TLS -> Transport Layer Security

1. Exchange a symmetric "one time pad"
2. They are talking to who they think they are talking to
3. No one was eaves dropping on our key exchange.

History Lesson

- SSL ≠ TLS even though people still call TLS SSL.
- Mid 90s Netscape
  - SSL 1.0 -> So Flawed never released
  - SSL 2.0 -> Released even though it was Flawed
  - SSL 3.0 -> Set the standard, but still Flawed (1996)
  - TLS 1.0 -> Fixed SSL 3.0 Flaws (1999)
  - TLS 1.3 -> TLS 1.0 is now deprecated (2018)

TLS 1.0 Downgrade attack

IF the server said it could only do SSL 3.0 the browser downgraded without a warning.