How Do We Know that Keys are Valid?

Cryptography is pretty hard to break.

Fooling the humans who use it … not so hard.

How do your browser and a server

- **know that no one in the middle of the Internet**
- **is "helping" to agree on a key?**

How do you know that the "public key for Lumetta" is really mine?

Trust has to start somewhere.

For most people, it's not with the government.

And it's not with most companies.