secure file storage for the 20th century

Lane Lawley

Can we store files in multiple servers

even if any of them can fail at any time?

What if every data center contains sensitive information we want to protect?

The government could take any of our data centers!

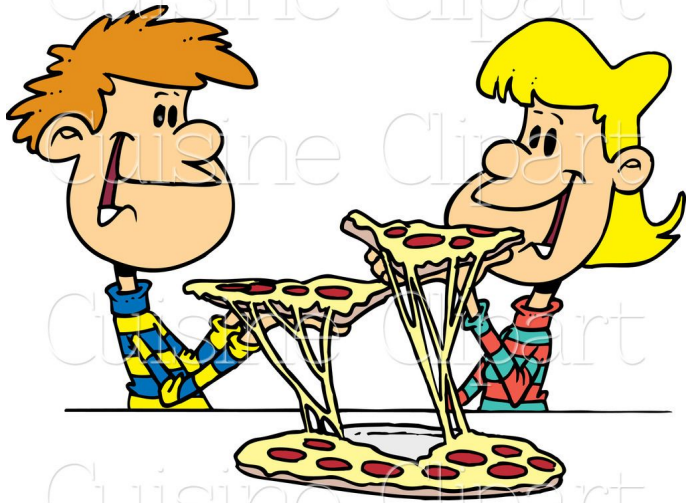
It might sound hard to believe, but as early as 2008, some technologists predict that the government could initiate large-scale tracking operations on its OWN citizens!!!

So let's give every country a piece of the file!

They can work together!

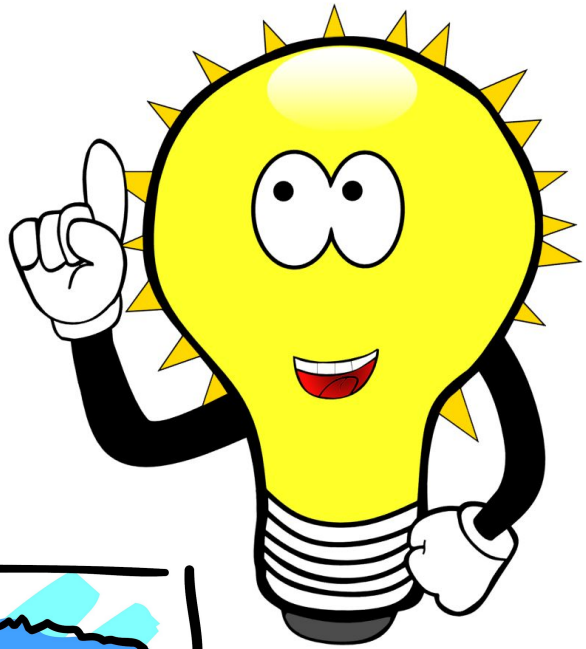
They can put it back together!

…right?



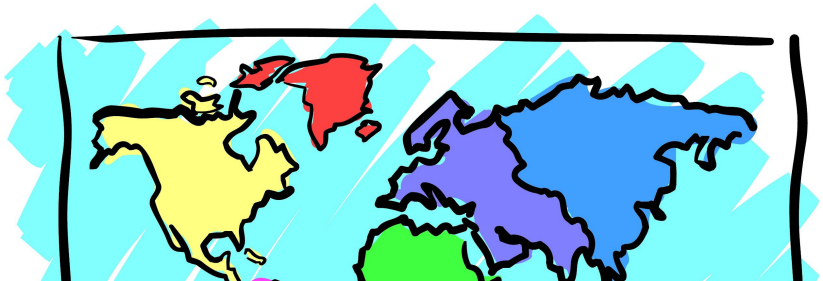
Better idea

We divide the KEYS into pieces (keys are small!)

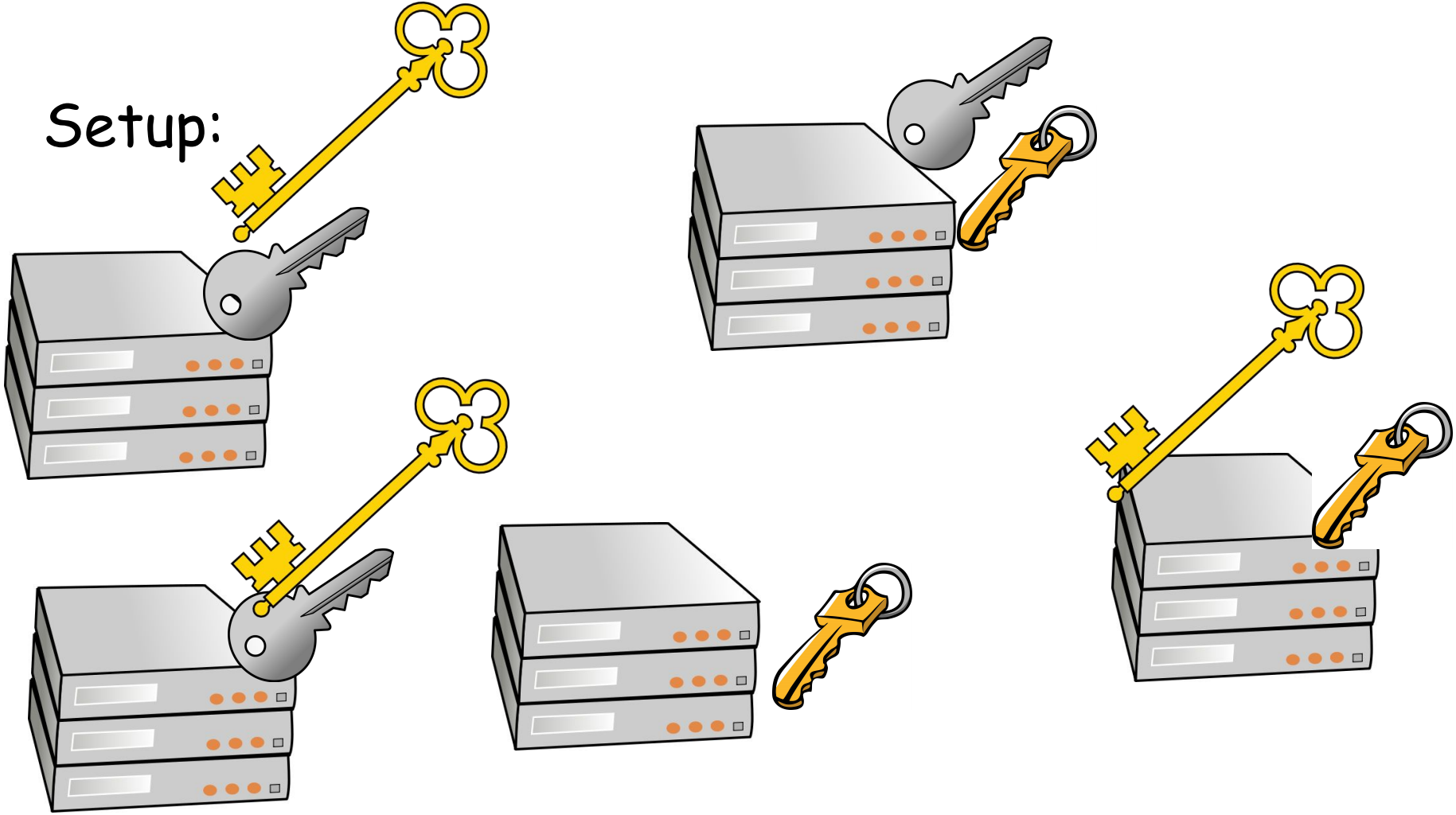


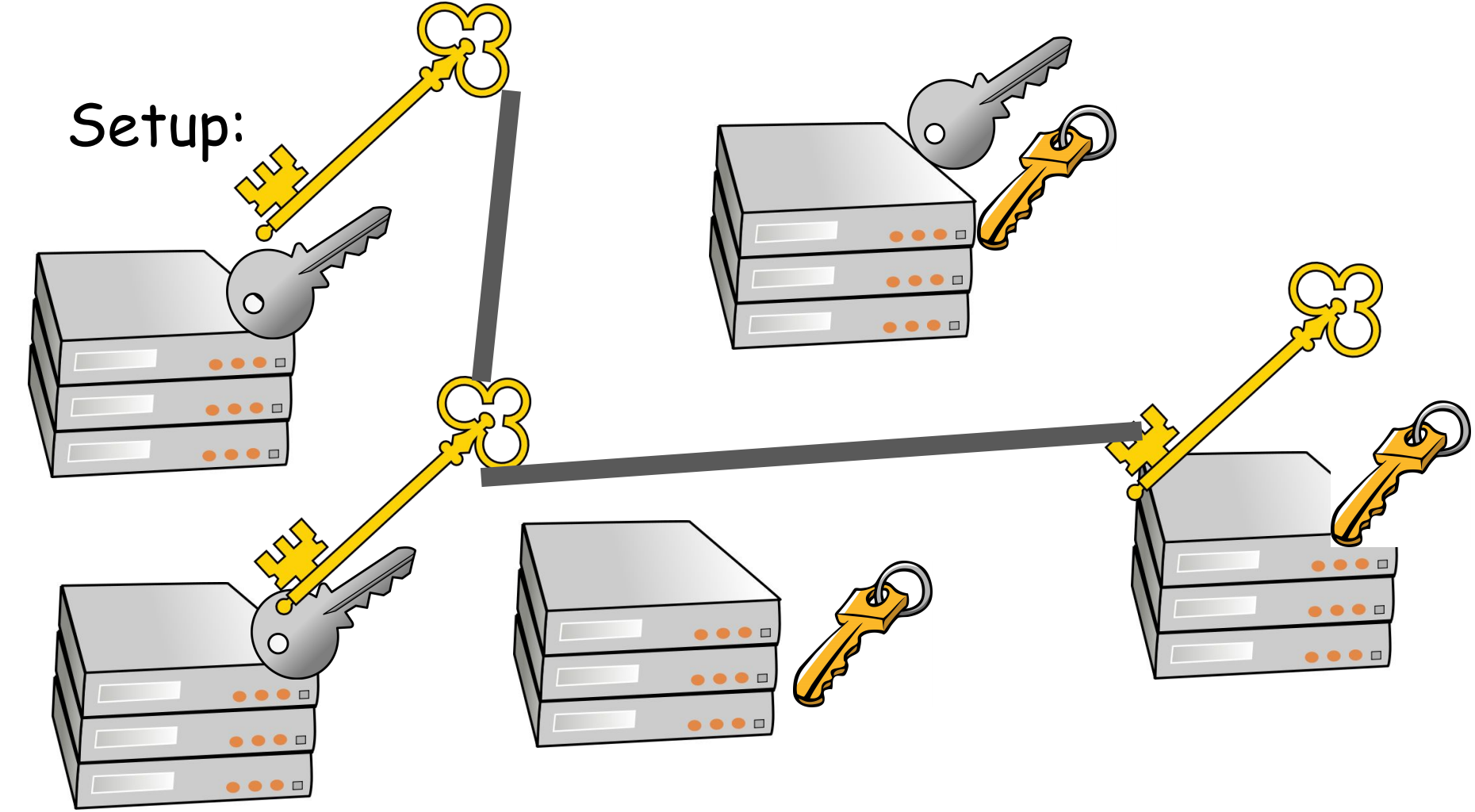
Then we give the keys to WAY MORE countries

Even if they don't have the files

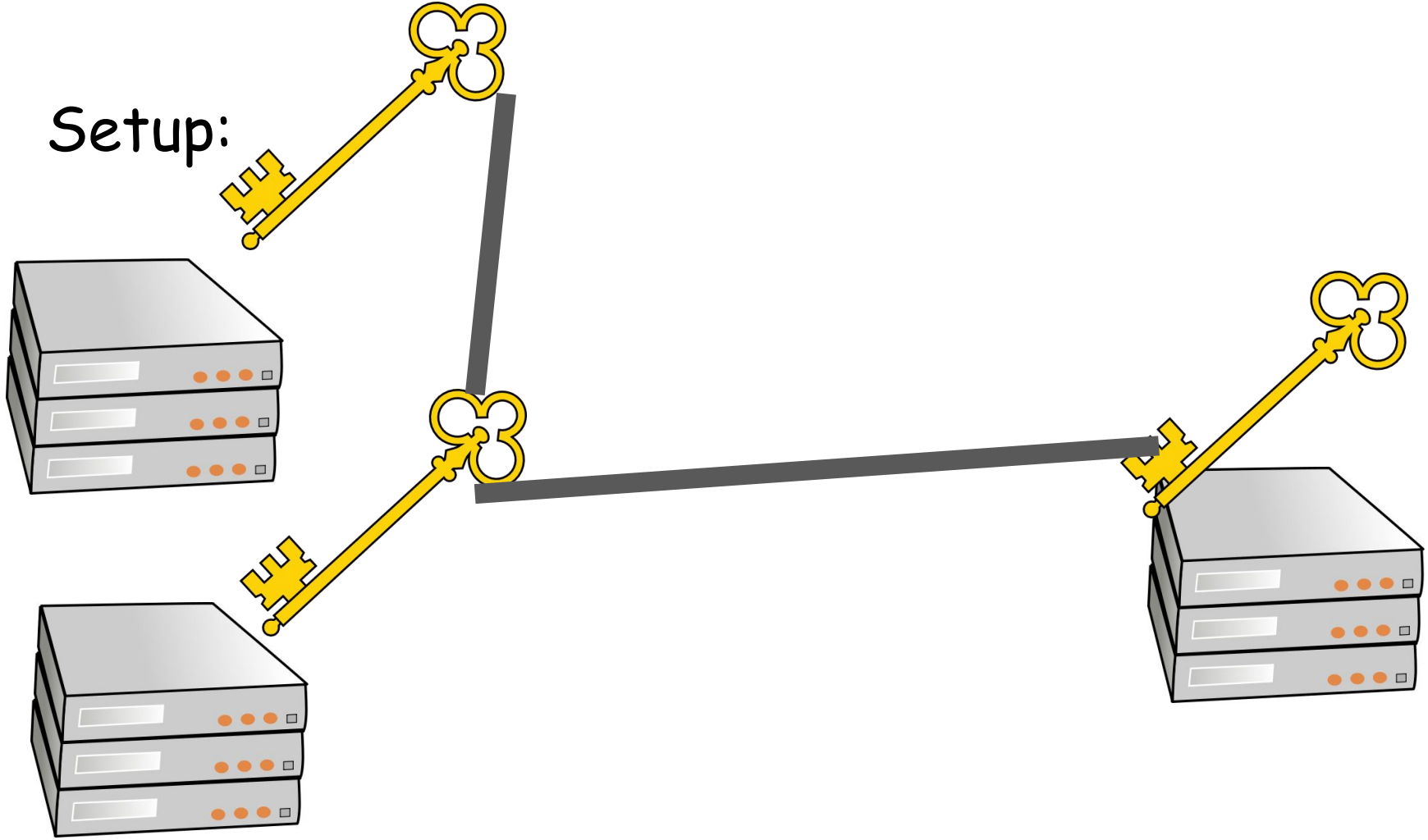


Setup:




Setup:

Setup:



Key sharing details

- Shamir's secret sharing

Key sharing details

- Shamir's secret sharing
- Client asks for all replicas for filename & their public keys

Key sharing details

- Shamir's secret sharing
- Client asks for all replicas for filename & their public keys
- Client makes key-pieces, encrypts w/ public keys, sends to coordinator

Key sharing details

- Shamir's secret sharing
- Client asks for all replicas for filename & their public keys
- Client makes key-pieces, encrypts w/ public keys, sends to coordinator
- When reading, client asks for key pieces

Key sharing details

- Shamir's secret sharing
- Client asks for all replicas for filename & their public keys
- Client makes key-pieces, encrypts w/ public keys, sends to coordinator
- When reading, client asks for key pieces
- Replicas encrypt their key pieces w/ client's public key, send back

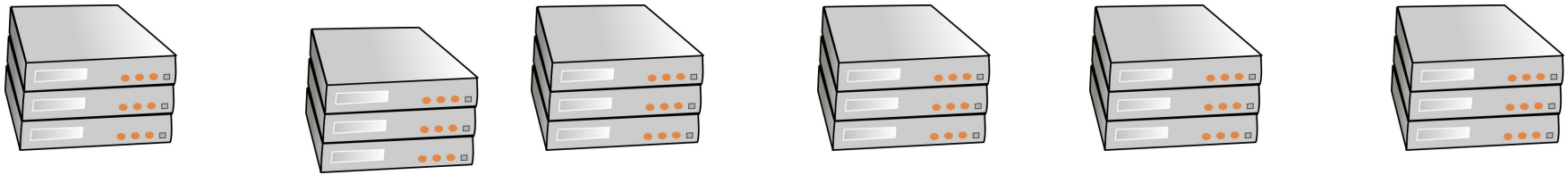
Key sharing details

- Shamir's secret sharing
- Client asks for all replicas for filename & their public keys
- Client makes key-pieces, encrypts w/ public keys, sends to coordinator
- When reading, client asks for key pieces
- Replicas encrypt their key pieces w/ client's public key, send back
- Client decrypts key pieces, assembles key, decrypts file

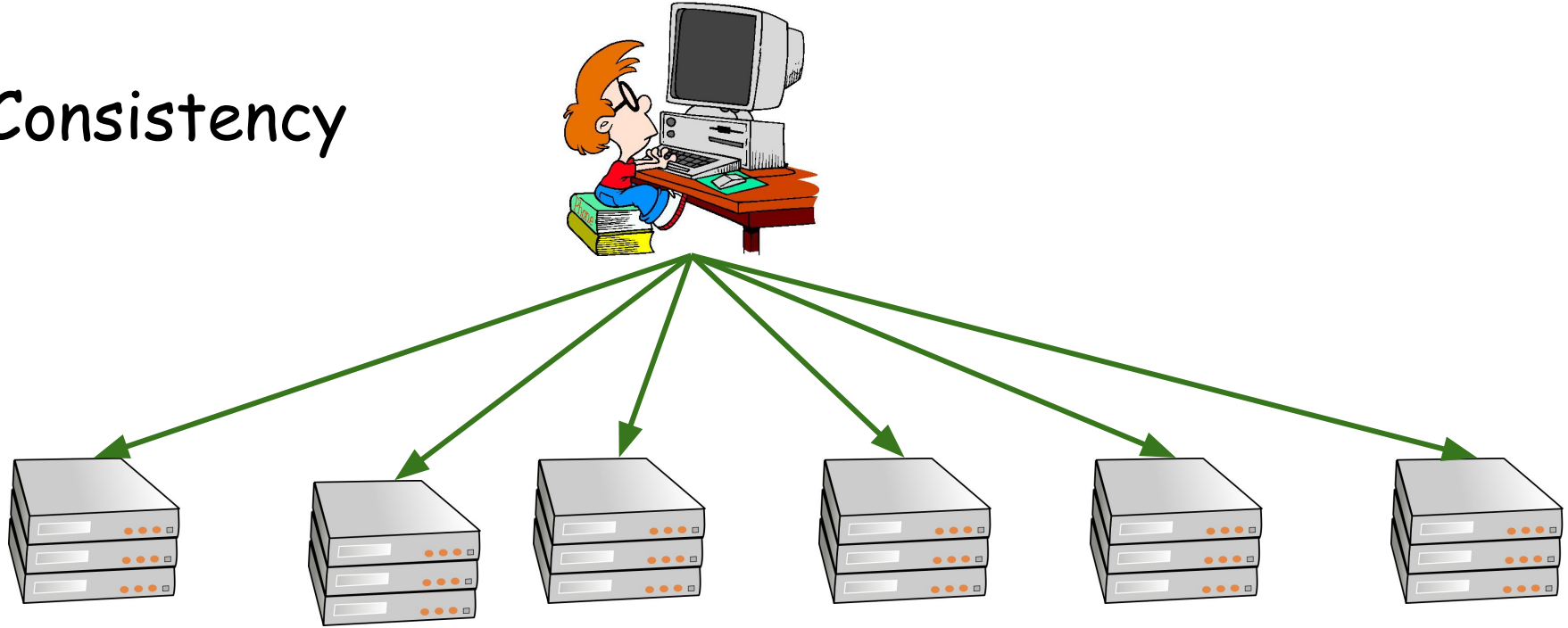
Ke s

- as for file
- , encrypts coordinator
- ks for key
- Replicas encrypt their key pieces
- Client decrypts key pieces, assemb

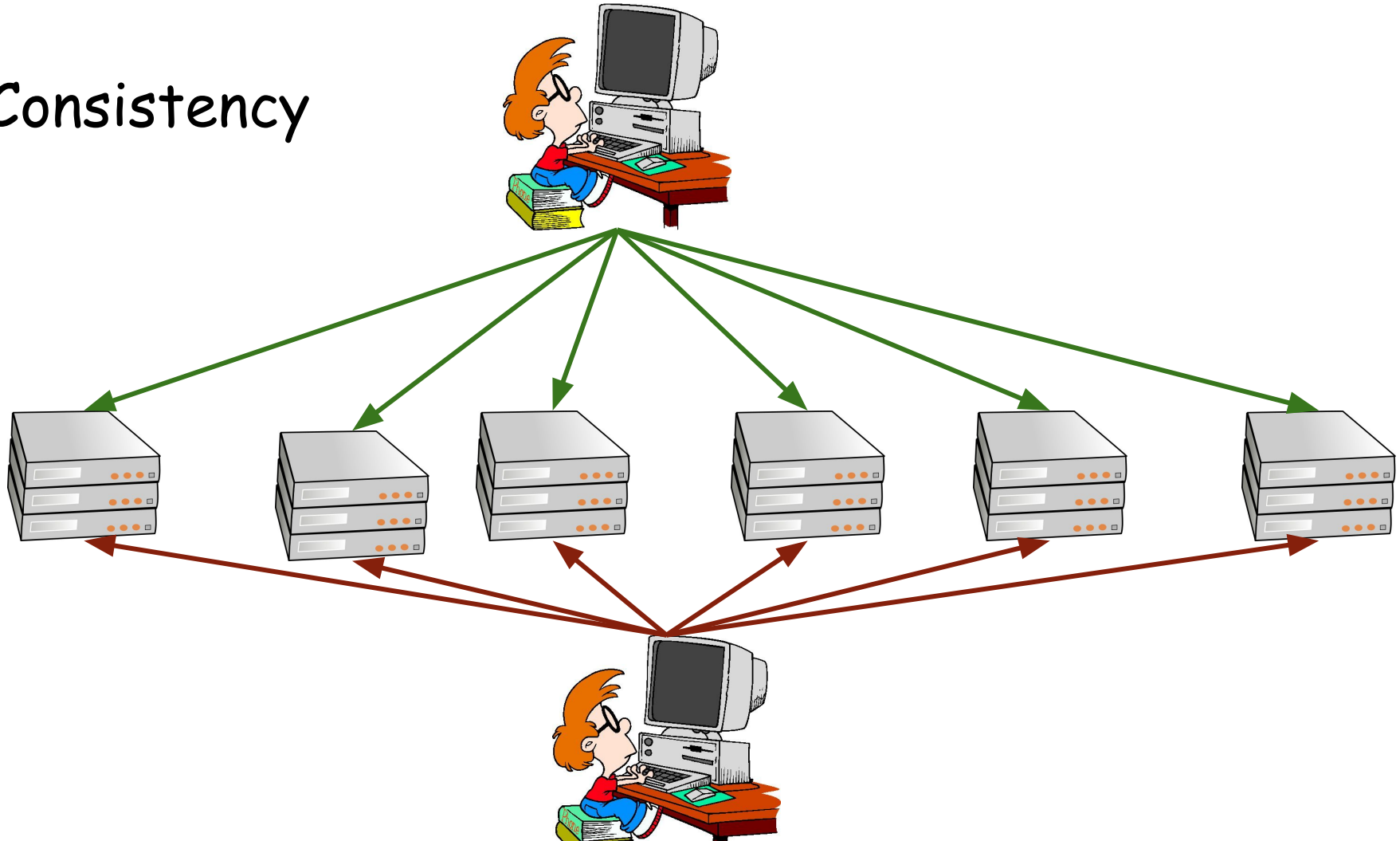
Consistency



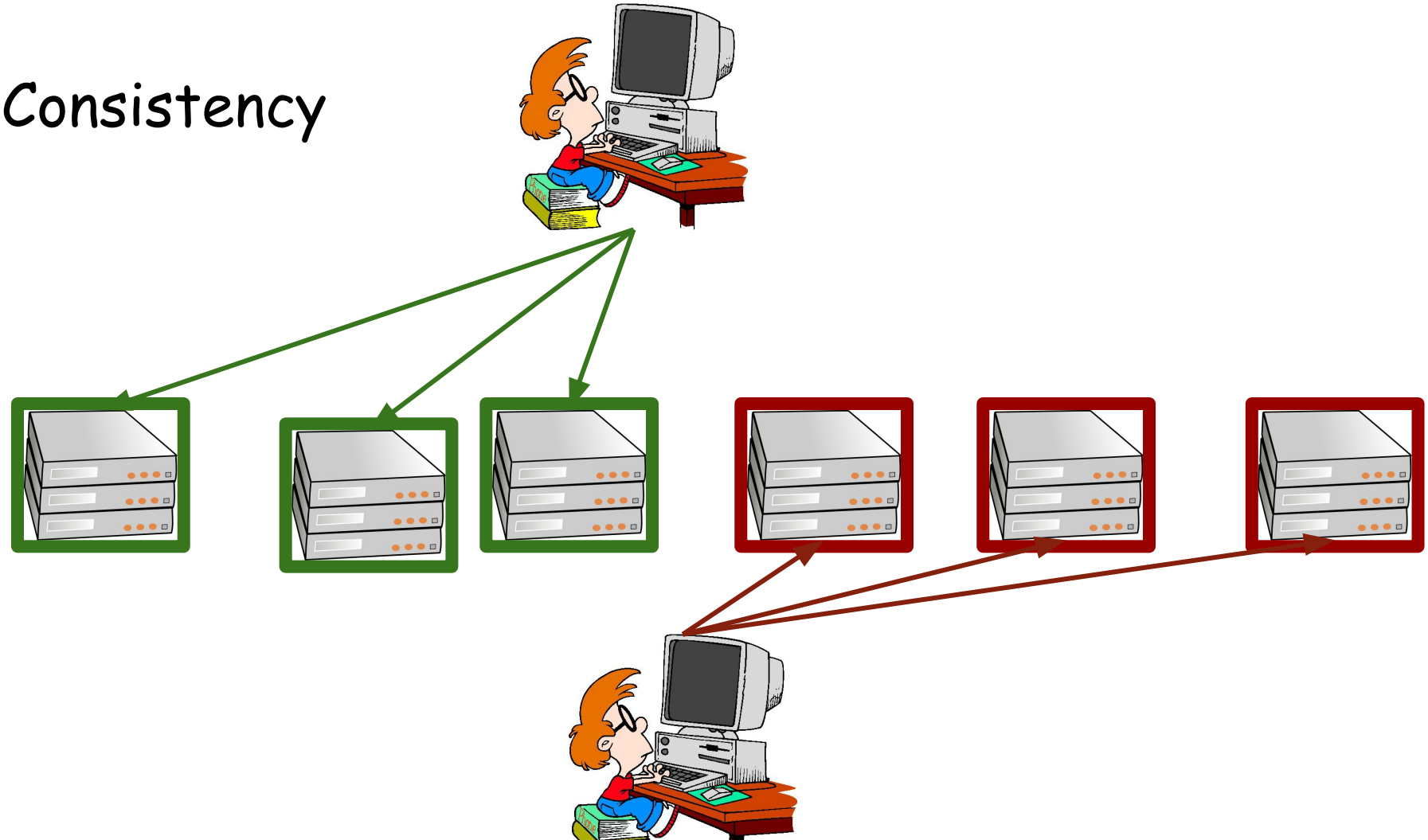
Consistency



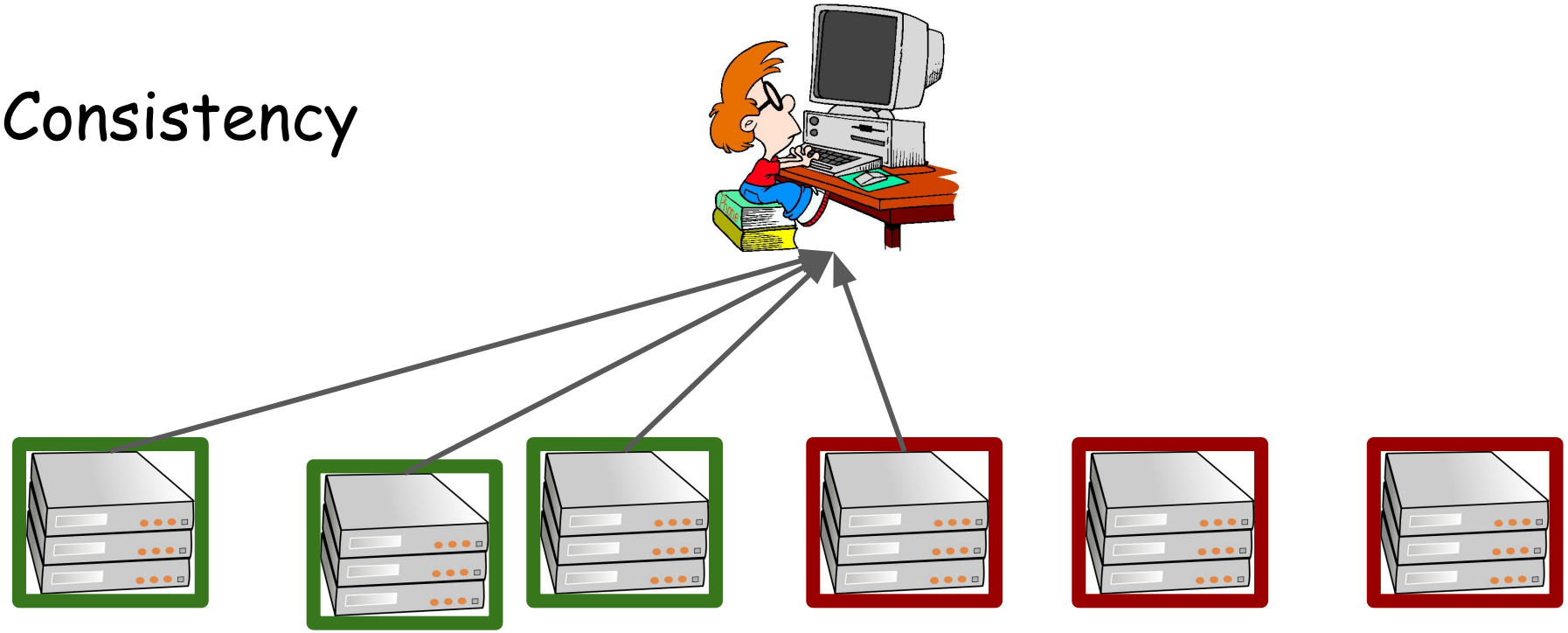
Consistency



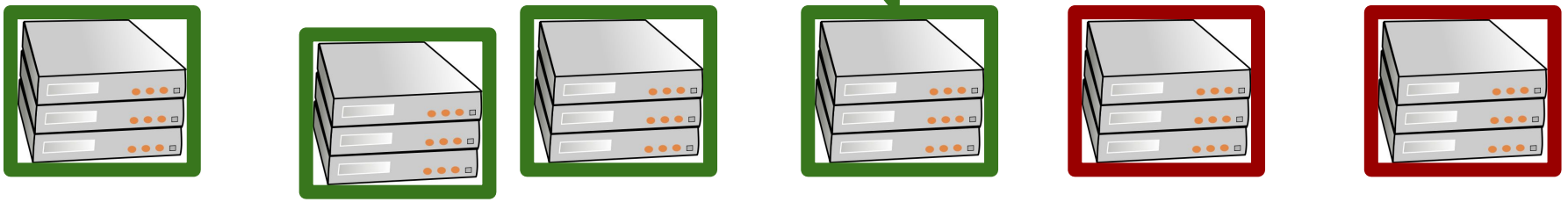
Consistency



Consistency



Read Repairs




QUESTIONS?