TLS 1.3 is much better than TLS 1.2

- ✓ Only one round in the handshake (vs 2 with TLS 1.2)
- ✓ Faster (use of elliptic curves)
- ✓ Certificate is encrypted (better confidentiality)
- ✓ Protocol has been formally proven
  (dos not prevent from implementation bugs)

Almost there …

✓ Does ensure the confidentiality of the communication

✓ Does authenticate Alice and bob

✓ Does prevent replay attacks

➡ But how to ensure the authenticity of the public keys without using a Public Key Server ?