Certificates 101

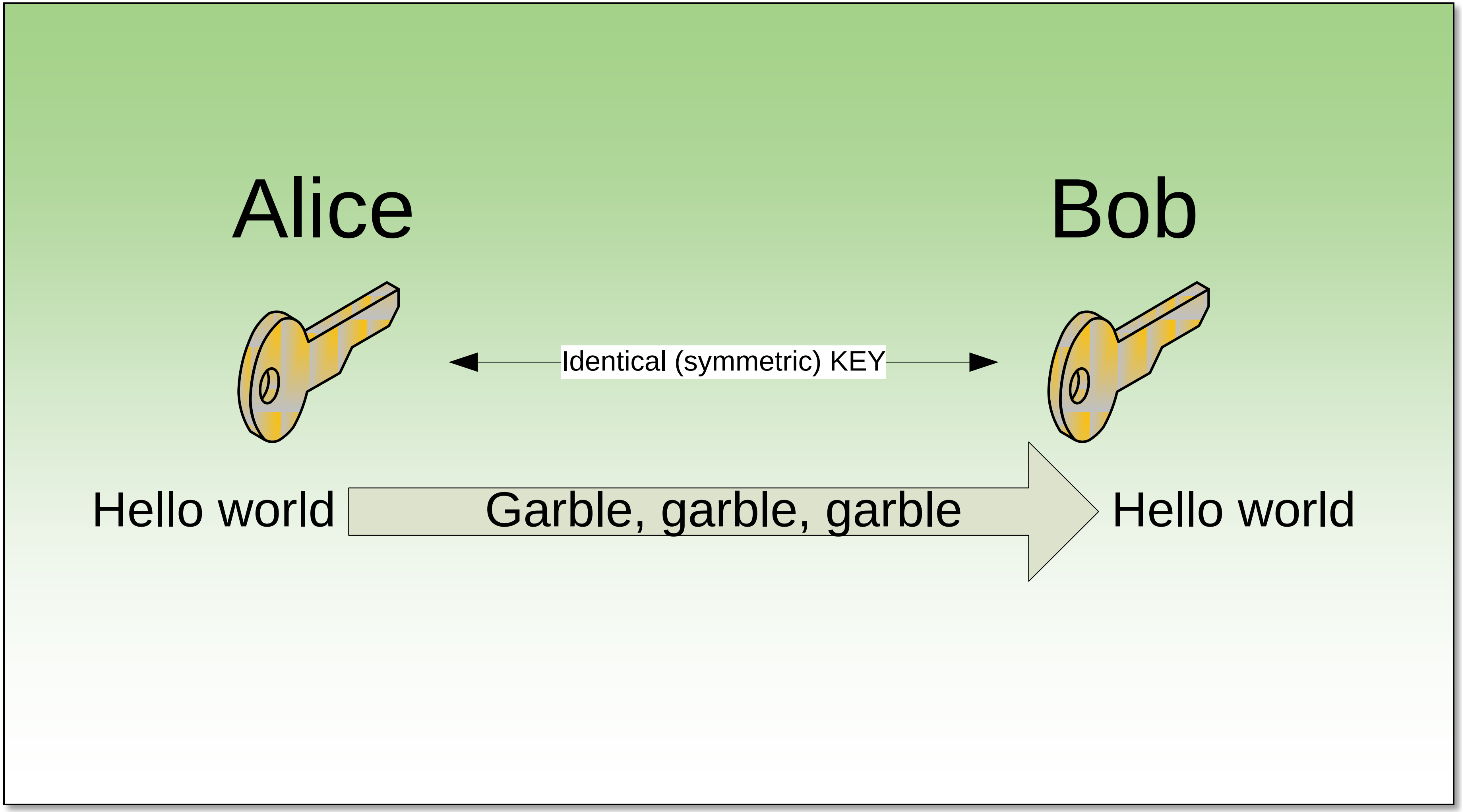
Paul Lemmers

http://www.pluralsight.com/

Overview

- This introduction
- Keys: encryption and signatures
- Certificates (certs) layout and files
- UI
- Different application usages
- Self signed
- Certificate Authority (CA)
- References

Symmetric KEY



Alice

Bob

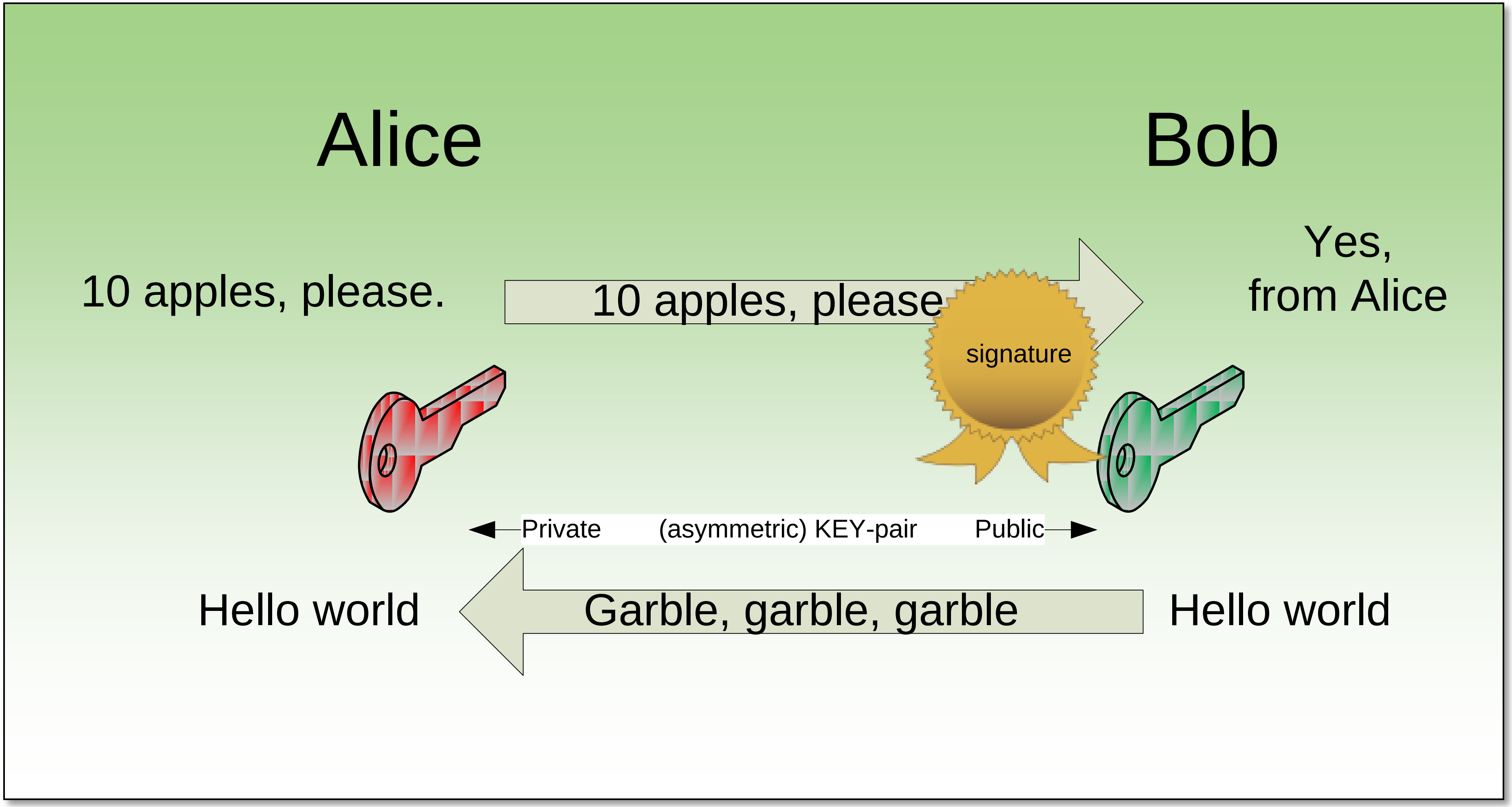
Identical (symmetric) KEY

Hello world

Garble, garble, garble

Hello world

Public-Private KEY-pair



Alice

Bob

10 apples, please.

10 apples, please

signature

Yes,
from Alice

Private (asymmetric) KEY-pair Public

Hello world

Garble, garble, garble

Hello world

Object IDentifier (OID)

- **A hierarchical numbering system to uniquely identify variables/attributes**
- **May have seen it in LDAP and/or SNMP**

- **Examples:**
  - 1.3.6.1.5.5.7.3.2 (Client Authentication, SSL)
  - 1.3.6.1.5.5.7.3.1 (Server Authentication, SSL)
  - 2.5.4.44 (givenName, LDAP)
  - 1.3.6.1.4.1.311.etc.etc. (Microsoft Enterprise space)

- **Once obtained, you use your "root" and define a hierarchy of your variables below it**

References

- **Peter Gutmann**
  - Everything you Never Wanted to Know about PKI but were Forced to Find Out. (Presentation with lots of facts but certainly not lacking humor.)
  - X.509 Style Guide. October 2000. (very detailed instruction on how to encode things, or not worry about them, also full of humor.)
  - His –draft- book.
- **Brian Komar**
  - Windows Server 2008 PKI and Certificate Security. 2008.
    ISBN-13 978-0-7356-2516-7. (Mostly infrastructure, not development)
- **RFC 5280 (PKIX Certificate and CRL Profile)**