Not a perfect protocol yet

- ✓ Does authenticate Alice and bob
- ✓ Does prevent replay attacks
- ✓ Does ensure the authenticity of the public keys
- ◉ But the Public Key Server is a single point of failure

TLS - Transport Layer Security

a.k.a SSL - Secure Sockets Layer