Sending a Private Message with a Public Key
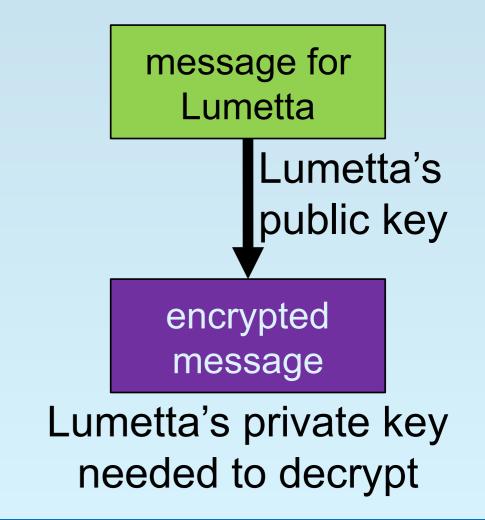
If you want to send a message
that only I can read, you
- **obtain my public key**
- **use it to encrypt** the message, and
- send (or even broadcast!)
  the encrypted message.

Only I have the private key,
so only I can decrypt the message.

message for Lumetta

Lumetta's public key

encrypted message

Lumetta's private key needed to decrypt