V3

generate_ed25519_key() = abc.onion

Per evitare la collezione di chiavi massiva questa generazione avviene modificata ogni giorno identificando l'operazione come "*blinded public key*".

Ciò vuol dire che il client, quando fa richiesta di accedere al sito ***facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd***, in automatico tale richiesta viene convertita calcolando la blinded public key alla data in cui viene fatta la richiesta, ad esempio ***ek4gJEtlHmwwadLvMNG7tYx/lJuJN1zQl6pMVkGmAcM***.

Indirizzi .onion V3

generate_ed25519_key() = abc.onion

Questa chiave pubblica può essere utilizzata sia per cifrare dati che l'Hidden Service invia al Directory Server che per mitigre la collezione degli indirizzi e le analisi massive su di essi (comportamento per altro sanzionato dal Bad Relay Team).

Indirizzi .onion V3

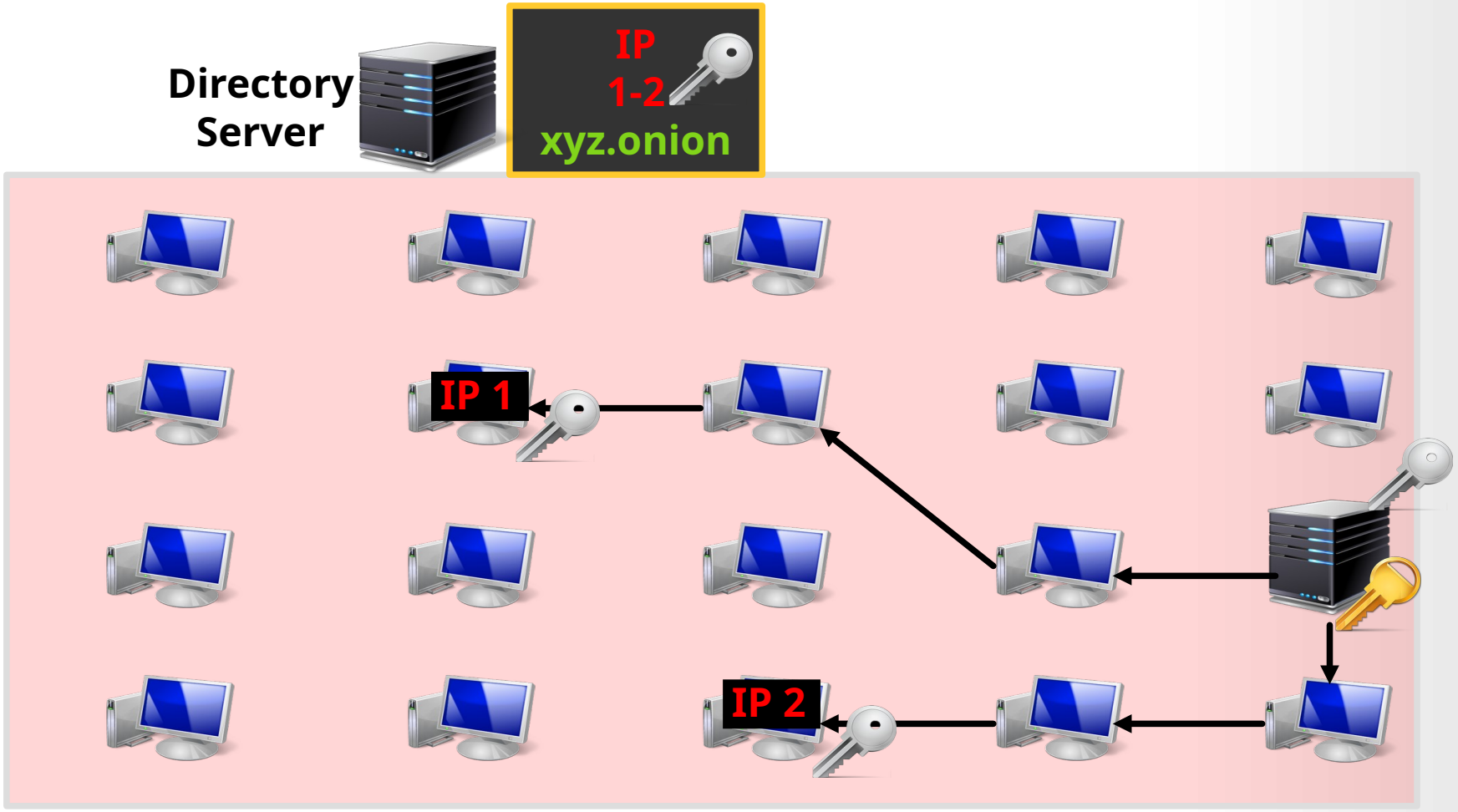
TODO:

- Esistono una sorta di motori di ricerca
- Esistono i vanity domain .onion

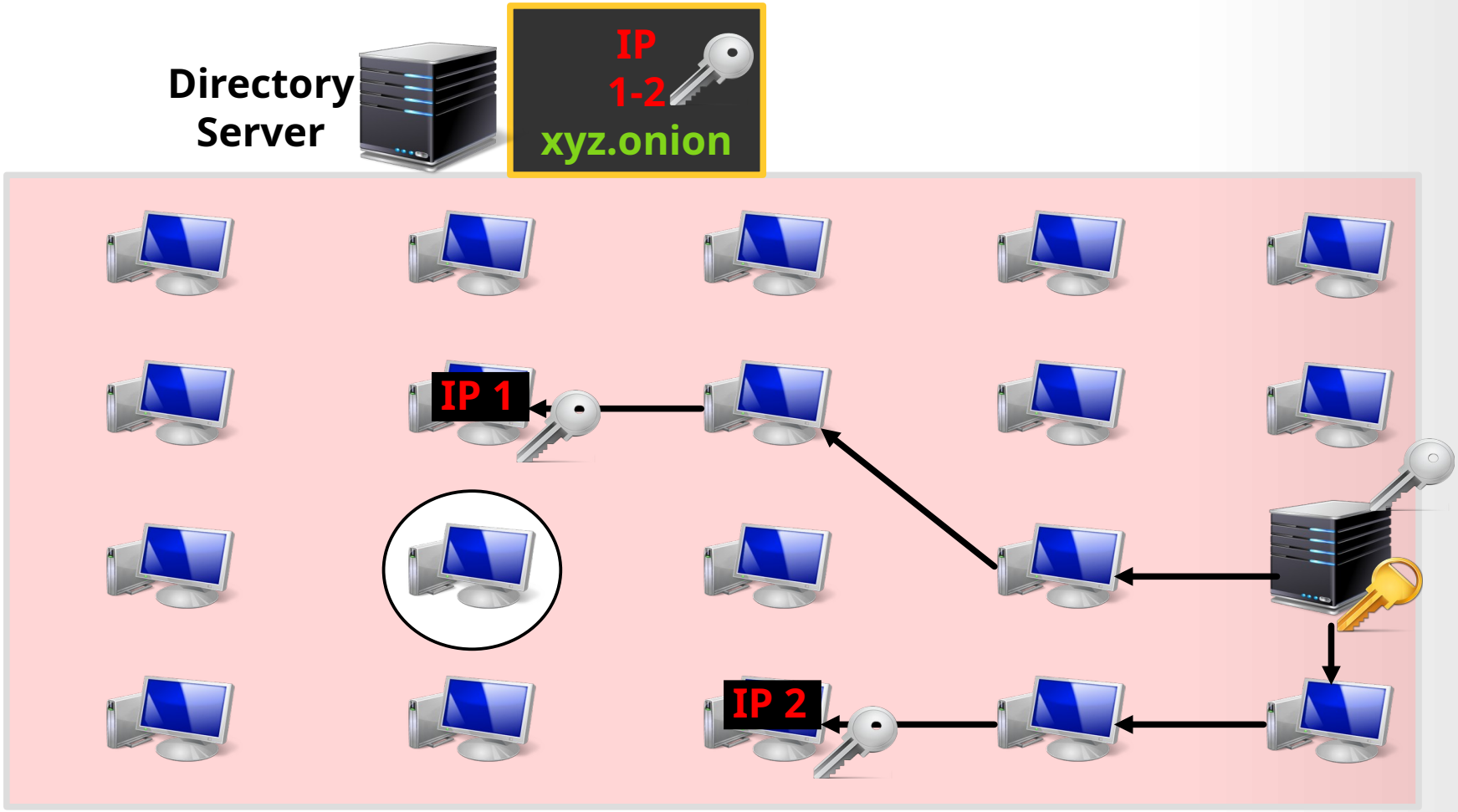
Tor

- ~~Il circuito Tor~~
- ~~Instaurazione di un Hidden Service~~
- ~~Indirizzi .onion V3~~
- Connessione ad un Hidden Service
- Bridge
- Pericoli

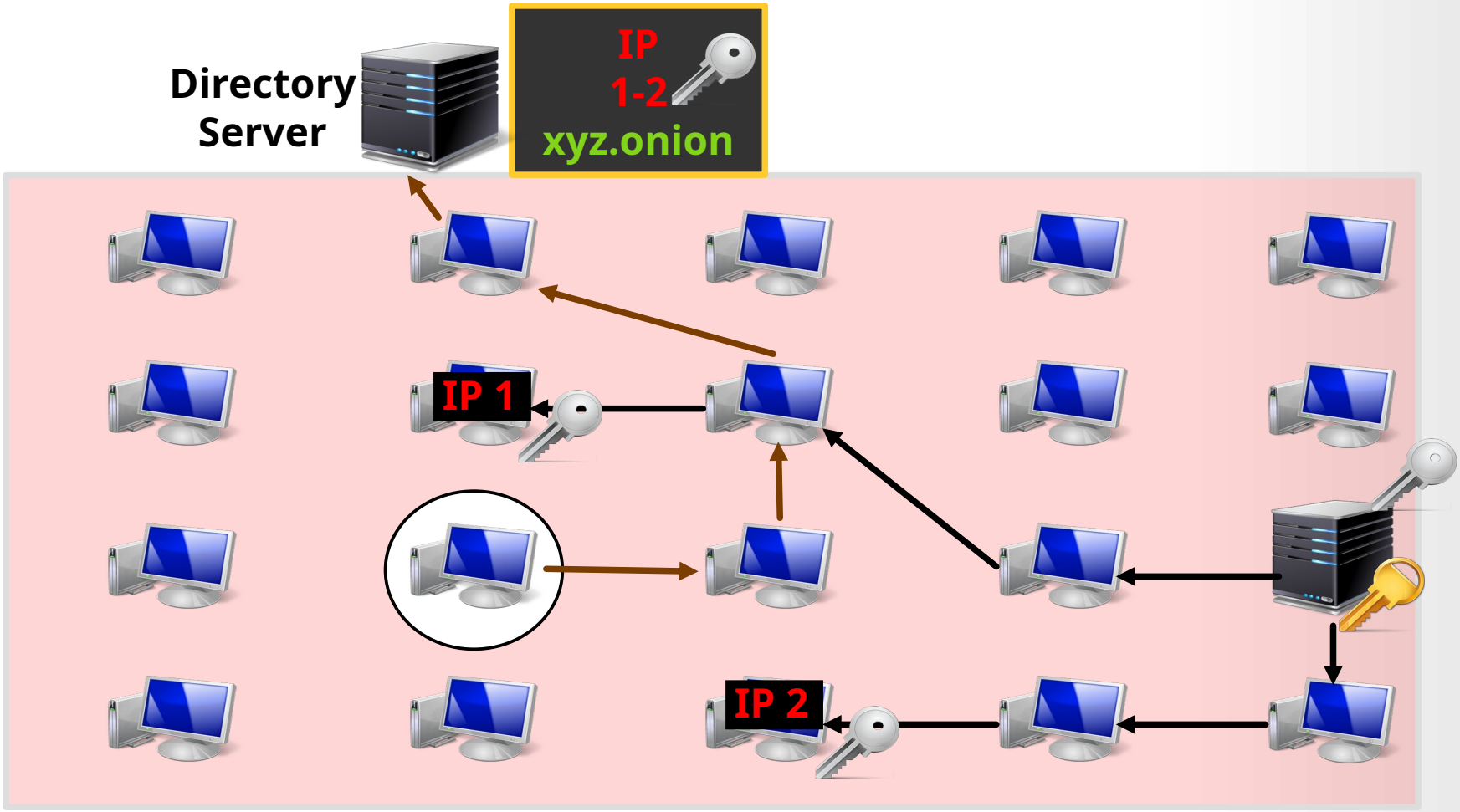
Hidden Services



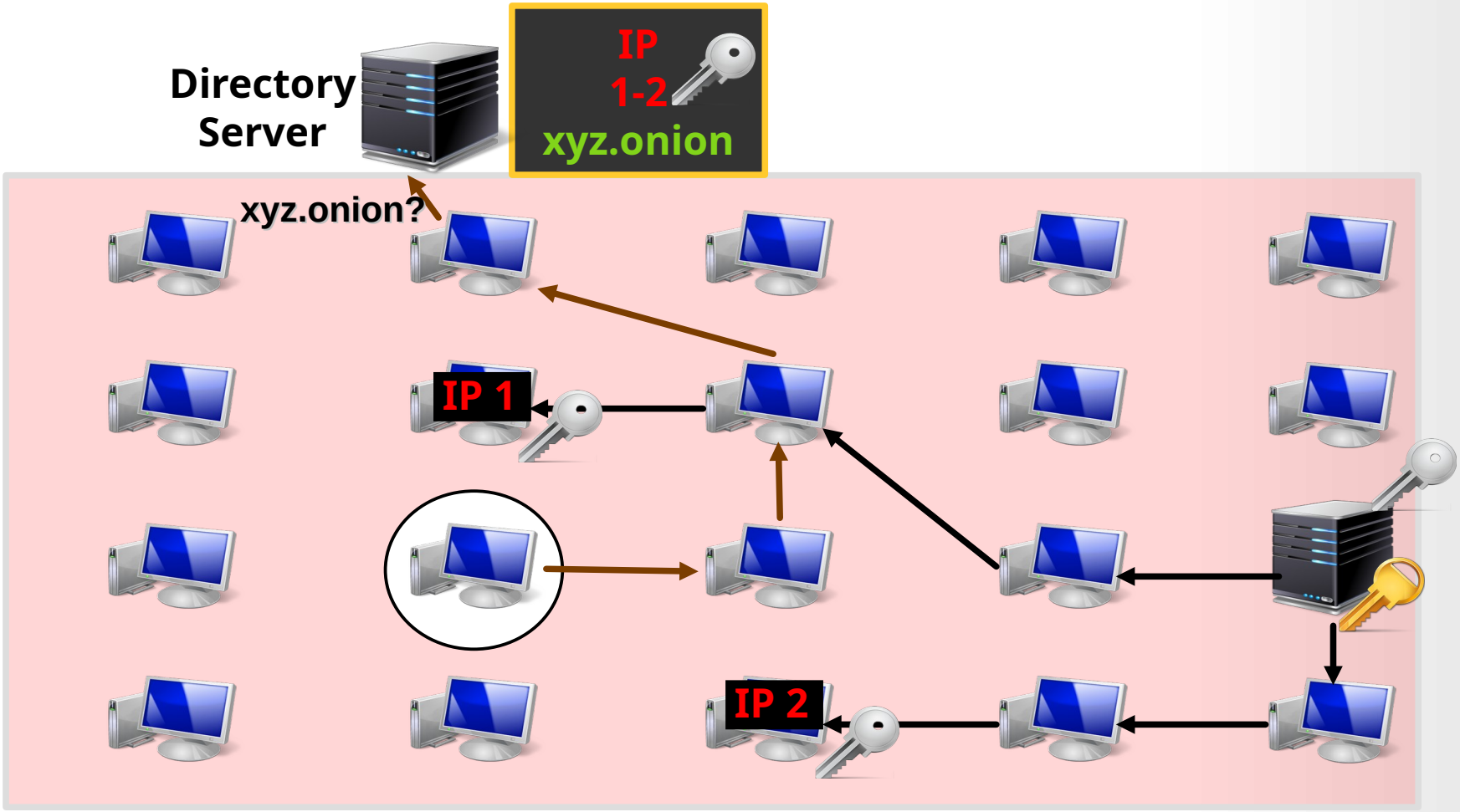
Hidden Services



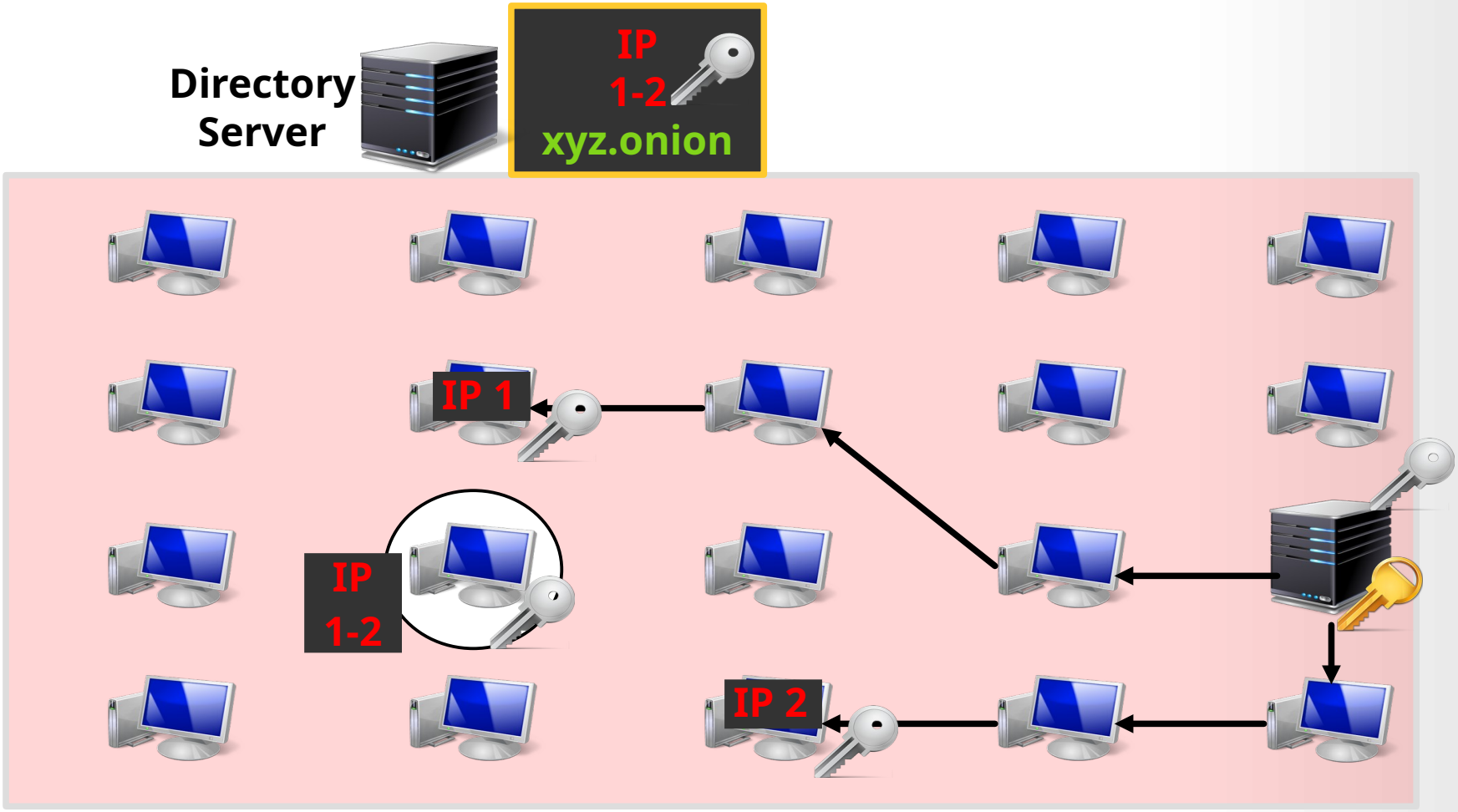
Hidden Services



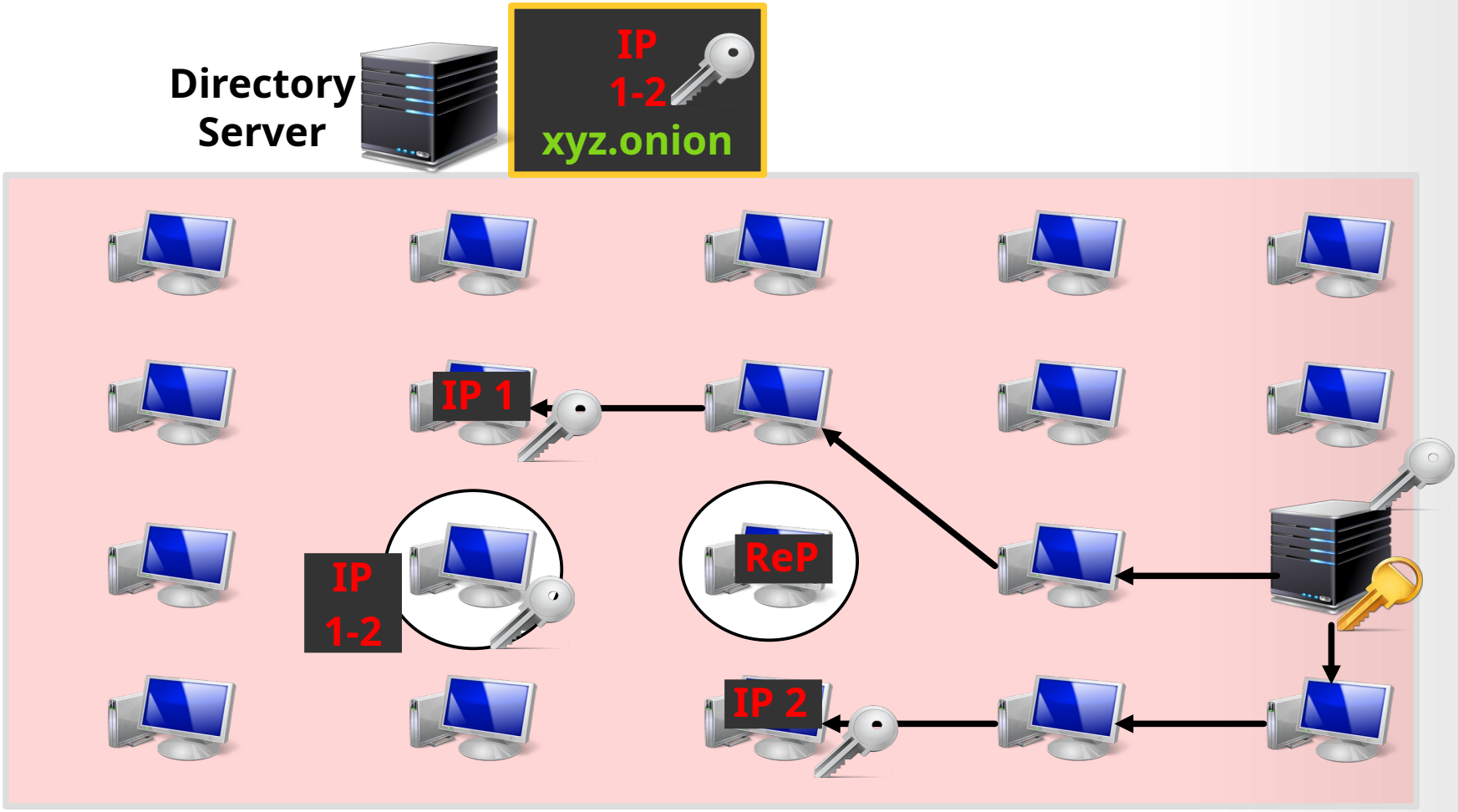
Hidden Services



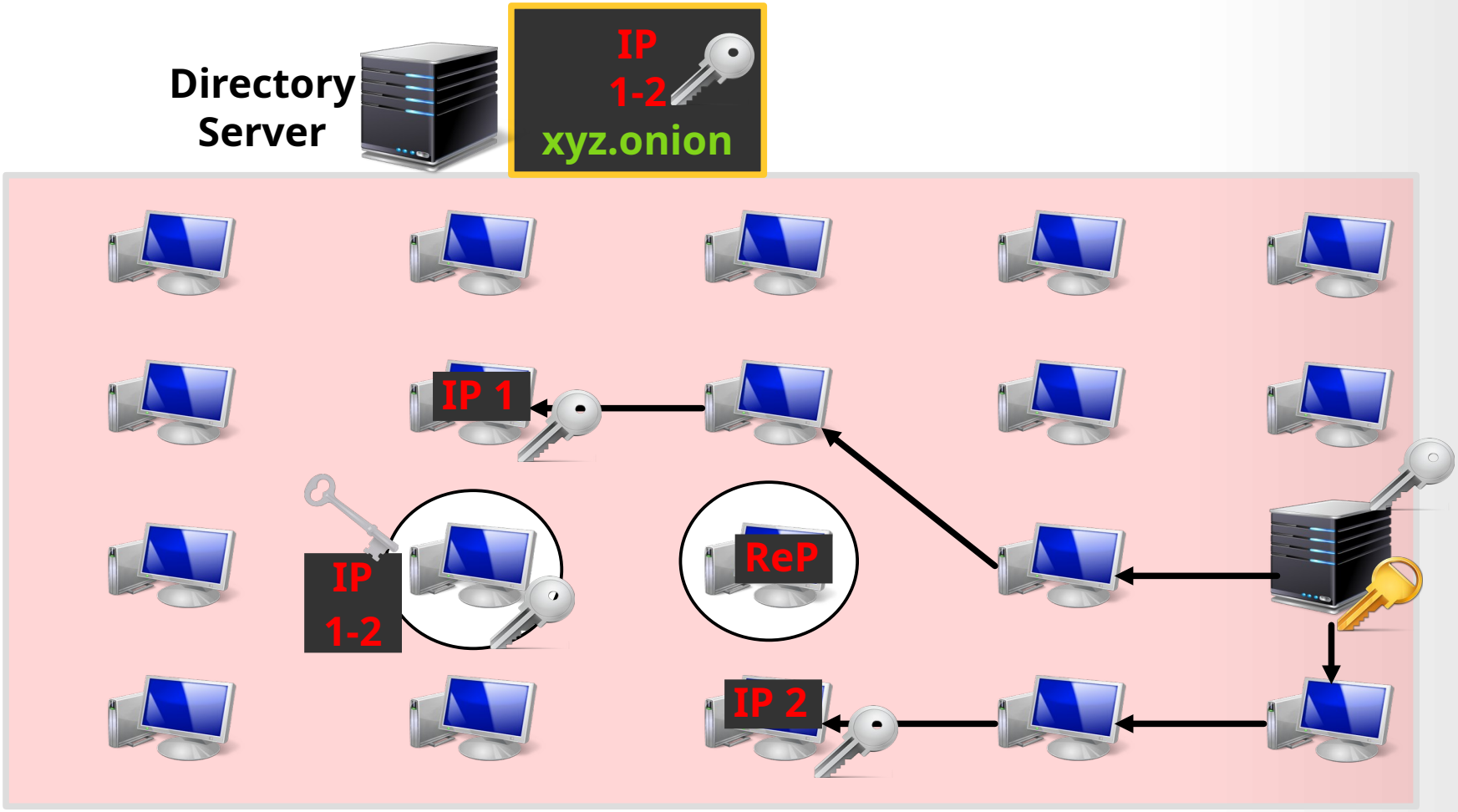
Hidden Services



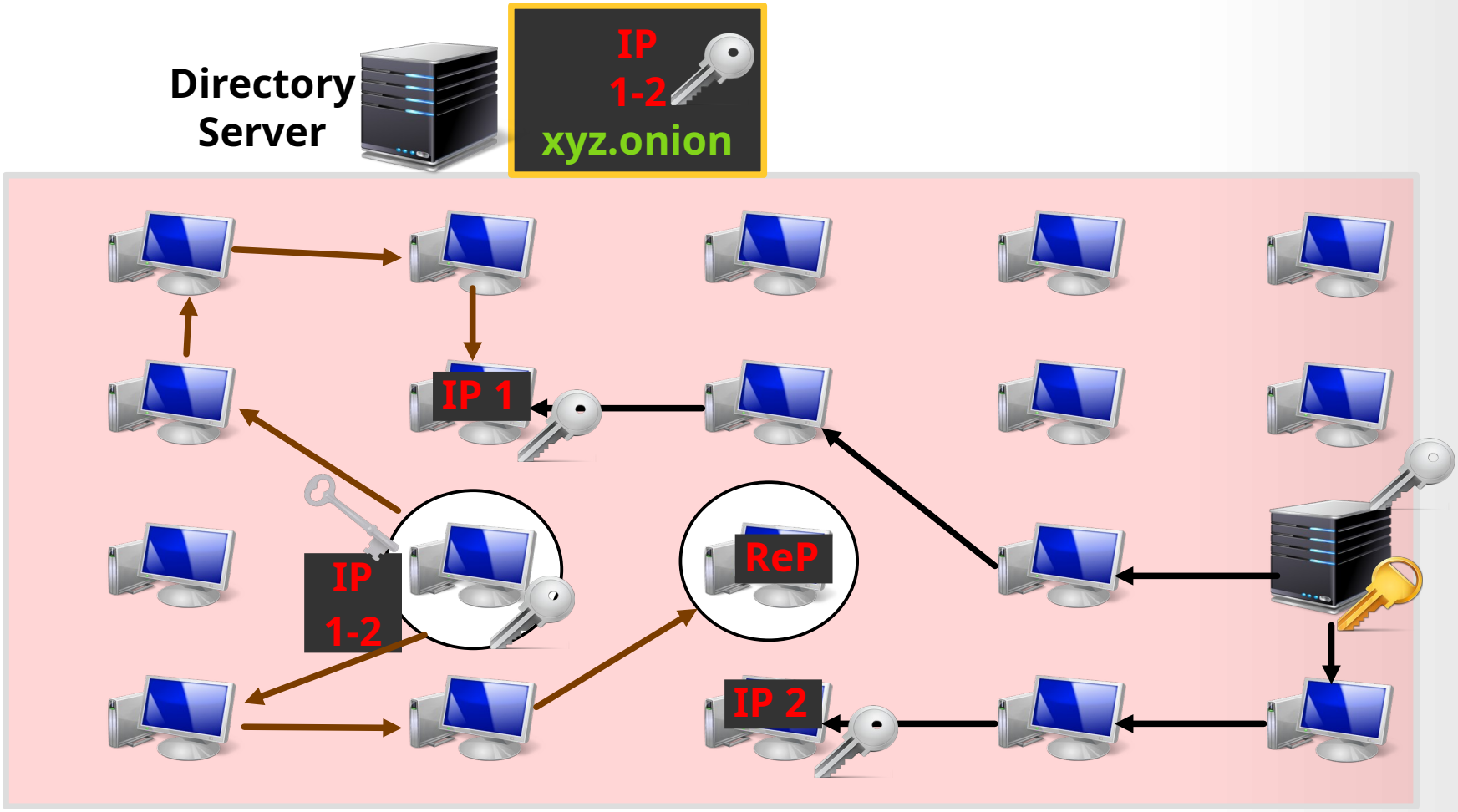
Hidden Services



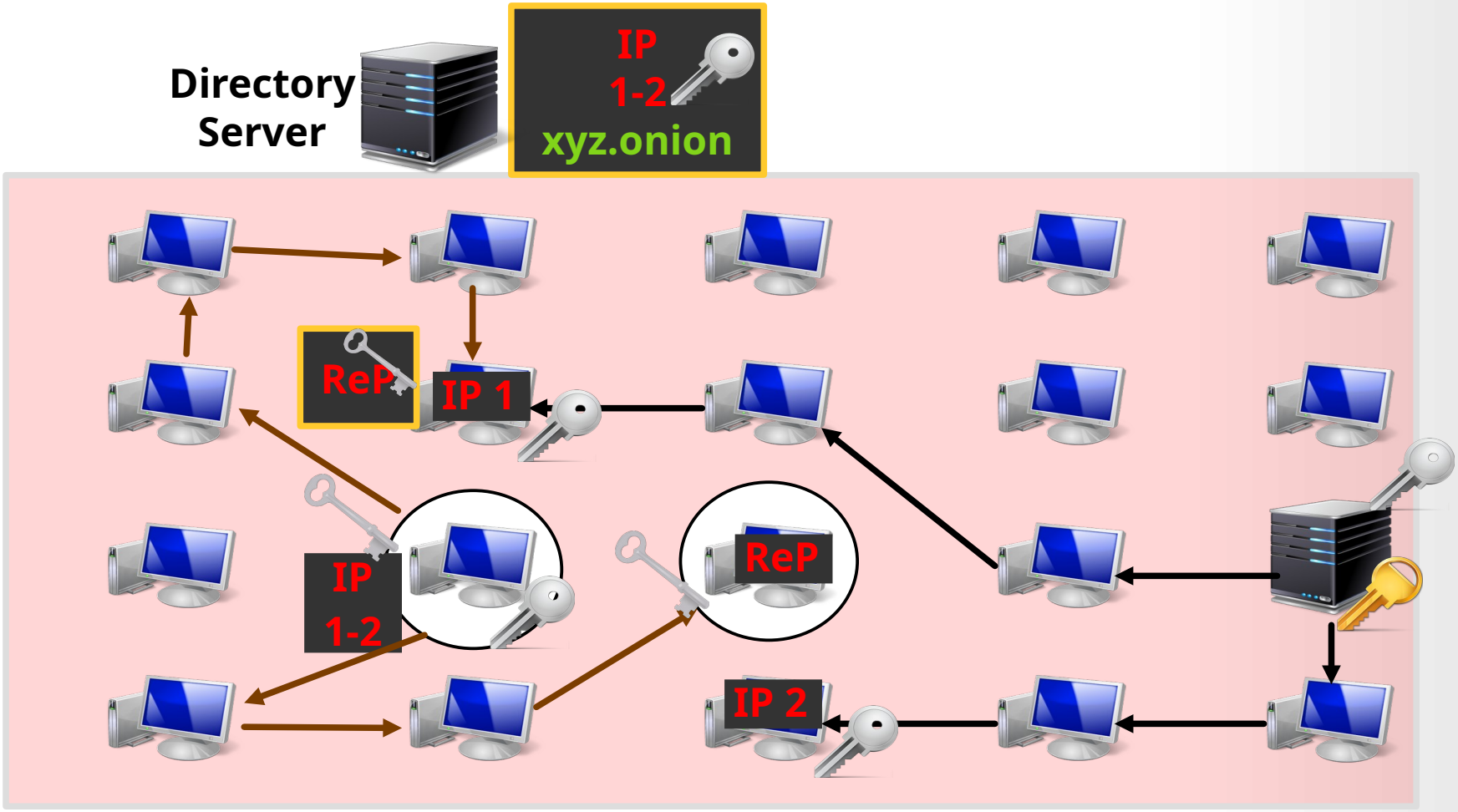
Hidden Services



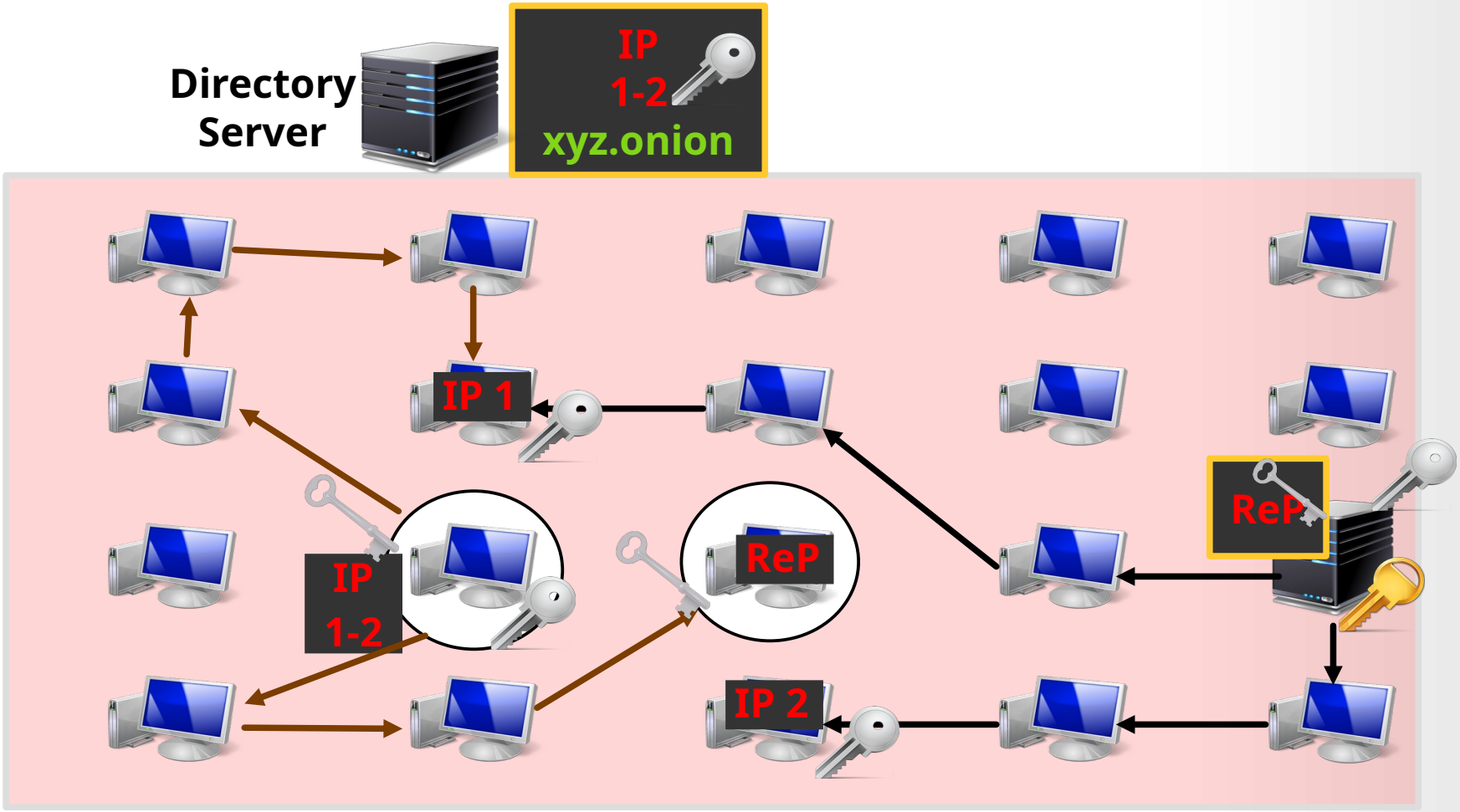
Hidden Services



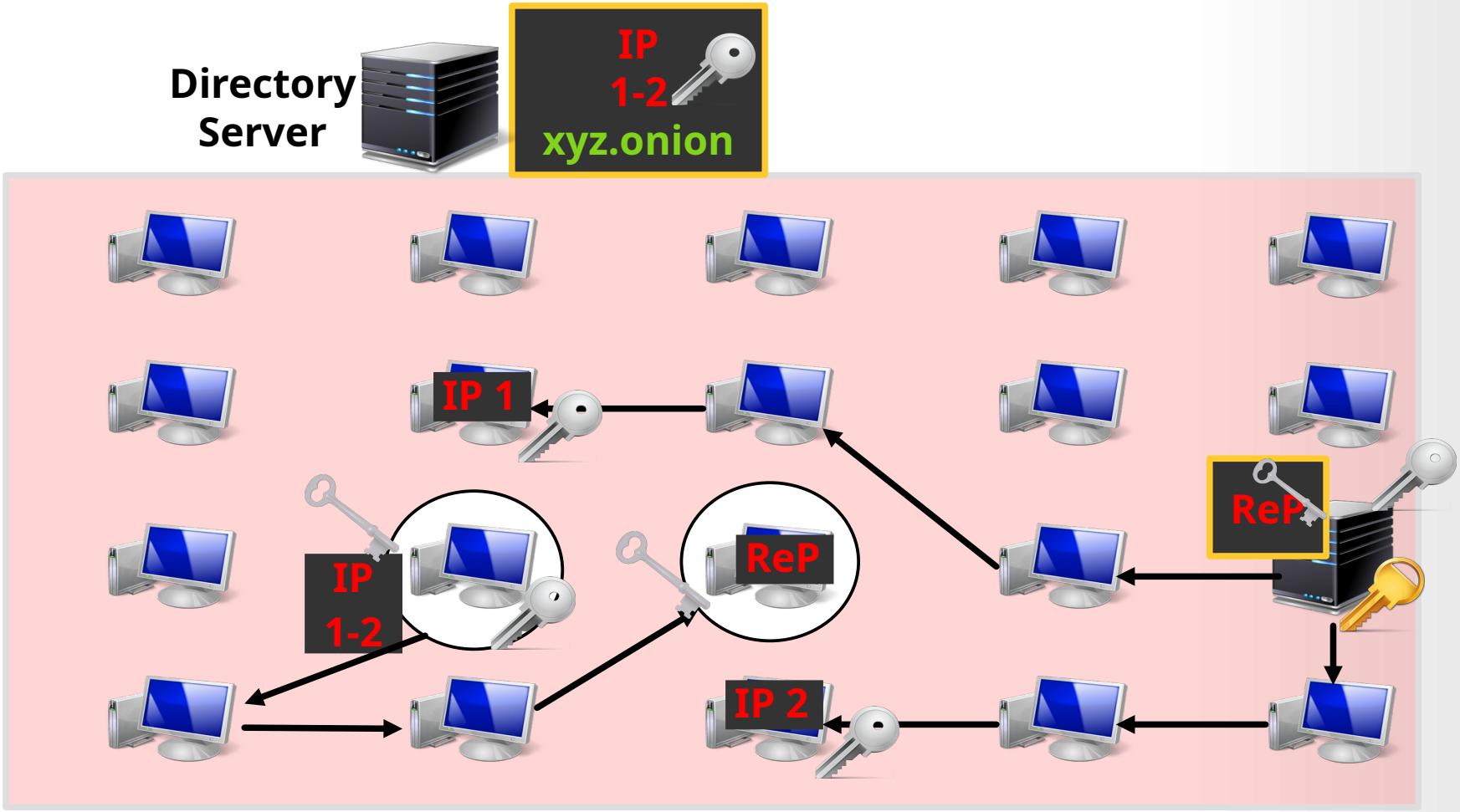
Hidden Services



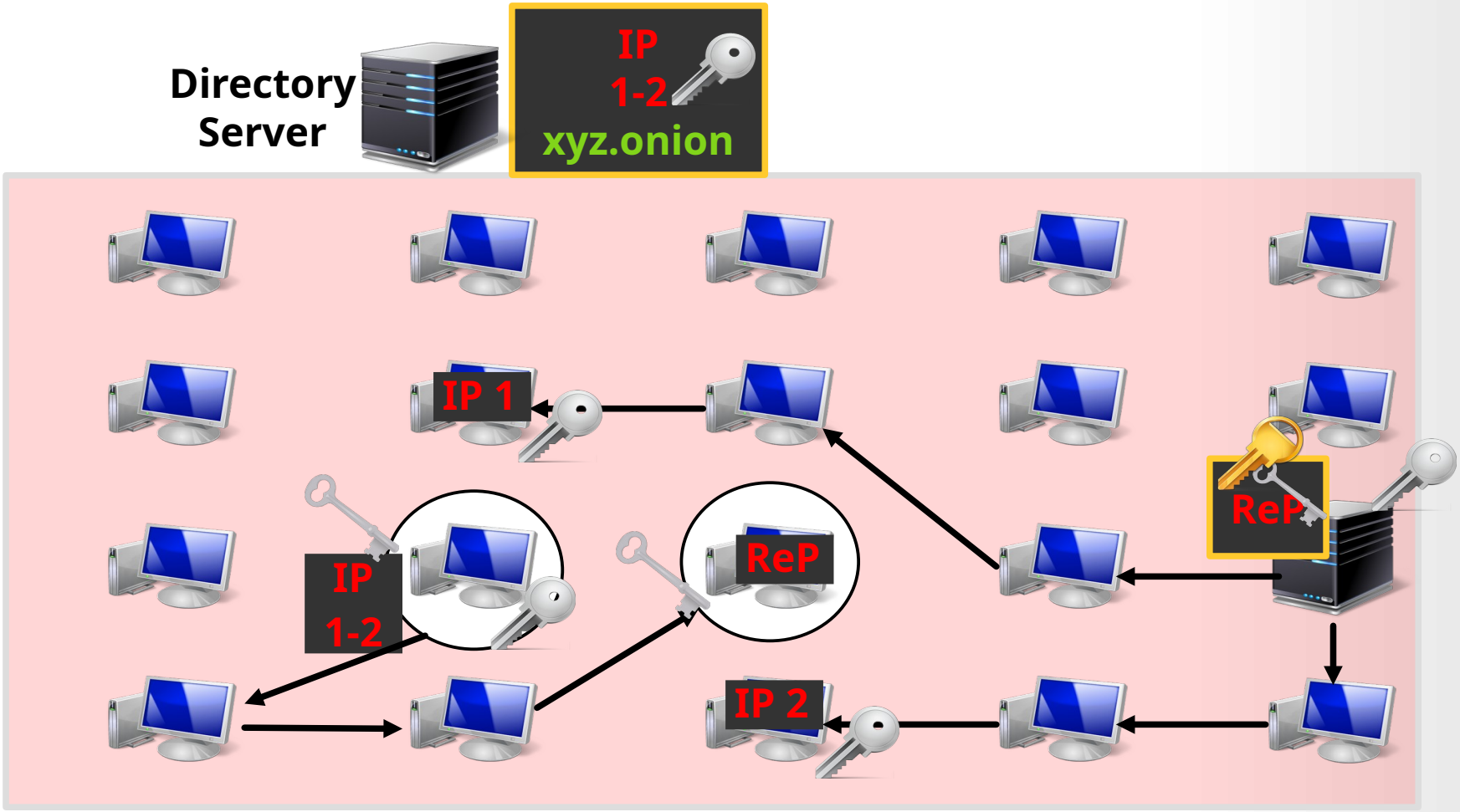
Hidden Services



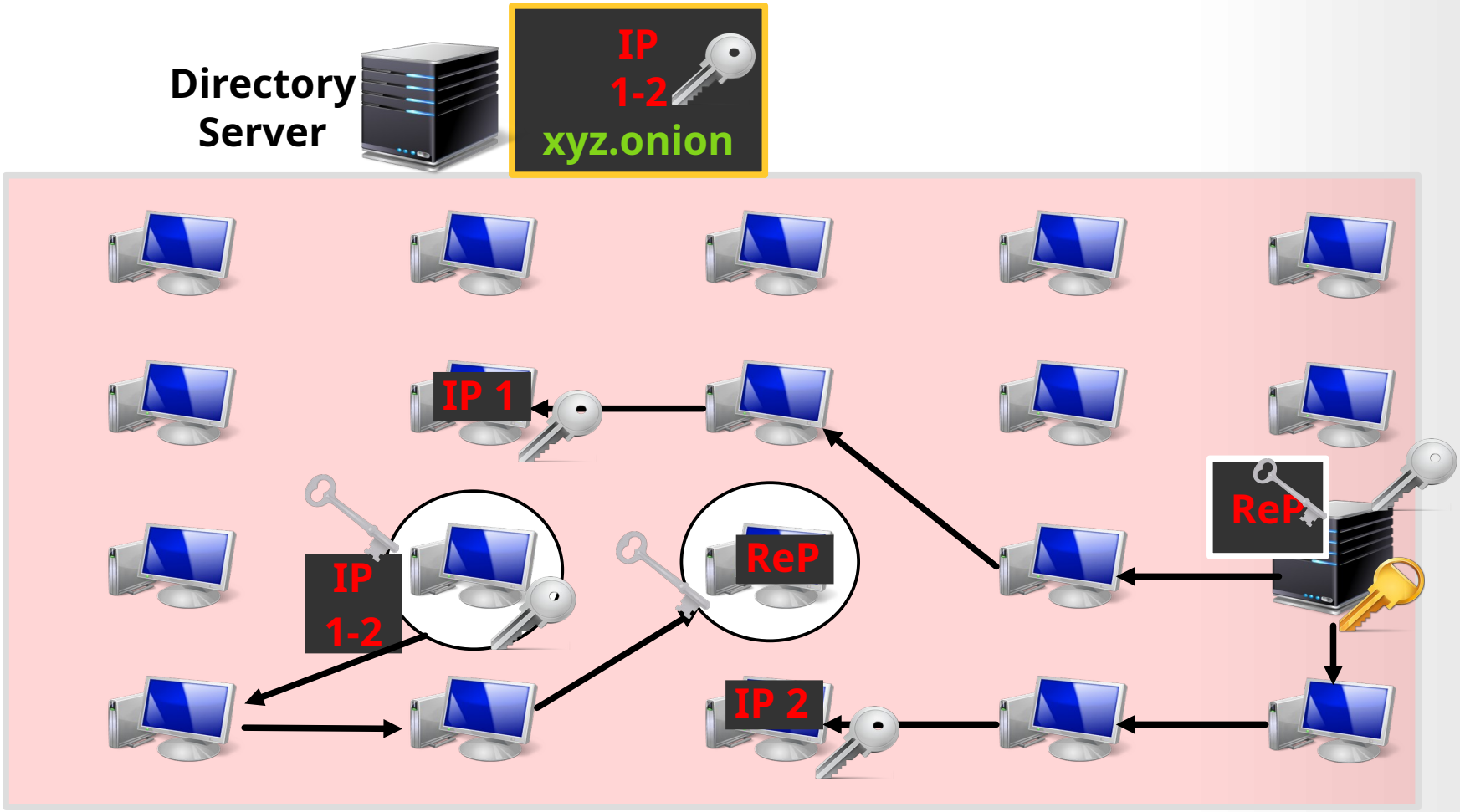
Hidden Services



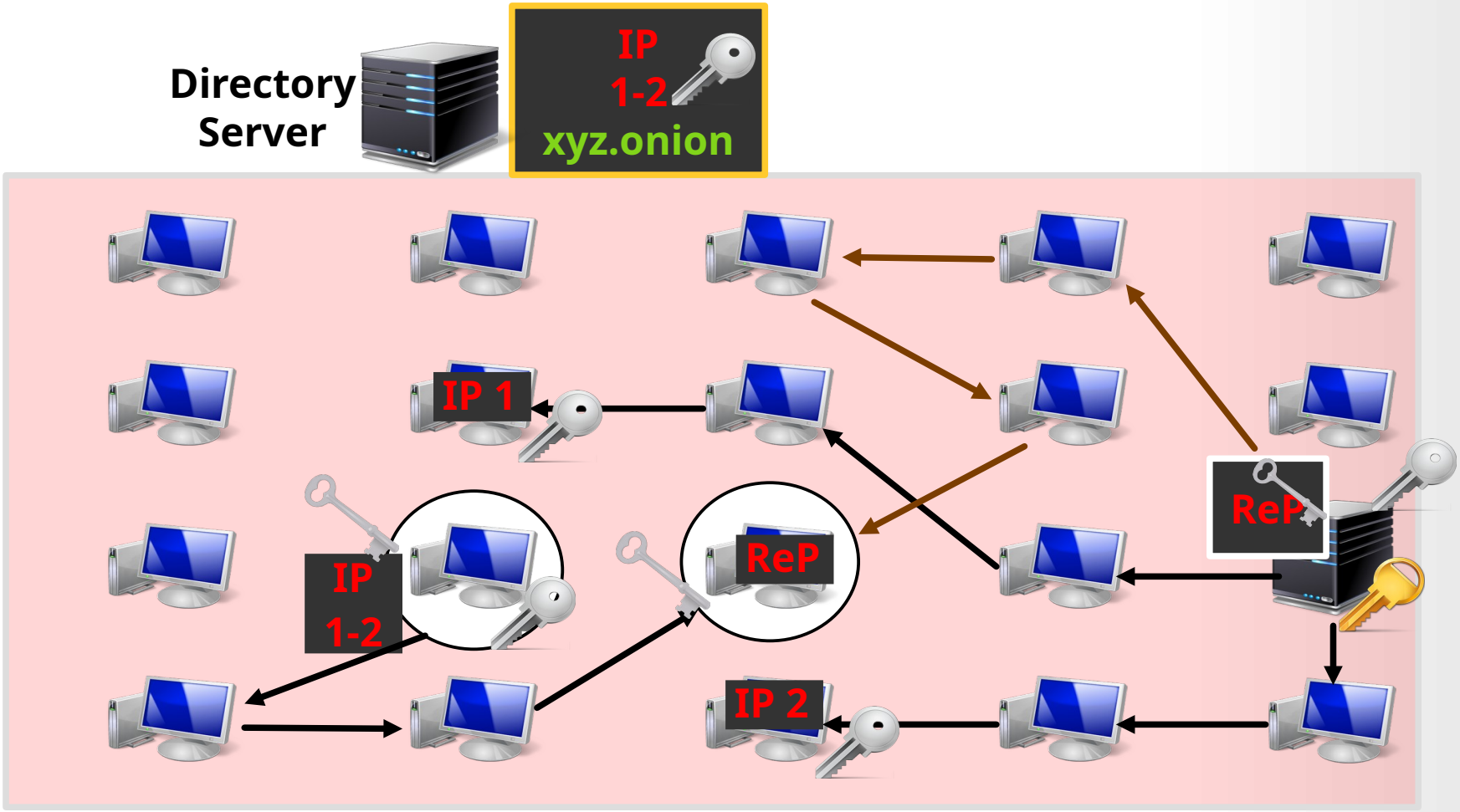
Hidden Services



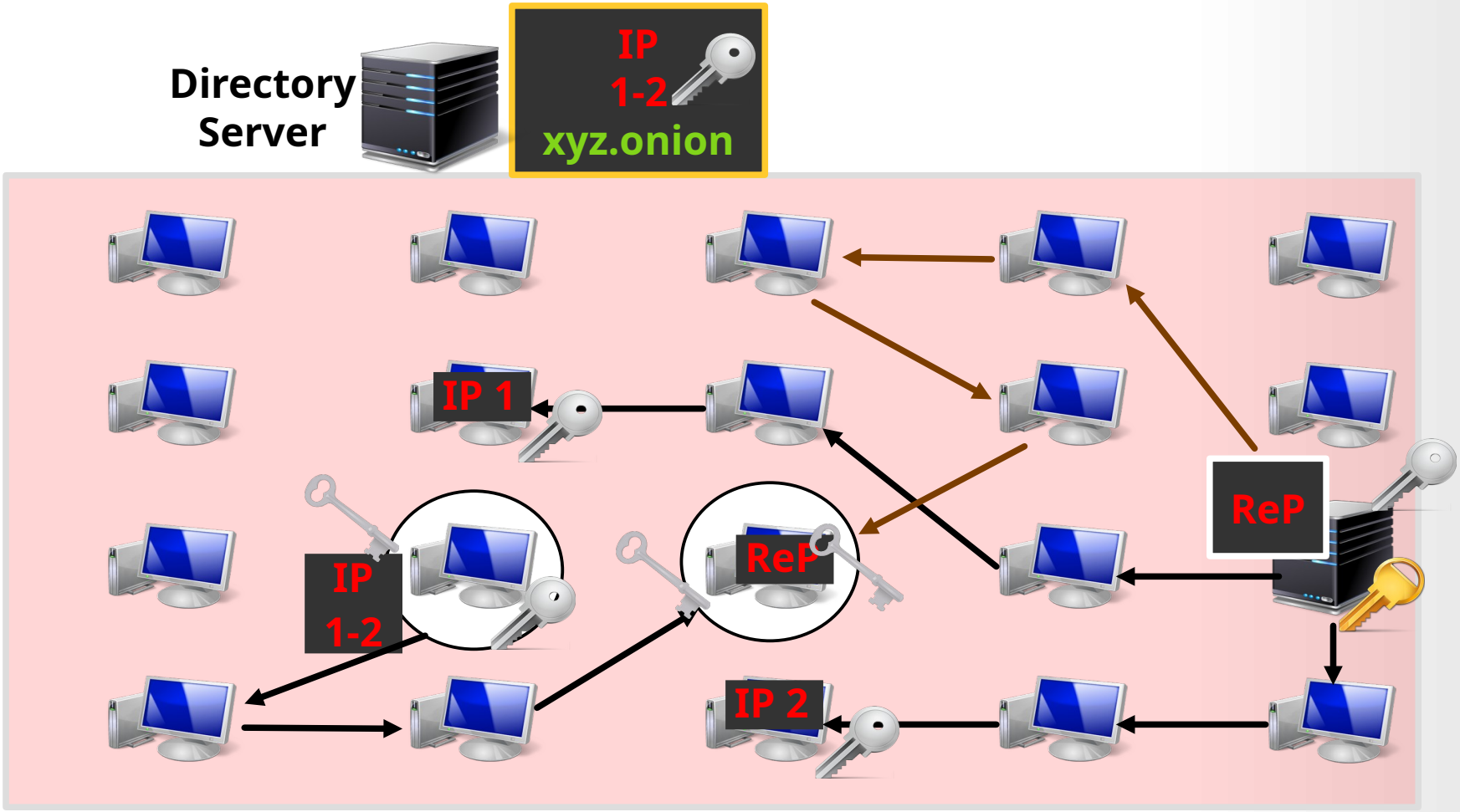
Hidden Services



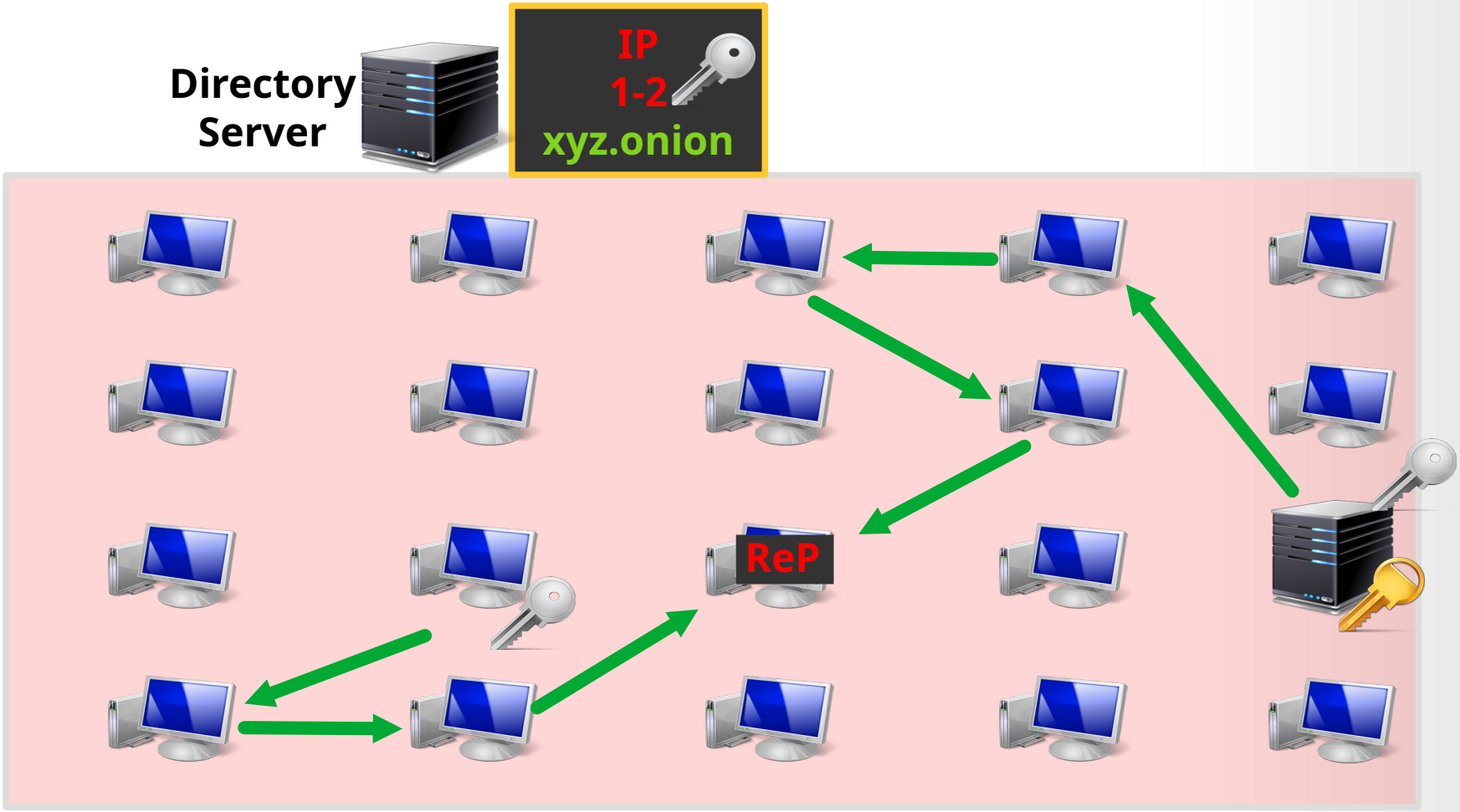
Hidden Services



Hidden Services



Hidden Services



Tor

- ~~Il circuito Tor~~
- ~~Instaurazione di un Hidden Service~~
- ~~Indirizzi .onion V3~~
- ~~Connessione ad un Hidden Service~~
- Bridge
- Pericoli

Tor

- ~~Il circuito Tor~~
- ~~Instaurazione di un Hidden Service~~
- ~~Indirizzi .onion V3~~
- ~~Connessione ad un Hidden Service~~
- ~~Bridge~~
- Pericoli

Pericoli

- DNS leak
- Javascript

Pericoli

Server DNS

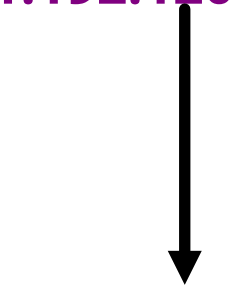
sito.com
aka
31.192.120.36

Chi è sito.com?

Pericoli

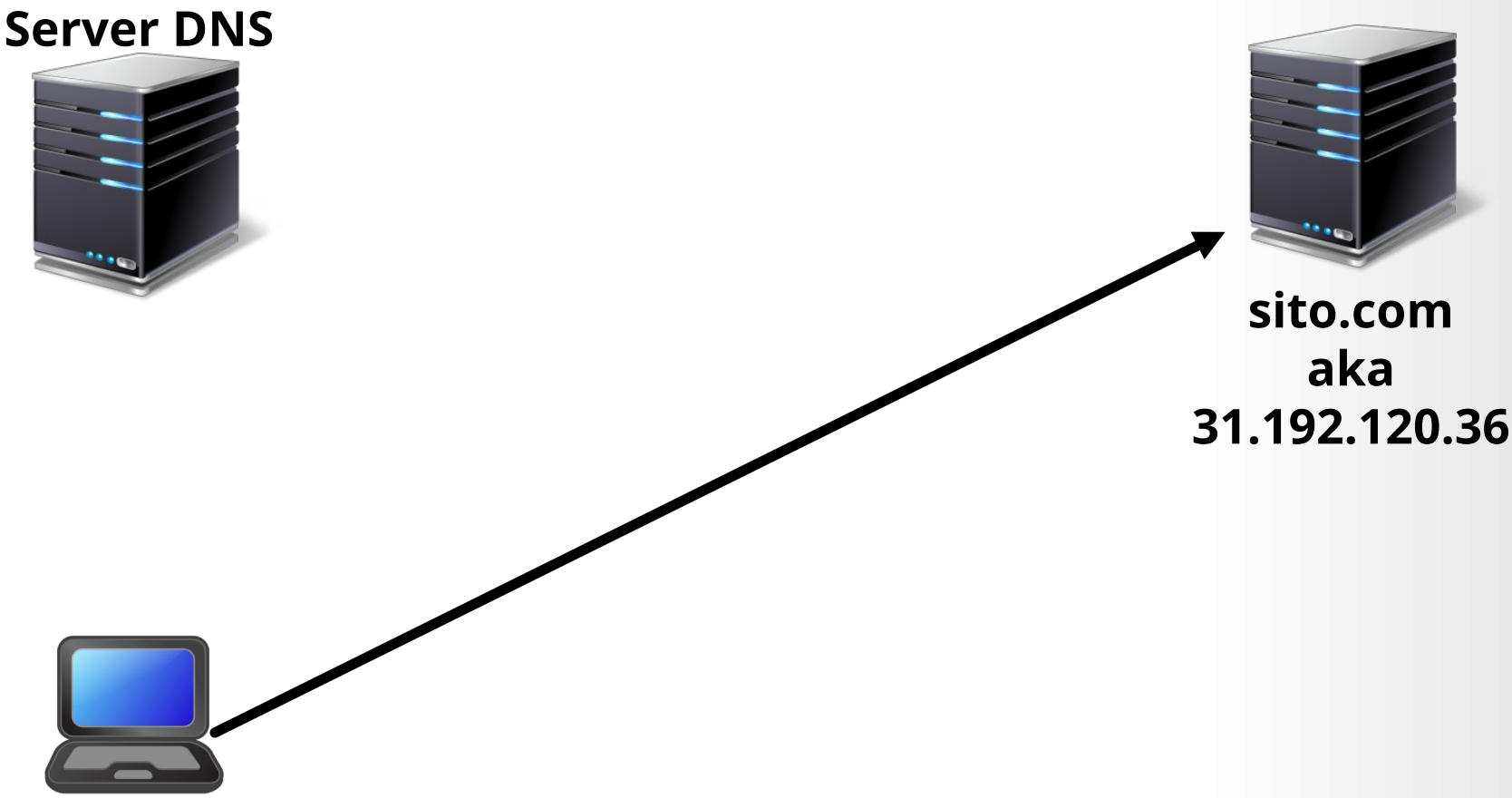
Server DNS

31.192.120.36

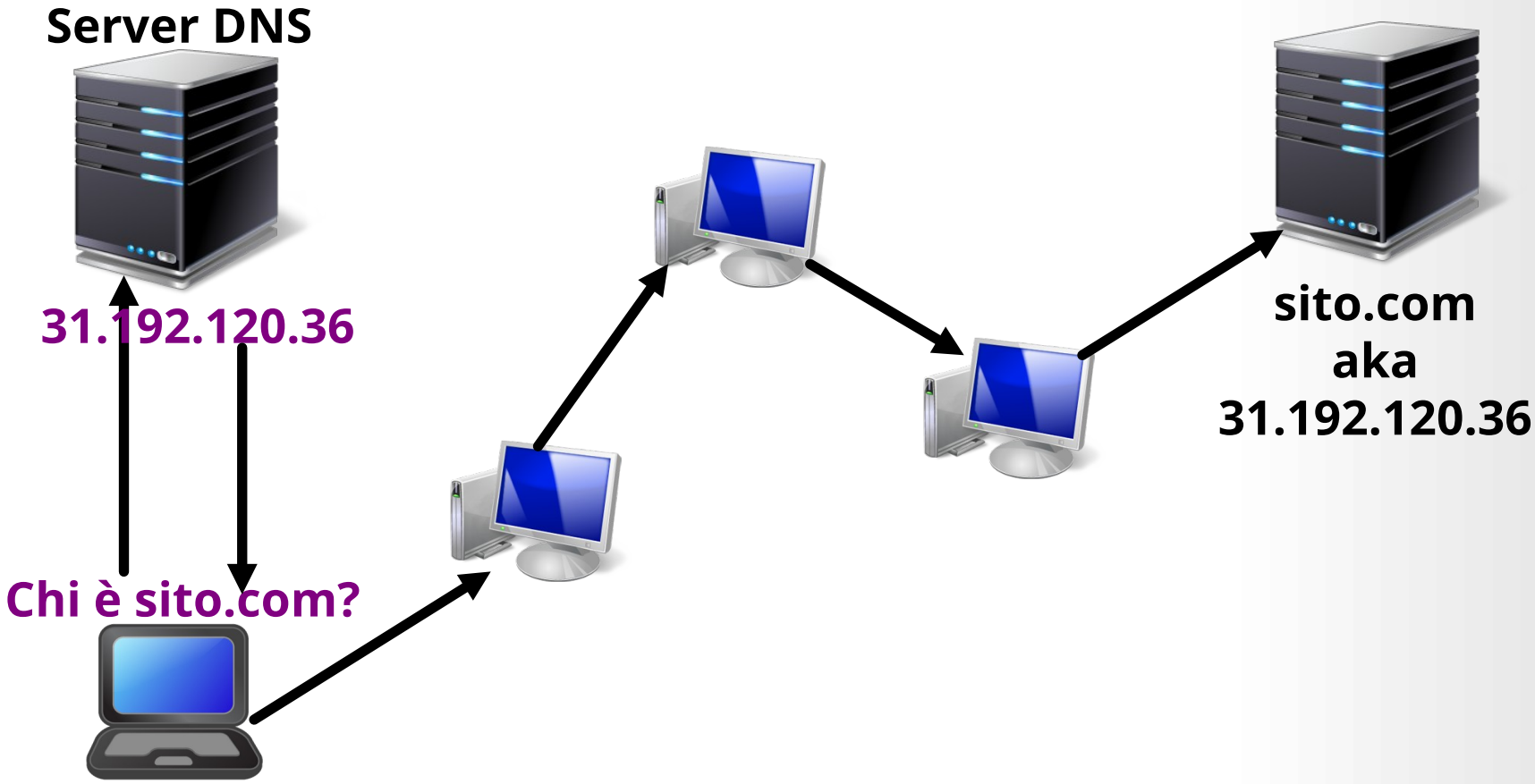


sito.com
aka
31.192.120.36

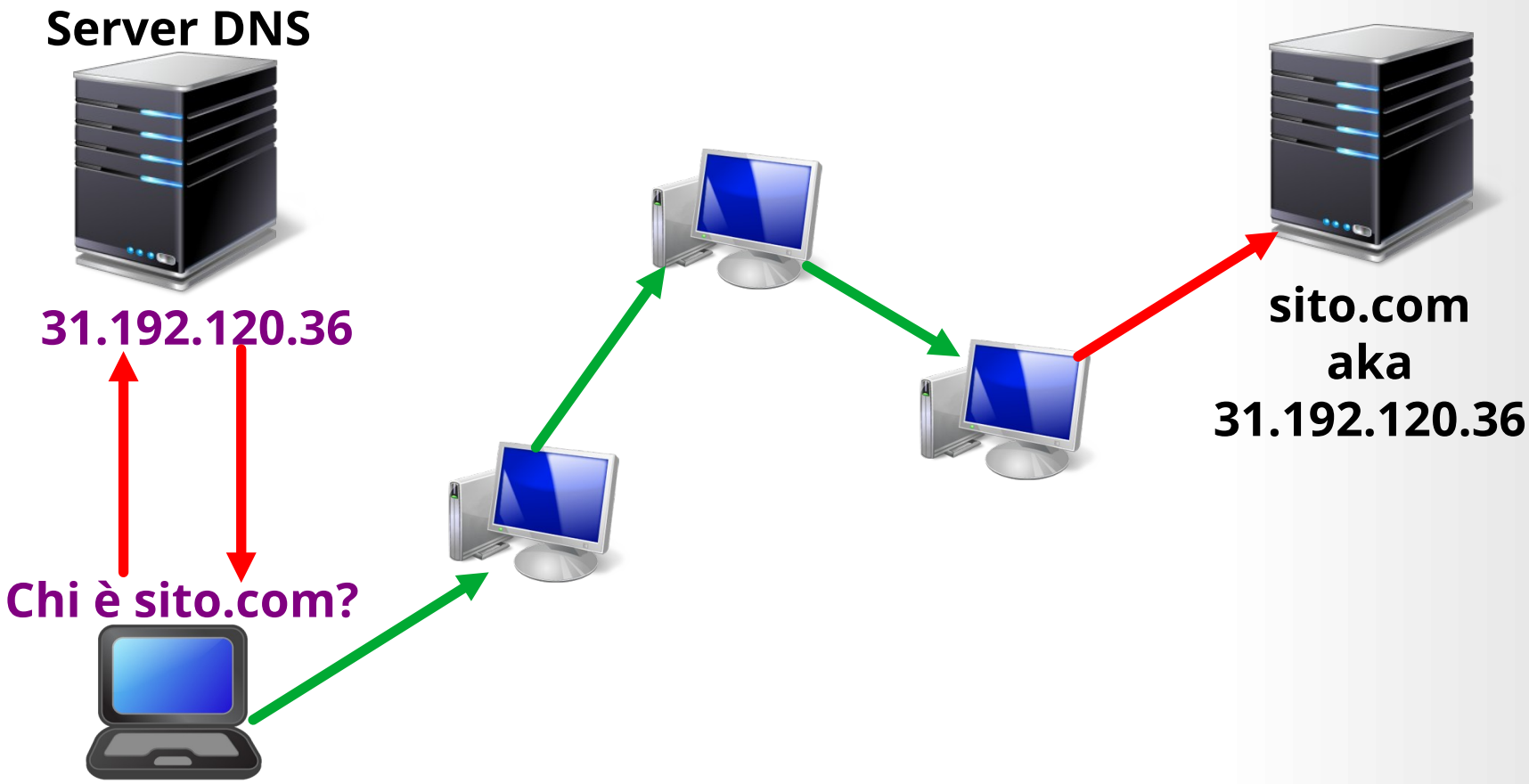
Pericoli



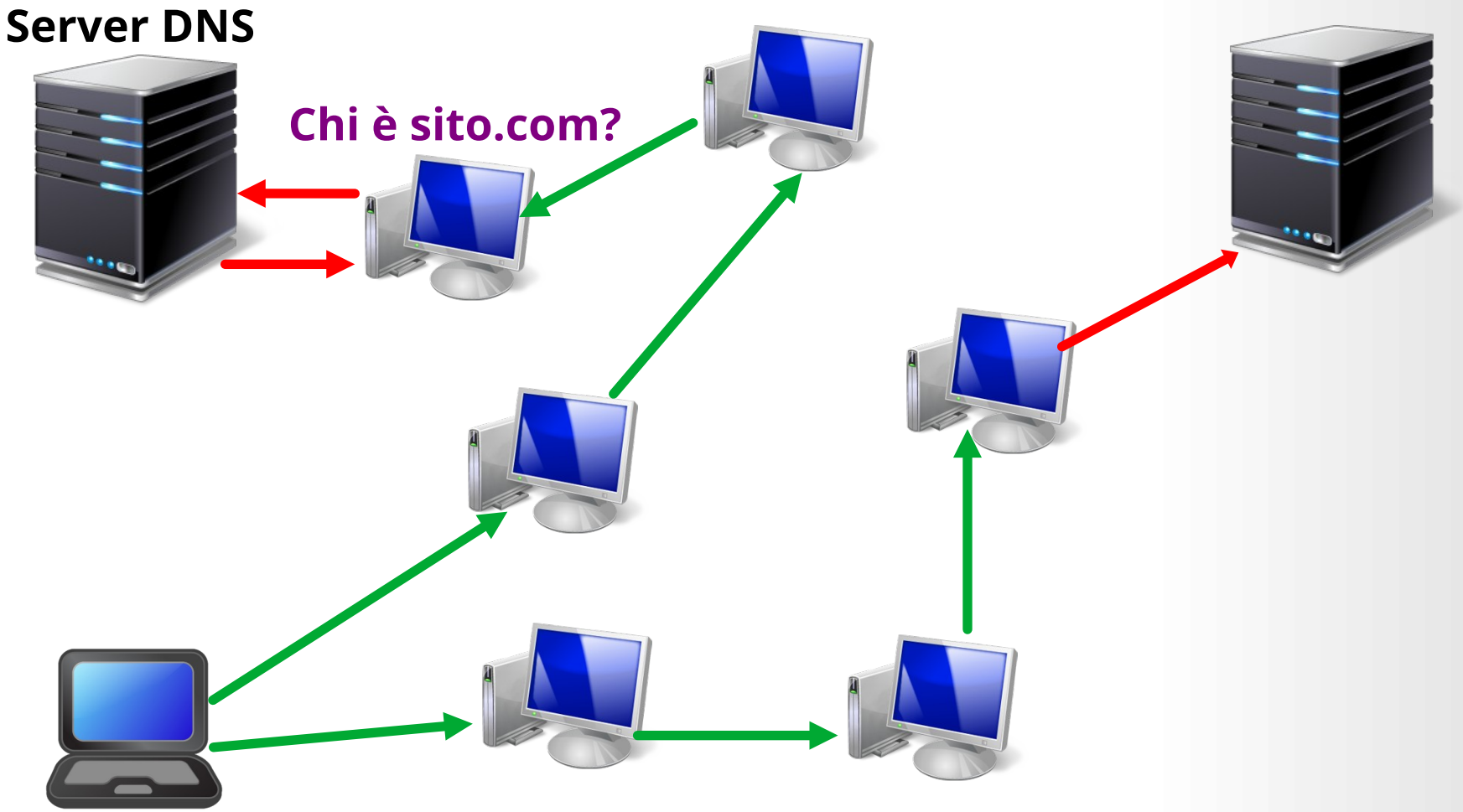
Pericoli


Server DNS
31.192.120.36
Chi è sito.com?
sito.com
aka
31.192.120.36

Pericoli


Server DNS
31.192.120.36
Chi è sito.com?
sito.com
aka
31.192.120.36

Pericoli



Pericoli