

Introducción a la criptografía de clave pública

Israel Herraiz
Universidad Politécnica de Madrid
<israel.herraiz@upm.es>

Madrid On Rails
1 de abril de 2011

(c) 2011 Israel Herráiz Tabernero

El autor de este documento hace entrega del mismo al Dominio Público.

Puedes, sin permiso previo del autor, copiarlo en cualquier formato o medio, reproducir parcial o totalmente sus contenidos, vender las copias, utilizar los contenidos para realizar una obra derivada y, en general, hacer todo aquello que podrías hacer con una obra de un autor que ha pasado al dominio público.

El paso de una obra al dominio público supone el fin de los derechos económicos del autor sobre ella, pero no de los derechos morales, que son inextinguibles. No puedes atribuirte su autoría total o parcial. Si citas el documento o utilizas partes de él para realizar una nueva obra, debes citar expresamente tanto al autor como el título. No puedes utilizar este documento o partes de él para insultar, injuriar o cometer delitos contra el honor de las personas y en general no puedes utilizarlo de manera que vulnere los derechos morales del autor.

Privacidad en las comunicaciones

- Por defecto, las comunicaciones electrónicas son totalmente abiertas
- Cualquier persona que actúe de enlace en la comunicación, puede espiar y extraer información

Ejemplo: búsqueda sensible en Google

¿Por dónde y por cuántos sitios pasa una búsqueda en Google?

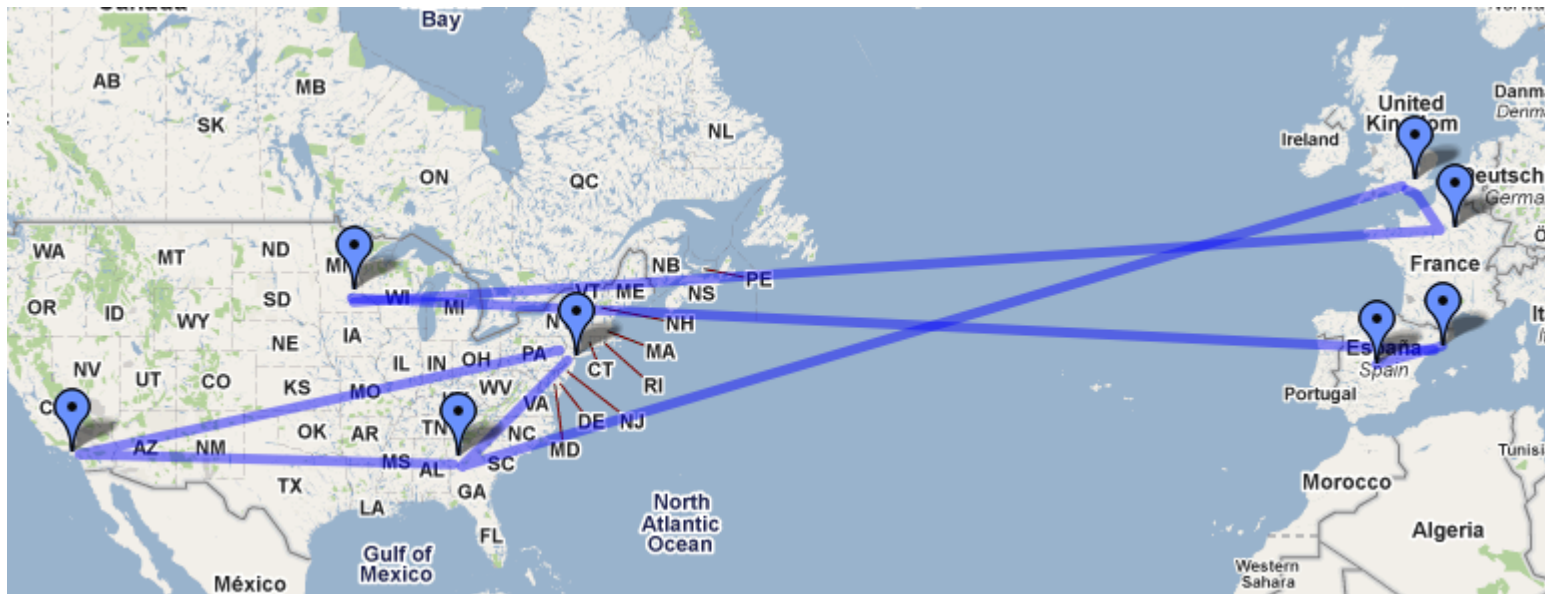
Llegando hasta Google

```
1 10.8.0.1 (10.8.0.1)
2 192.168.1.1 (192.168.1.1)
3 62.81.125.179.static.user.ono.com (62.81.125.179)
4 10.115.49.217 (10.115.49.217)
5 10.127.151.49 (10.127.151.49)
6 10.127.10.137 (10.127.10.137)
7 10.127.10.133 (10.127.10.133)
8 10.127.3.82 (10.127.3.82)
9 213.242.71.21 (213.242.71.21)
10 ae-5-5.ebr1.Paris1.Level3.net (4.69.141.42)
11 ae-45-45.ebr1.London1.Level3.net (4.69.143.101)
12 ae-1-51.edge3.London1.Level3.net (4.69.139.73)
13 unknown.Level3.net (212.113.15.186)
14 209.85.255.78 (209.85.255.78)
15 66.249.95.173 (66.249.95.173)
16 216.239.49.45 (216.239.49.45)
17 * * *
18 ww-in-f147.1e100.net (209.85.229.147)
```

Llegando hasta Google

```
1 10.8.0.1 (10.8.0.1)
2 192.168.1.1 (192.168.1.1) Getafe
3 62.81.125.179.static.user.ono.com (62.81.125.179)
4 10.115.49.217 (10.115.49.217)
5 10.127.151.49 (10.127.151.49) Barcelona
6 10.127.10.137 (10.127.10.137)
7 10.127.10.133 (10.127.10.133)
8 10.127.3.82 (10.127.3.82)
9 213.242.71.21 (213.242.71.21) Mineápolis
10 ae-5-5.ebr1.Paris1.Level3.net (4.69.141.42) París
11 ae-45-45.ebr1.London1.Level3.net (4.69.143.101)
12 ae-1-51.edge3.London1.Level3.net (4.69.139.73) Londres
13 unknown.Level3.net (212.113.15.186)
14 209.85.255.78 (209.85.255.78) Atlanta
15 66.249.95.173 (66.249.95.173) Nueva York
16 216.239.49.45 (216.239.49.45) Los Ángeles
17 * * *
18 ww-in-f147.1e100.net (209.85.229.147) Atlanta
```

Todos los caminos llevan a Google



¿Y cuál es el problema?

**¿Qué
información sensible
se podría capturar
por el camino?**

Información capturada sin cifrado

- Localización geográfica aproximada
 - Con la dirección IP
- Navegador y sistema operativo usado
- Cualquier dato escrito en un formulario
 - Incluyendo passwords
- Cookies
 - Como curiosidad
 - <http://www.youtube.com/watch?v=yyLdxO6xvh8>
 - <http://www.youtube.com/watch?v=1FgKL2ywrX0>

Solución

**Cifrado obligatorio,
usando
Criptografía
de Clave Pública**

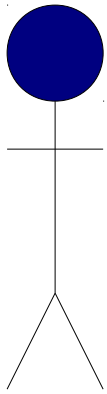
Contenidos

- Criptografía de clave pública
- PGP / GnuPG
- Protocolos para certificación de identidades
 - Firmado de claves

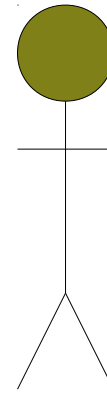
Criptografía

- Para cifrar información, tradicionalmente se usaba un password y un algoritmo
- Esquema simétrico
 - Requiere compartir el password entre los dos extremos de la comunicación
 - P.e.: libros de passwords de los submarinos en la WWII
- Esquema asimétrico: claves pública y privada
 - Permite comunicarse por un canal inseguro sin compartir previamente ningún secreto

Criptografía de clave pública

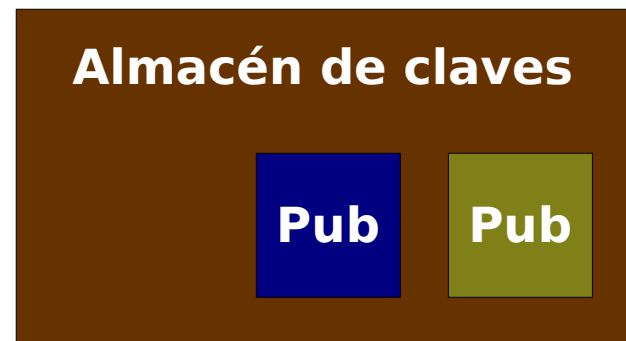
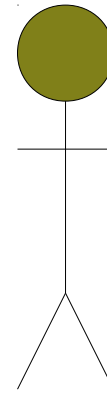
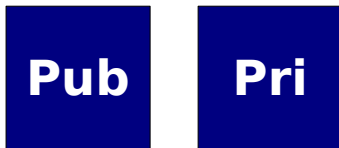
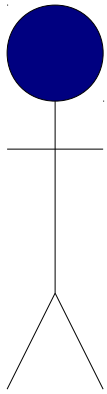


Pub **Pri**

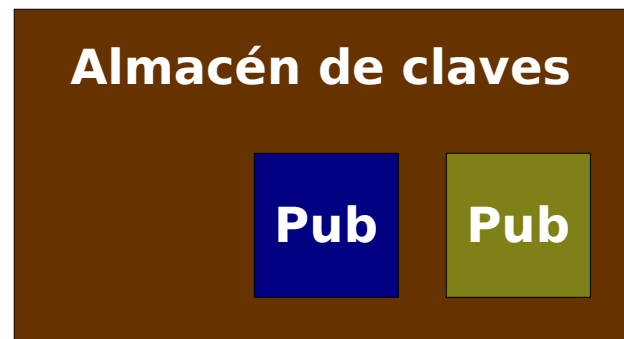
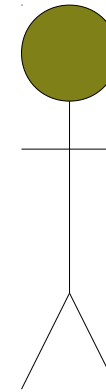
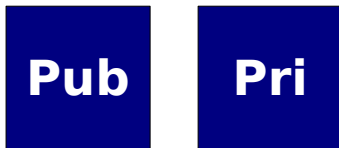
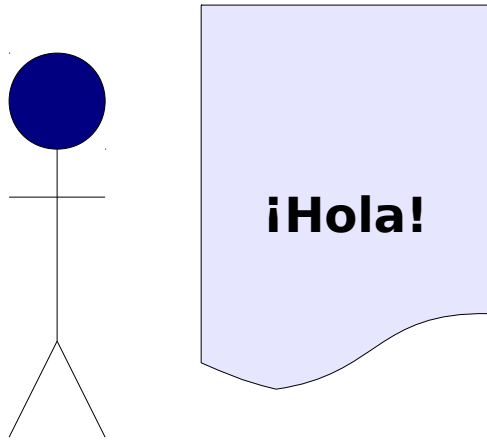


Pub **Pri**

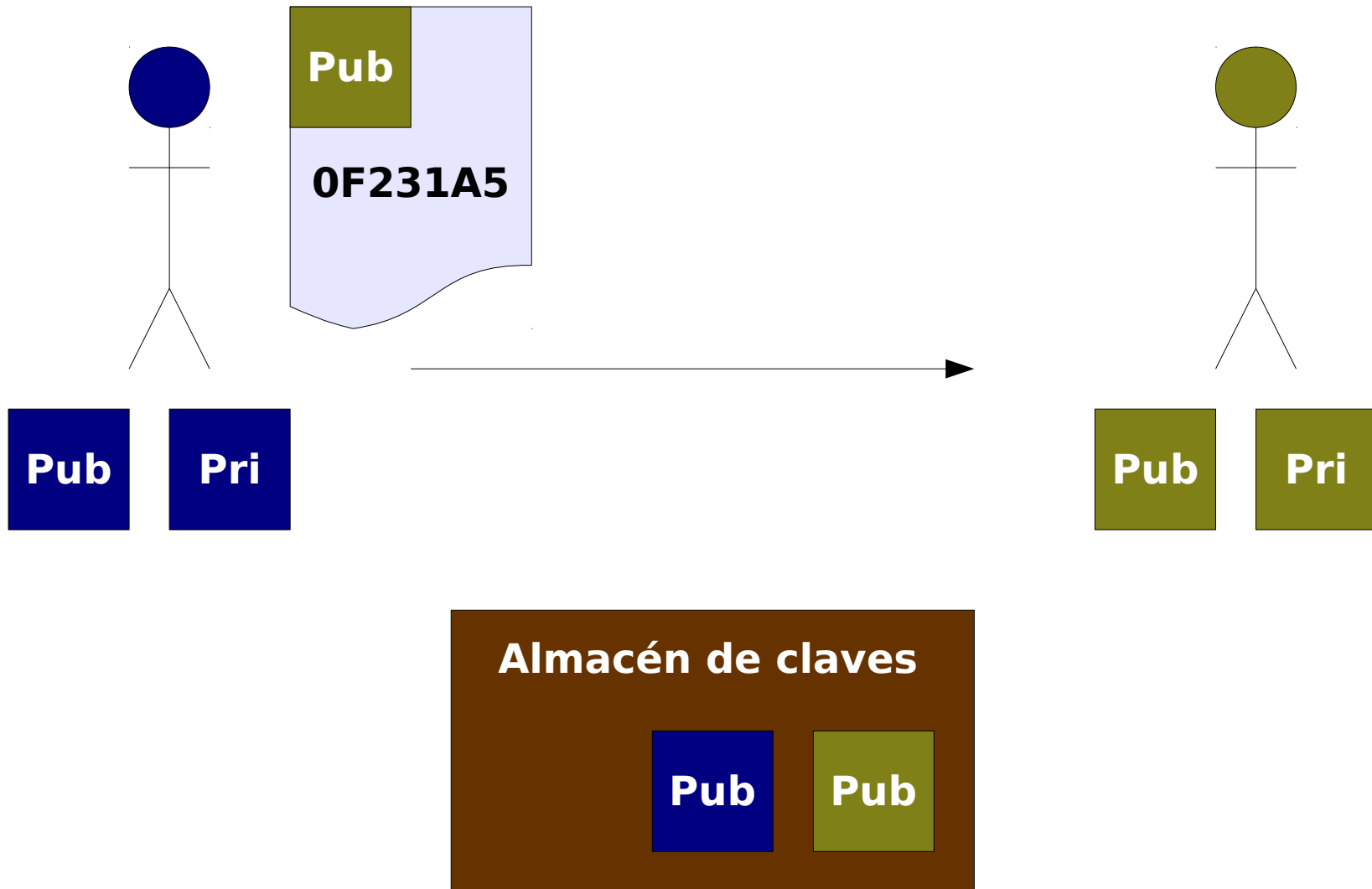
Criptografía de clave pública



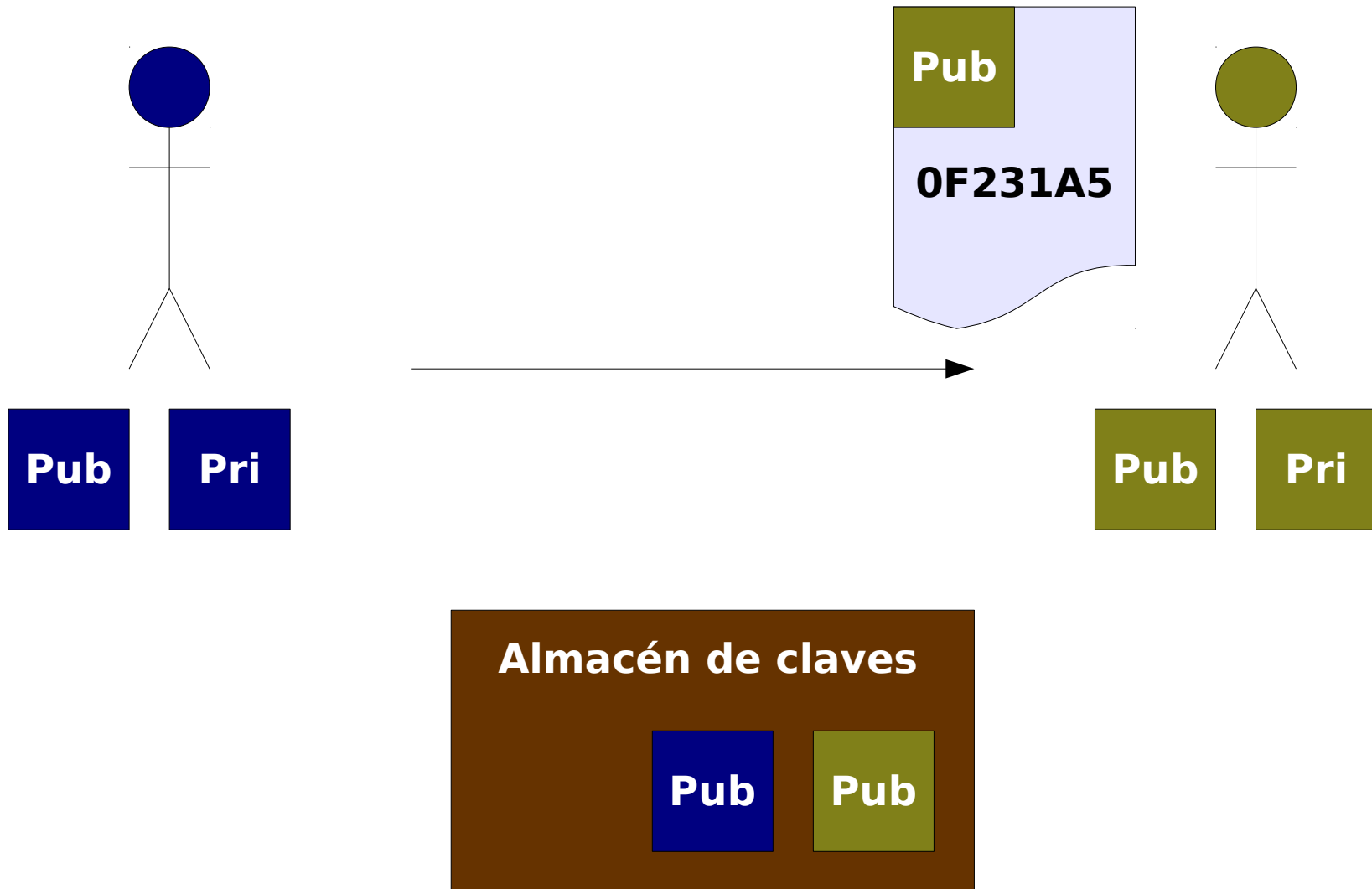
Criptografía de clave pública



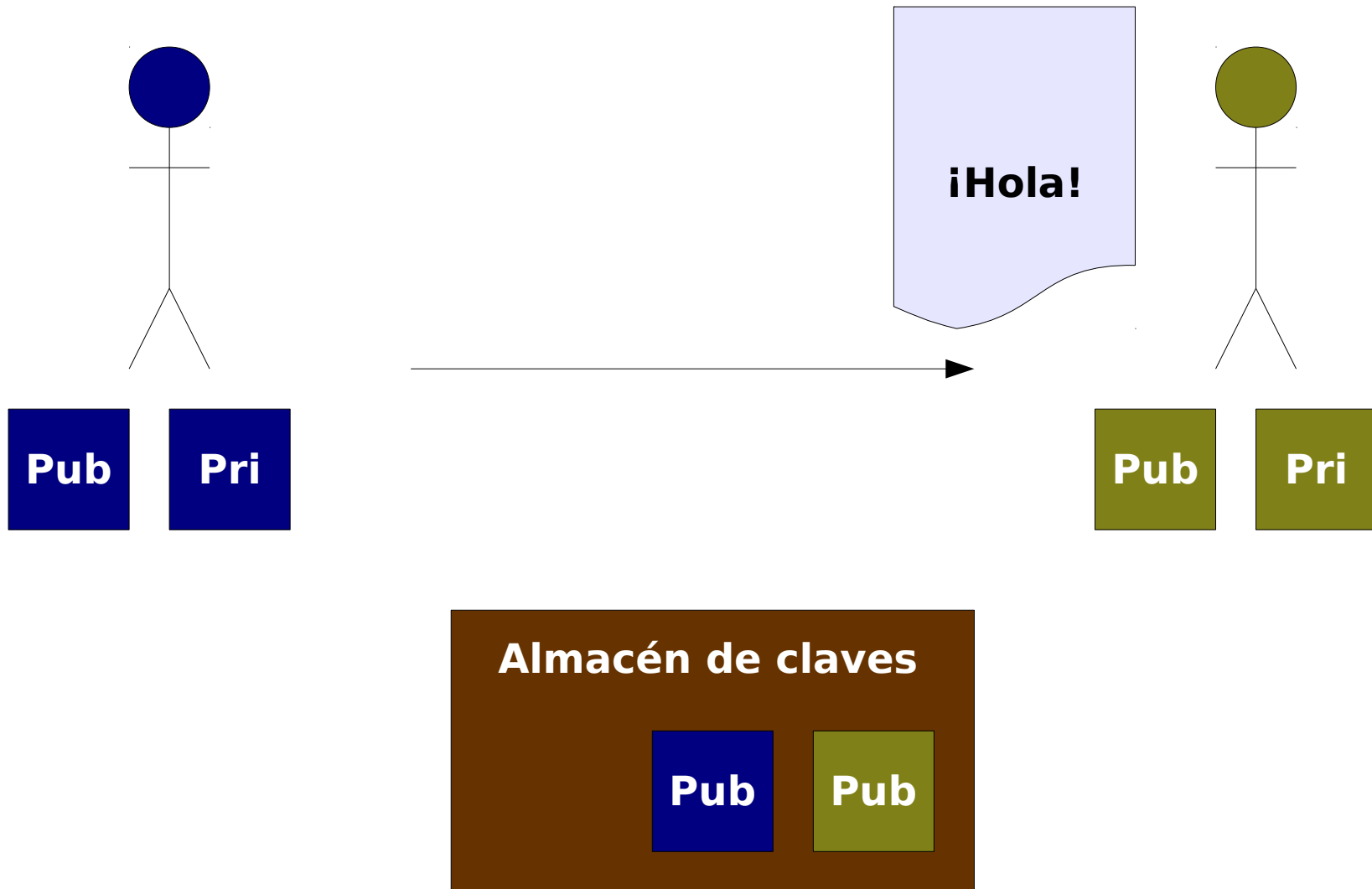
Criptografía de clave pública



Criptografía de clave pública



Criptografía de clave pública



¿Cómo funciona?

- Diferentes algoritmos
 - ¿Qué algoritmos habéis visto en la clase anterior?
 - A grandes rasgos, las claves son números primos
- Desde **un punto de vista matemático**, los mensajes son *descifrables*
- Desde **un punto de vista computacional**, descifrar un mensaje sin tener la clave privada lleva demasiado tiempo
 - La longitud de la clave es un parámetro fundamental

Ejercicio

Crea tu
par de claves
pública y privada

Una clave pública

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
```

```
Version: GnuPG v1.4.10 (GNU/Linux)
```

```
JeP5F/eRS9G8EE1fObRRW6mRf+bGSelufEMiOi3UB/5P0GBx8iM0QIjezR0R+2n8  
bMjuJmWHTjvEepInx9iual4J4BT/9FznFs7o4tFVVfYBacFrhWjQyAf2xoP3gyn3  
501V55VHVB+oidXUVNSNHZbXwrd1sH42x7x8o17PDFJrWjiq4kAb2EfSOIuSS6na  
K9Y06bqh3yRbVtRdZOuCLcY8QJwt/mx//uQqG6NuSvYhx1QyC6g==XuDES0IuSSa  
mQINBEtUTEQBEACEjdGQhscmsDXM7xG2/ZYFpMQg/GmPlJ85uJJUkLr2T+5Rw8Xv  
VfZjNZkMwsq94BGFrbXu477tKhQ5wiUBBz/jJ01a39Wrazgp21fvEon2T0Vay45t  
2BYbU4AF815UL6o74Y1W5SLdAofwy1ZS8pX4CKjGAB0T+fDiwkAepQ145nzX0ulv
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

Una clave privada

```
-----BEGIN PGP PRIVATE KEY BLOCK-----  
Version: GnuPG v1.4.10 (GNU/Linux)  
  
mQINBEtUTeQBEACejdGQhscmsDXM7xG2/ZYFpMQg/GmPlJ85uJJUkLr2T+5Rw8Xv  
JeP5F/eRS9G8EE1fObRRW6mRf+bGSelufEMiOi3UB/5P0GBx8iM0QIjezR0R+2n8  
VfZjNZkMwsq94BGFrbXu477tKhQ5wiUBBz/jJ01a39Wrazgp21fvEon2T0Vay45t  
2BYbU4AF815UL6o74Y1W5SLdAofwylZS8pX4CKjGAB0T+fDiwkAepQl45nzX0ulv  
bMjuJmWHTjvEeplnx9iual4J4BT/9FznFs7o4tFVVfYBacFrhWjQyAf2xoP3gyn3  
5O1V55VHVB+oidXUVNSNHZbXwrd1sH42x7x8o17PDFJrWjiq4kAb2EfSOIuSS6na  
K9Y06bqh3yRbVtRdZOuCLcY8QJwt/mx//uQqG6NuSvYhx1QyC6g==XuDES0IuSSa  
  
-----END PGP PRIVATE KEY BLOCK-----
```

Repositorios de claves públicas

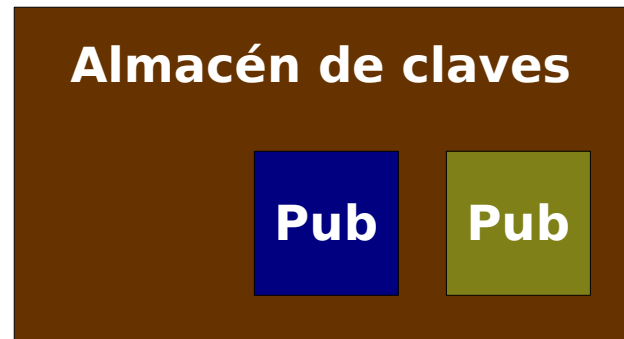
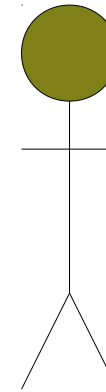
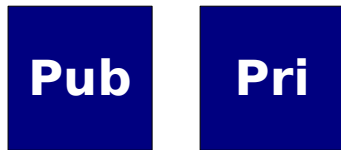
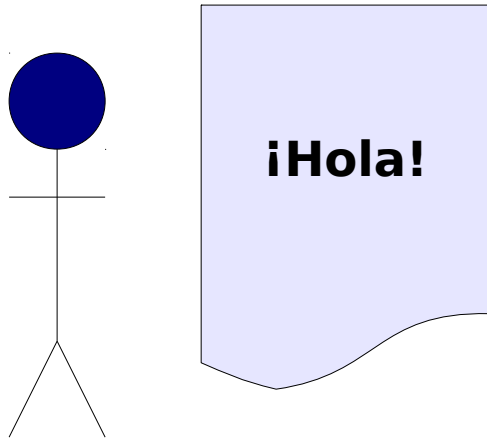
- Servidores en Internet que contienen claves públicas PGP
- Están federados
 - Contienen *todas* las claves públicas del mundo
- En España, hay un servidor público ofrecido por RedIRIS
 - URL: pgp.rediris.es

Ejercicio

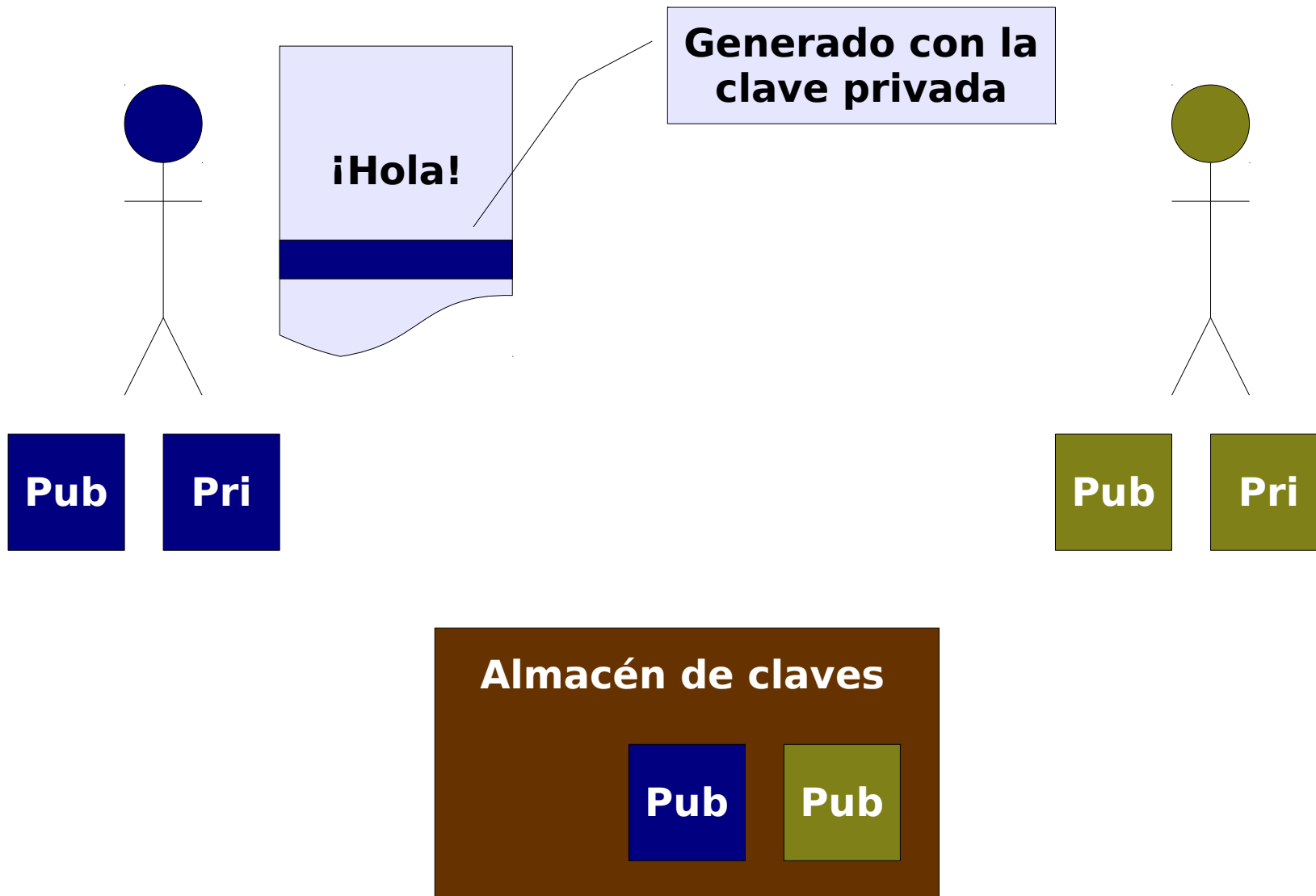
Sube tu clave
a un repositorio
de claves

Baja las claves
de tus compañeros

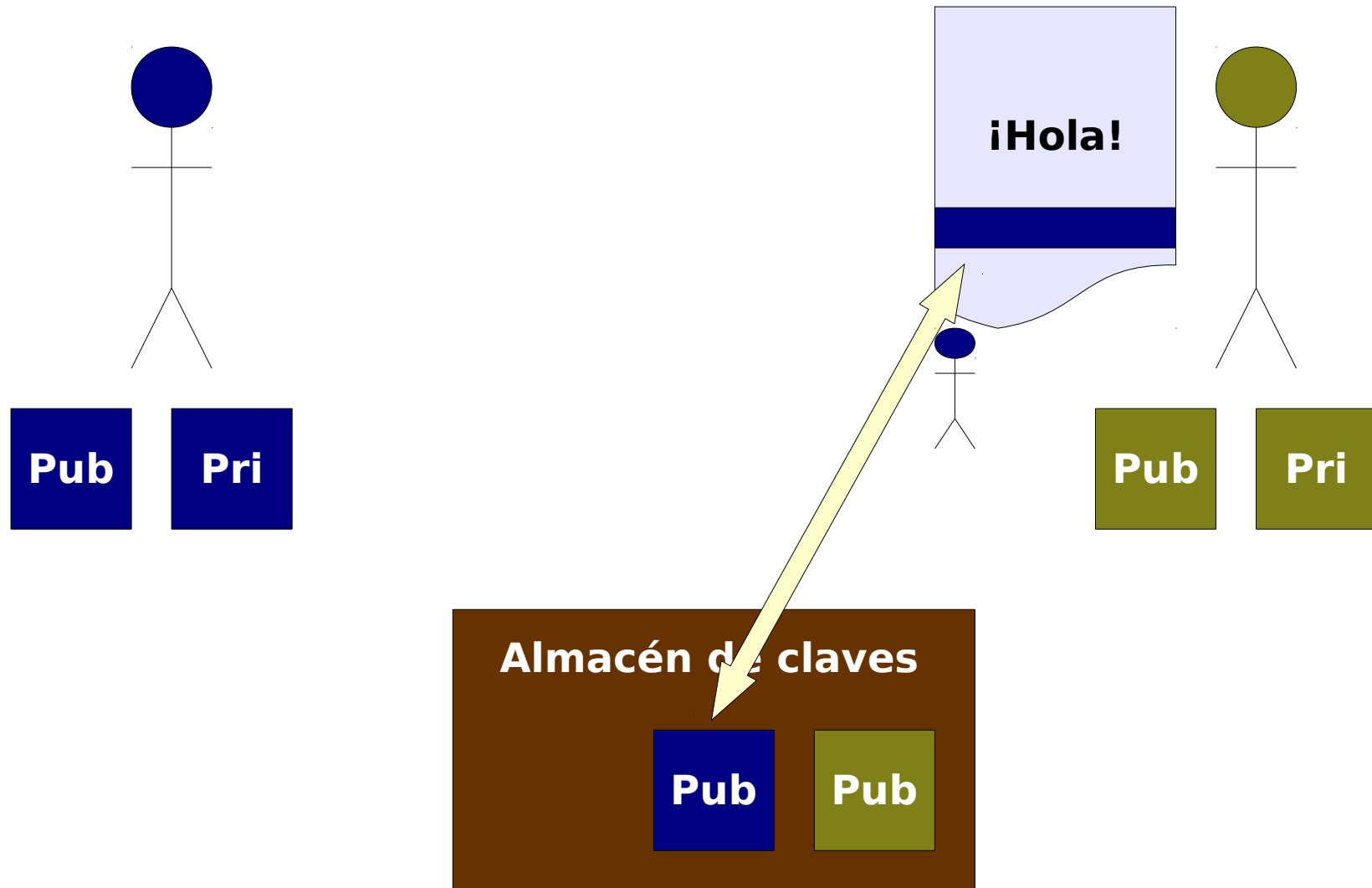
Firmado de documentos



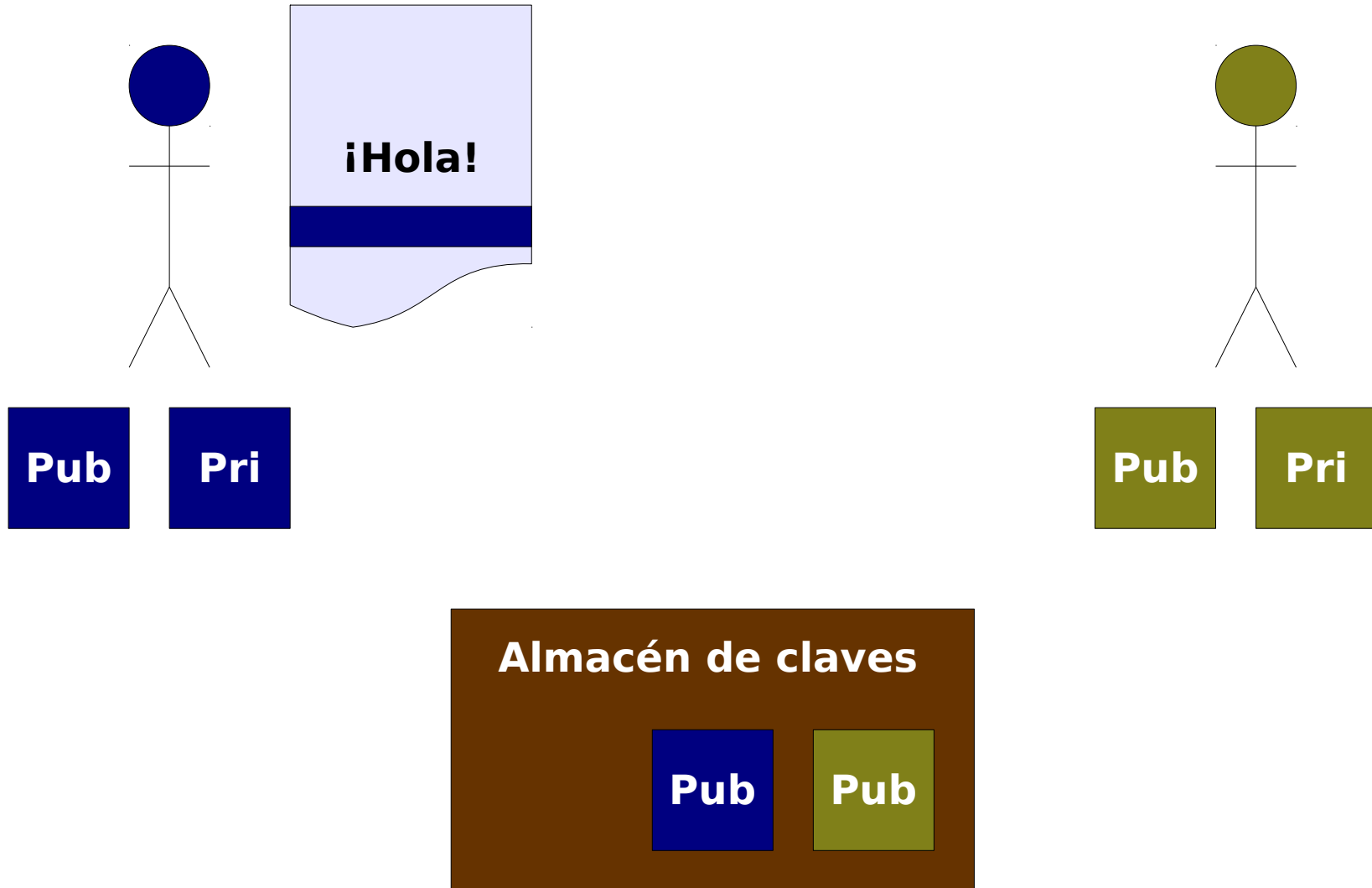
Firmado de documentos



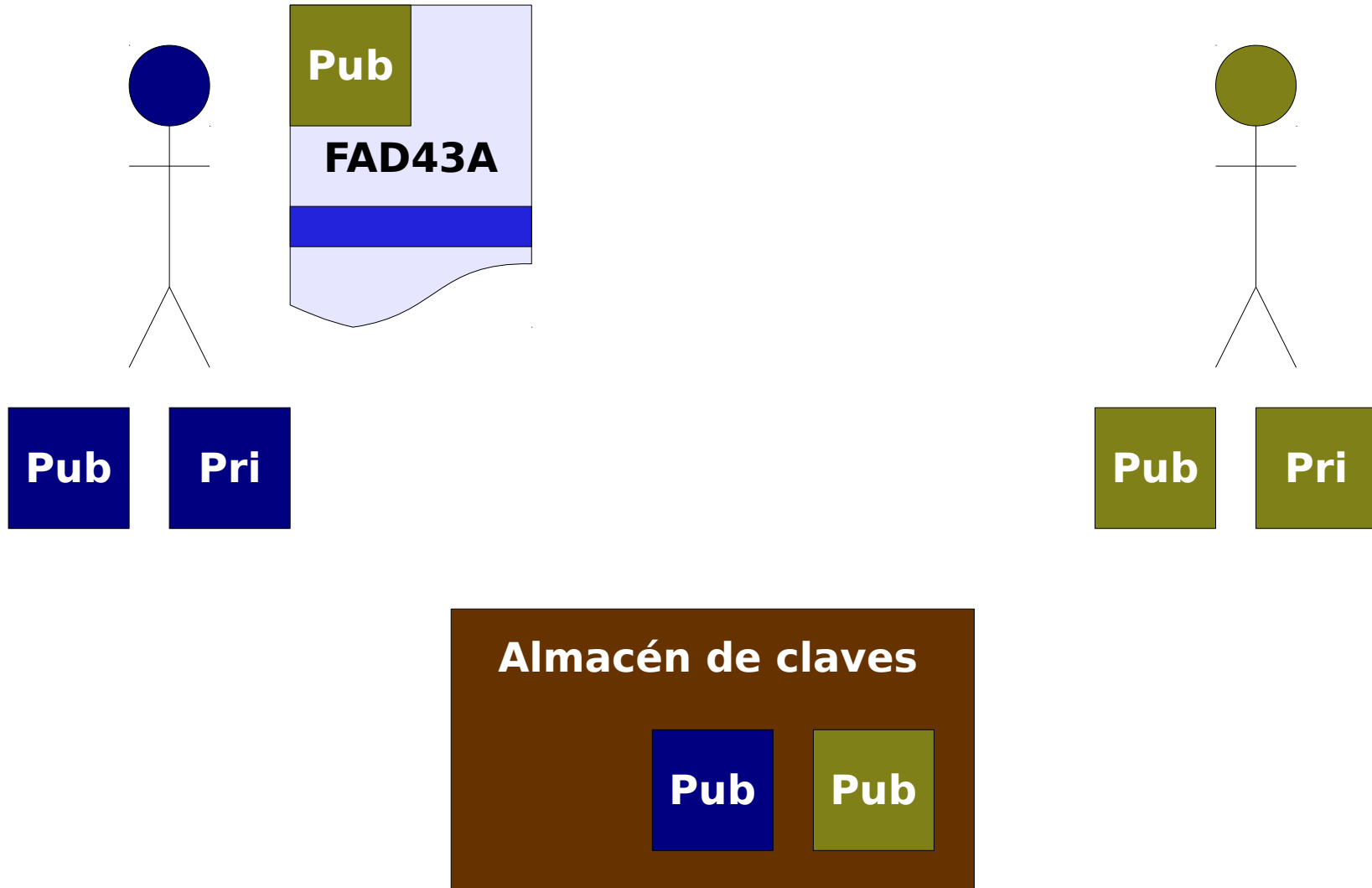
Firmado de documentos



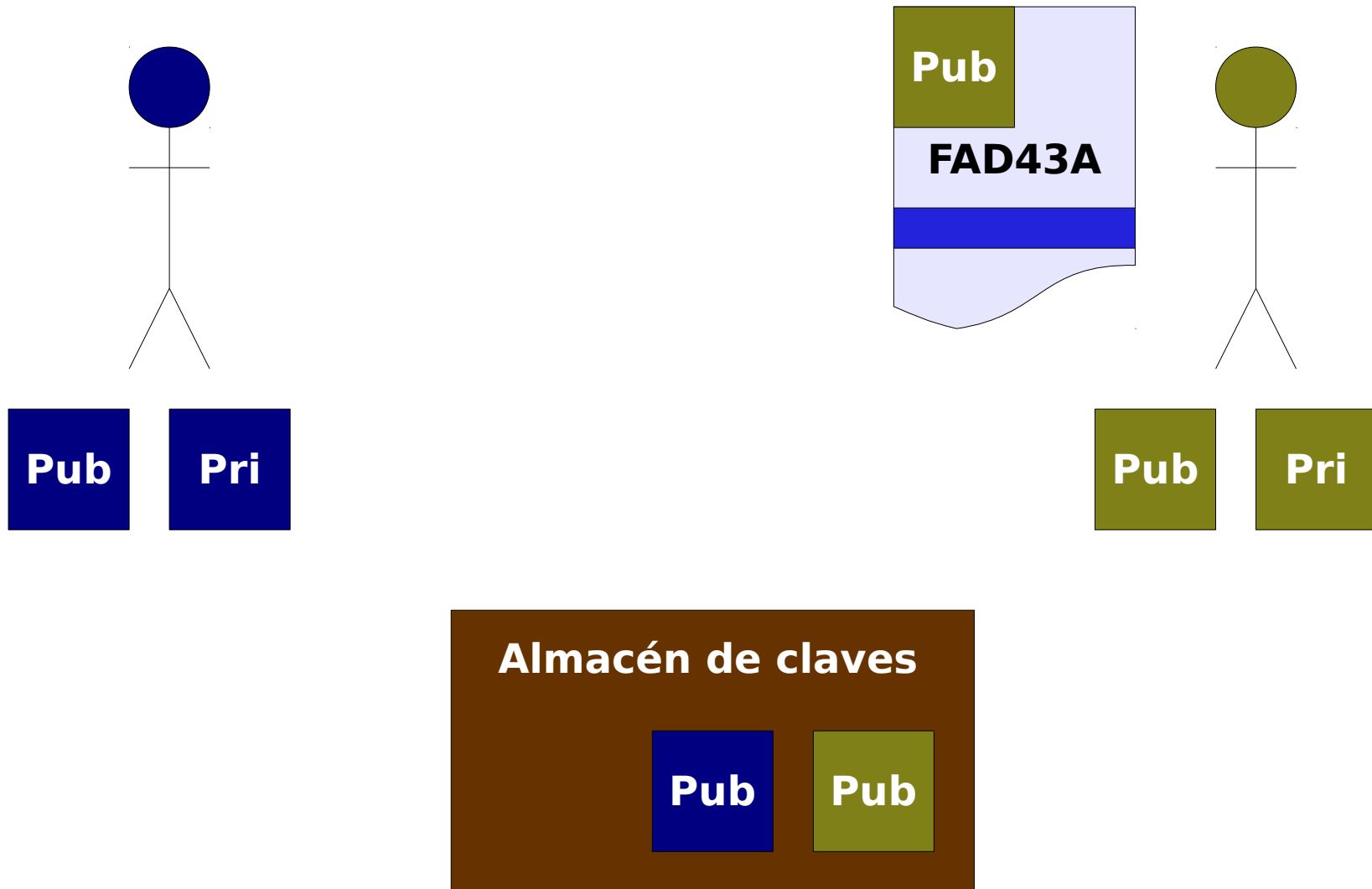
Cifrado y firmado de documentos



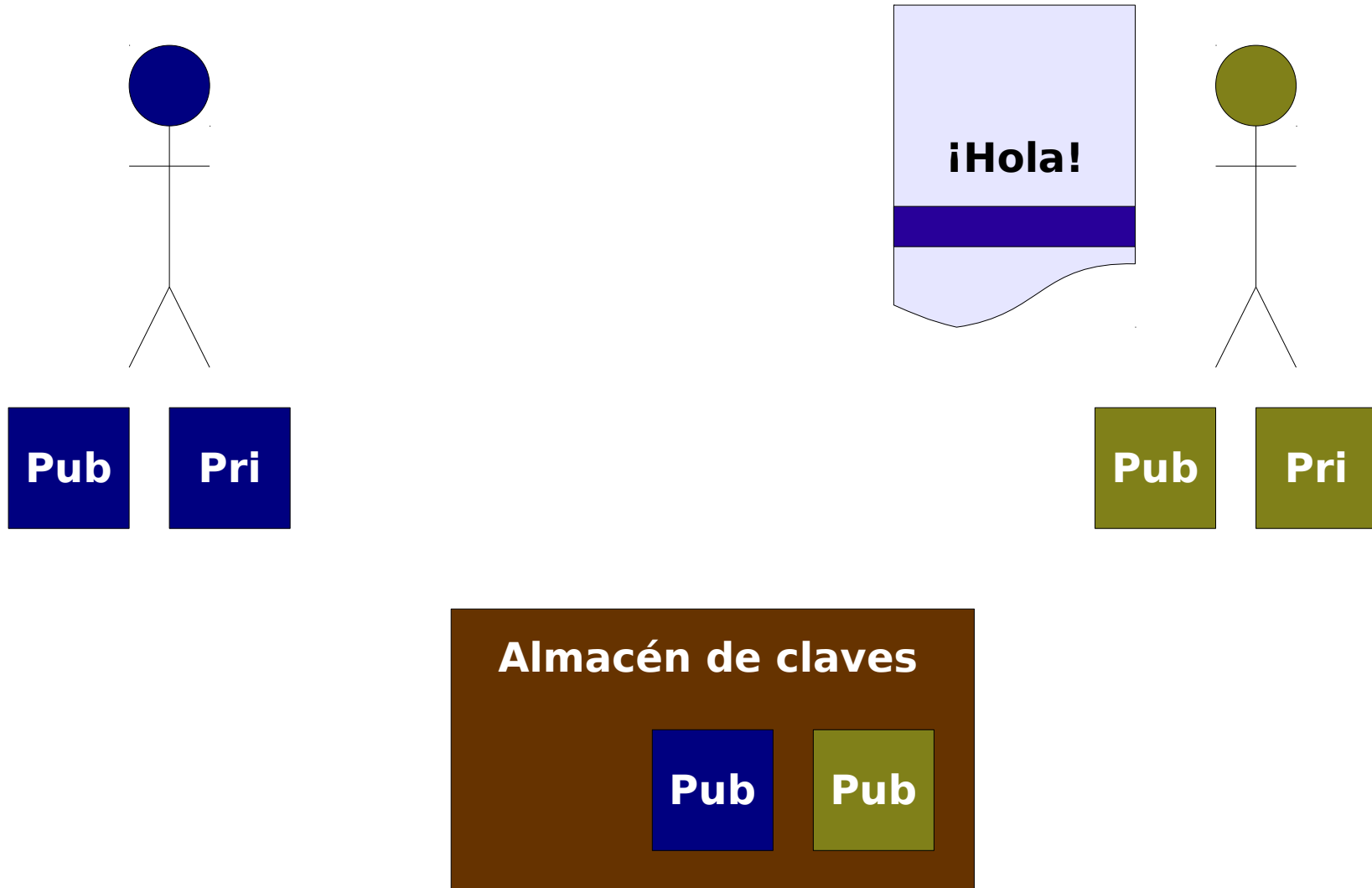
Cifrado y firmado de documentos



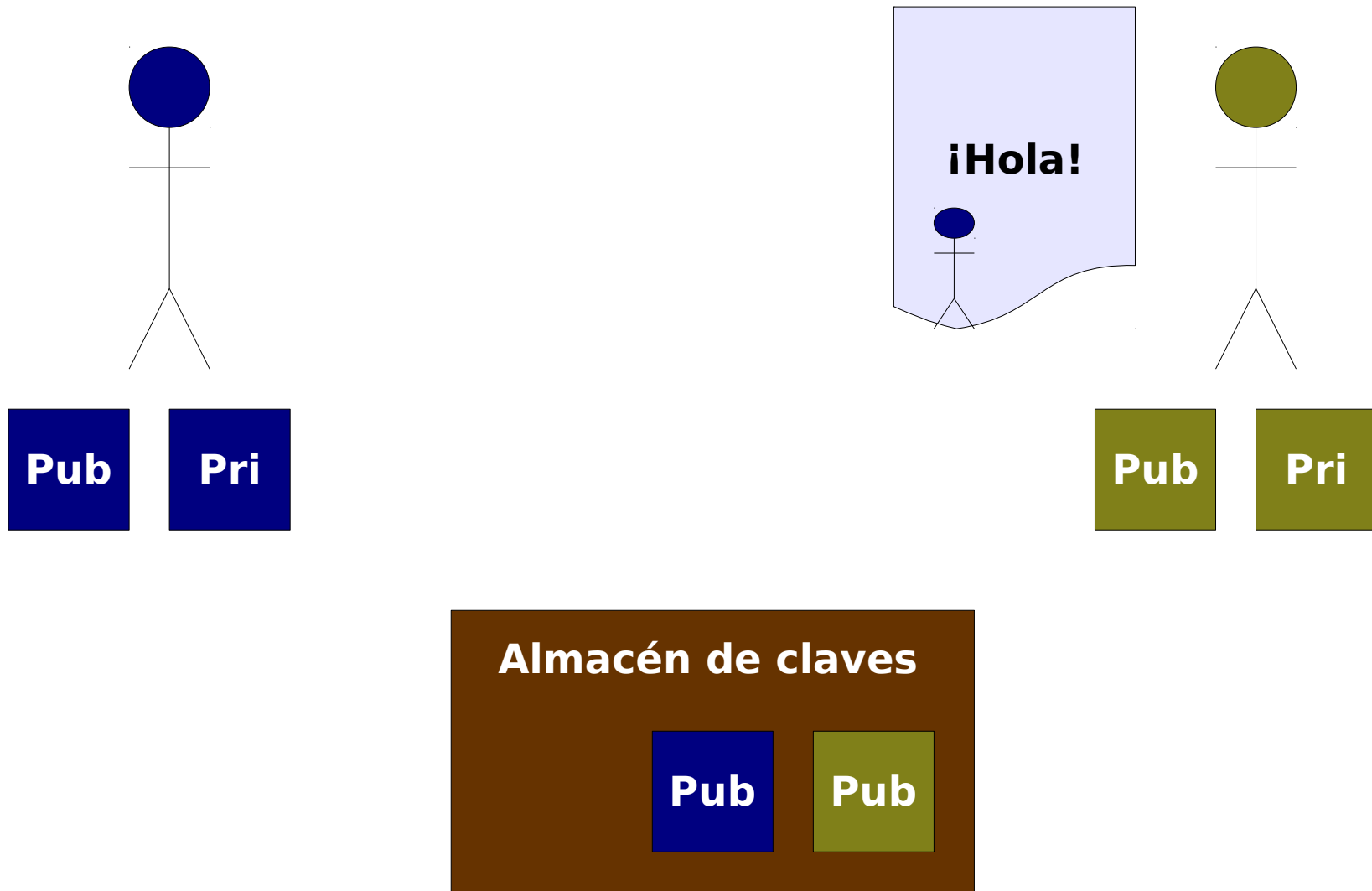
Cifrado y firmado de documentos



Cifrado y firmado de documentos



Cifrado y firmado de documentos



Cifrado y firmado de documentos

- Transmisión segura de información sin necesidad de compartir ningún secreto previo
- Firma de documentos con validez legal
 - No repudio de documentos
- En resumen, lograr en Internet la misma seguridad e intimidad que tenemos con una persona en vivo

Ejercicio

Cifra y firma un texto

Comprueba el texto
y la firma de un
compañero

Certificación de identidades

**¿Cómo sabemos
que las claves públicas
pertenecen a quienes dicen
que son sus dueños?**

**Clave Pública
de
Barack Obama**

**¿Podemos asegurar que la
clave es efectivamente de
Barack Obama?**

Certificación de identidades

**Autoridades de
Certificación**

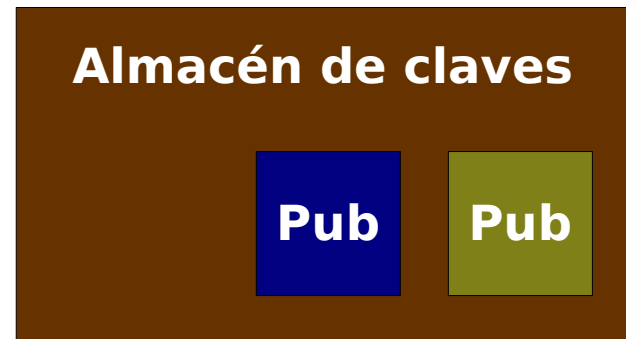
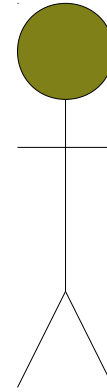
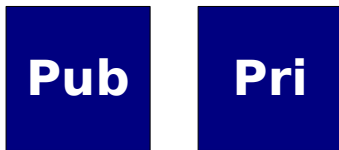
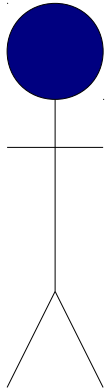
**Cadena de
Confianza**

Firma de claves públicas

- La clave pública es un documento de texto plano que se puede firmar
- La firma mutua de claves públicas con identificación en persona añade la certificación de identidades a la criptografía de clave pública

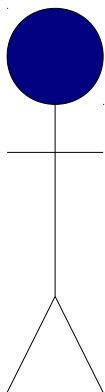
Firma de claves públicas

Barack Obama

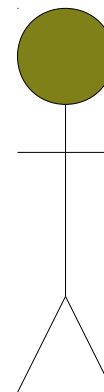


Firma de claves públicas

Barack Obama



Mi clave es FE0A7AF2
Mi nombre es Barack Obama
Mi fingerprint es
D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2



Pub

Pri

Pub

Pri

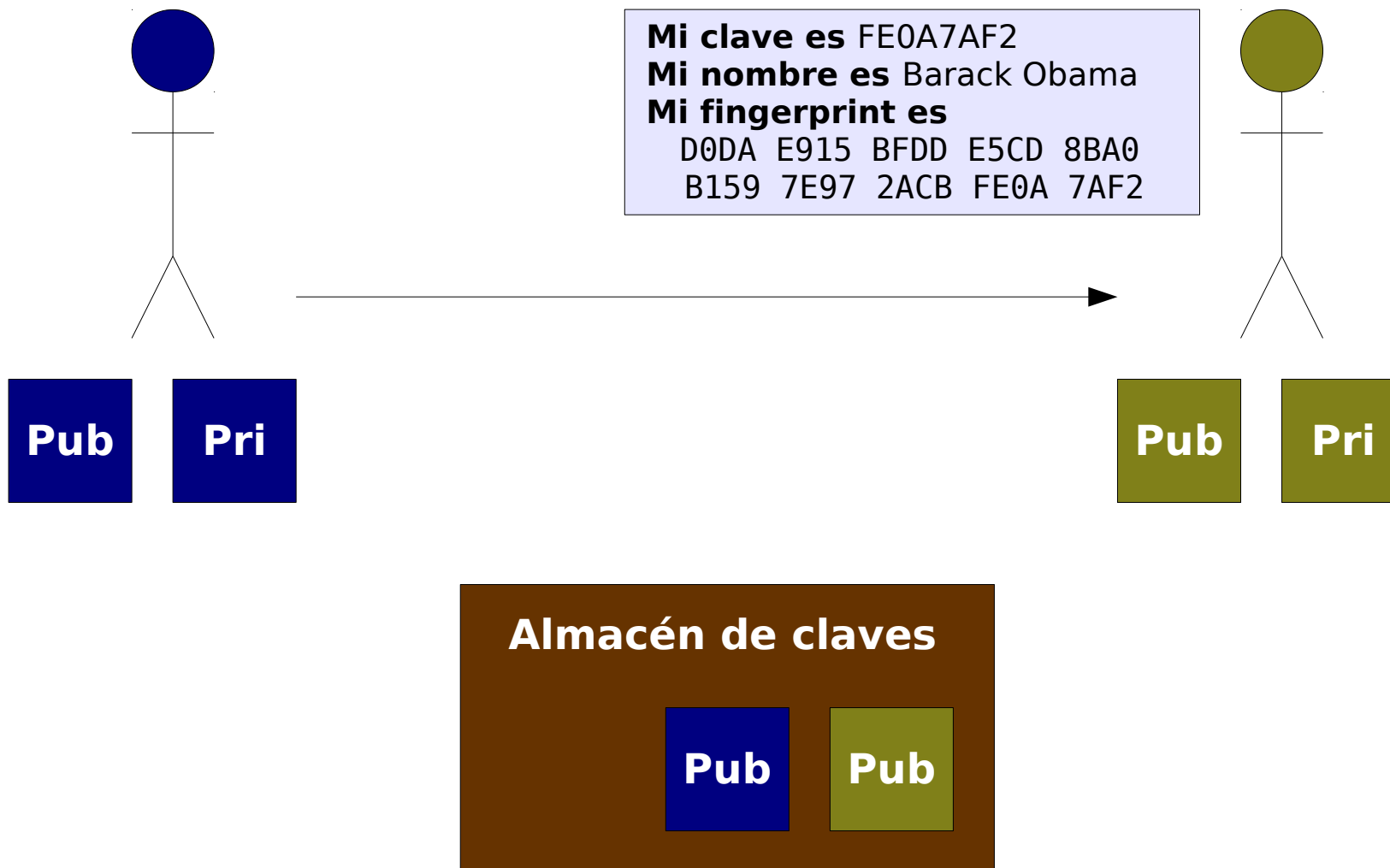
Almacén de claves

Pub

Pub

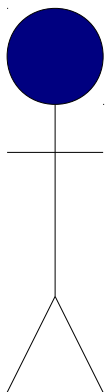
Firma de claves públicas

Barack Obama



Firma de claves públicas

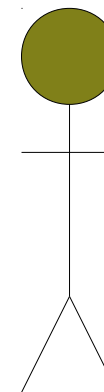
Barack Obama



Pub

Pri

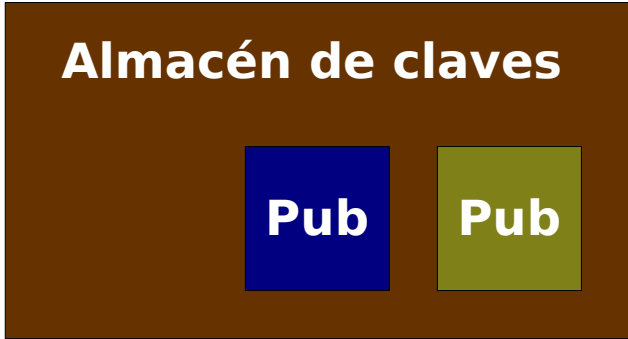
Mi clave es FE0A7AF2
Mi nombre es Barack Obama
Mi fingerprint es
D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2



Déjame tu pasaporte

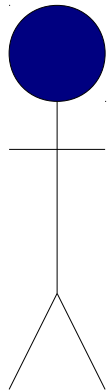
Pub

Pri

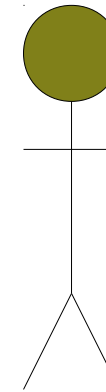


Firma de claves públicas

Barack Obama



Mi clave es FE0A7AF2
Mi nombre es Barack Obama
Mi fingerprint es
D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2



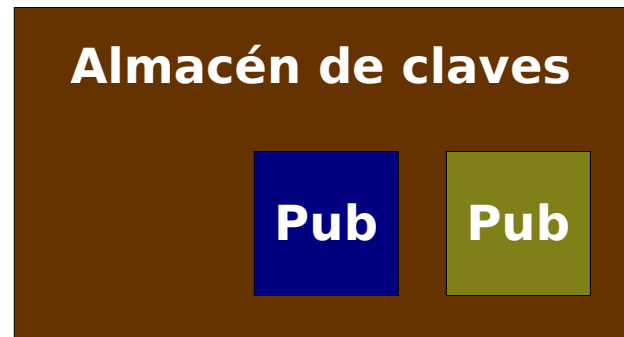
Déjame tu pasaporte

Pub

Pri

Pub

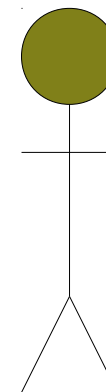
Pri



Firma de claves públicas

Pub
Barack Obama
D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2

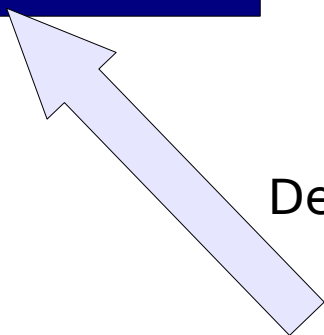
Mi clave es FE0A7AF2
Mi nombre es Barack Obama
Mi fingerprint es
D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2



Pub

Pri

Descarga de FE0A7AF2



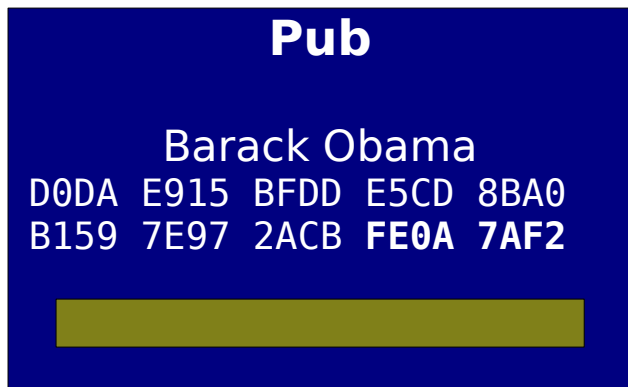
Almacén de claves
Pub **Pub**

Firma de claves públicas

Pub

Barack Obama

D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2

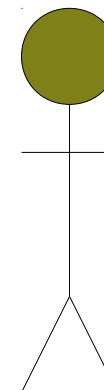
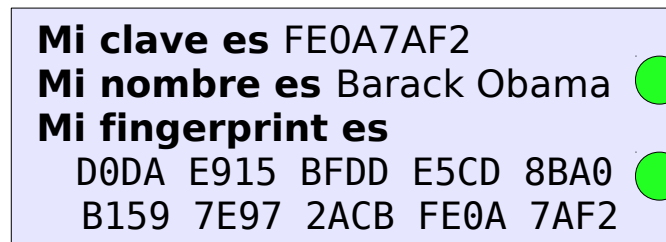


Mi clave es FE0A7AF2

Mi nombre es Barack Obama

Mi fingerprint es

D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2

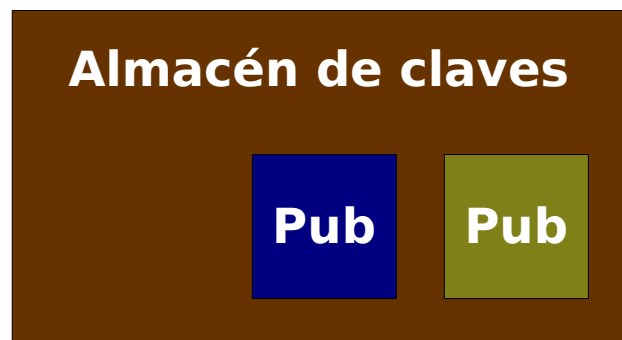


Pub

Pri

Almacén de claves

Pub Pub

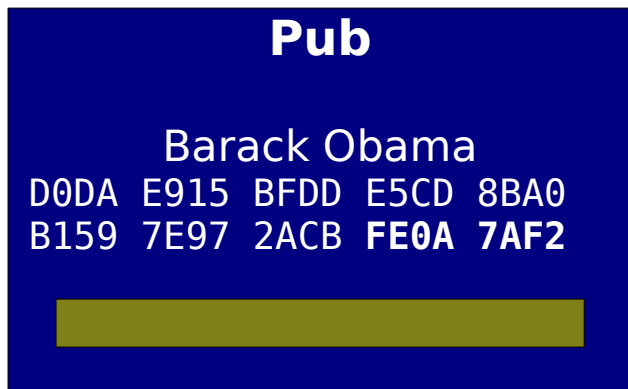


Firma de claves públicas

Pub

Barack Obama

D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2

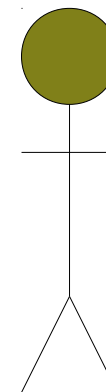
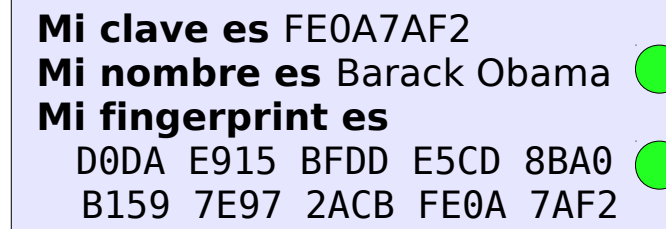


Mi clave es FE0A7AF2

Mi nombre es Barack Obama

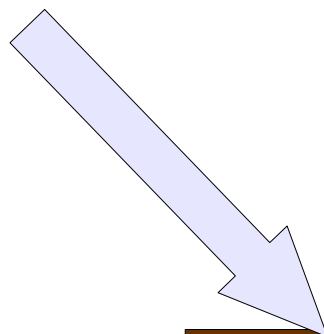
Mi fingerprint es

D0DA E915 BFDD E5CD 8BA0
B159 7E97 2ACB FE0A 7AF2



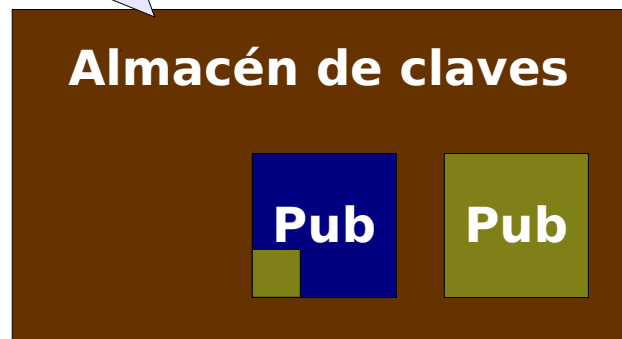
Pub

Pri



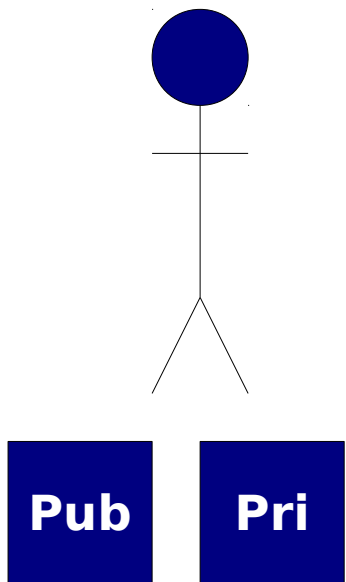
Almacén de claves

Pub **Pub**

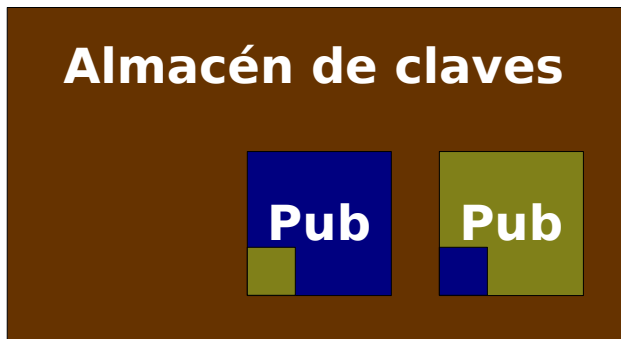
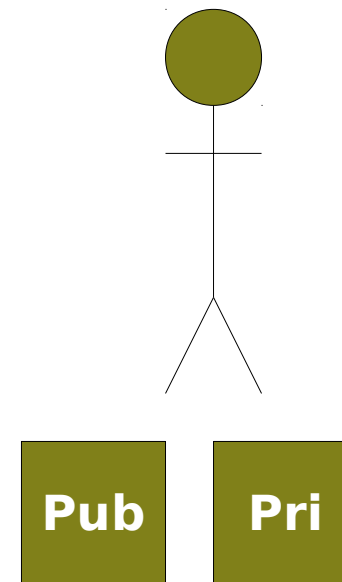


Firma de claves públicas

Barack Obama



La firma de claves suele ser mutua



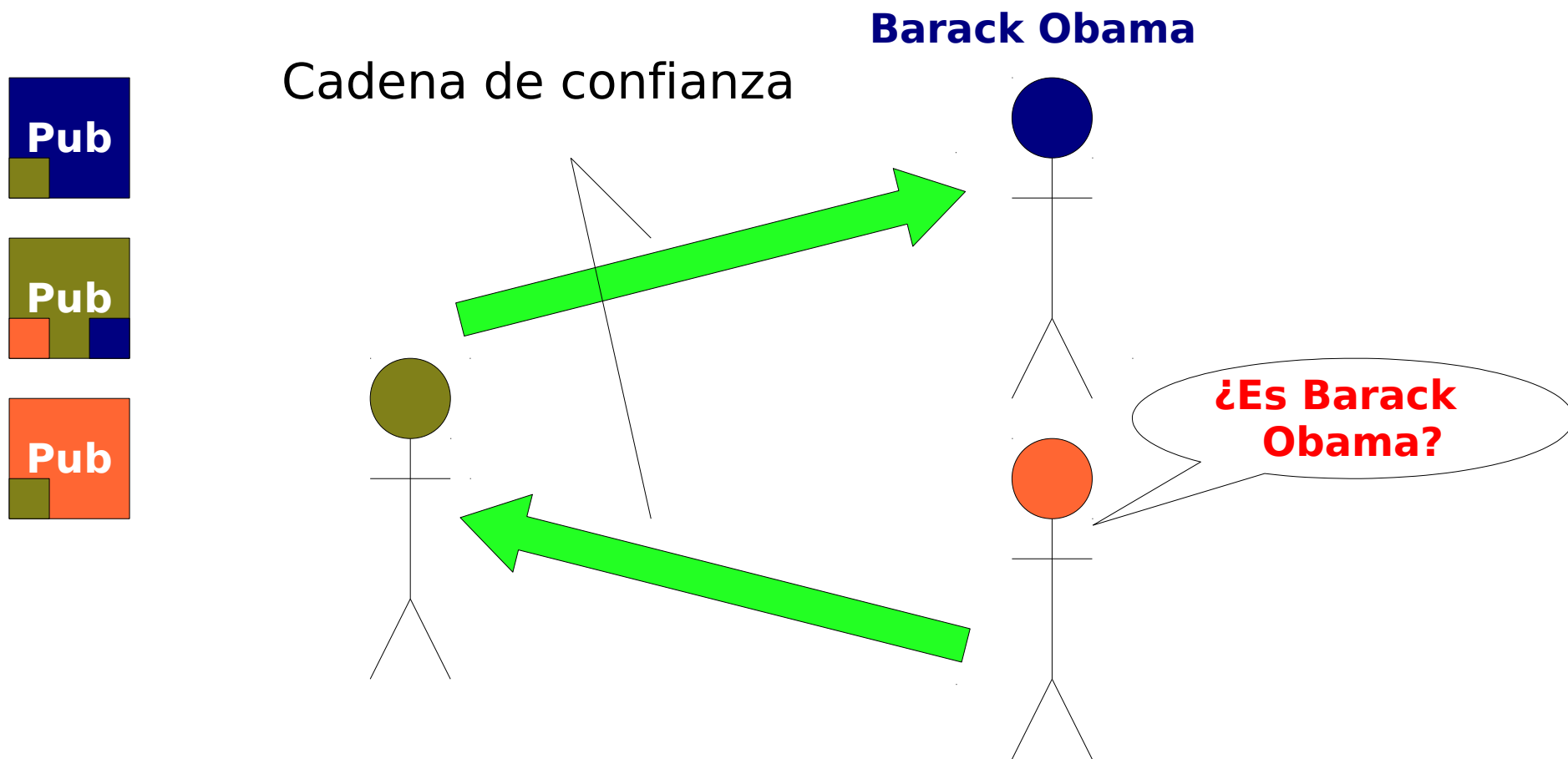
Firma de claves públicas

- Responsabilidad
 - Estás certificando la identidad de una persona



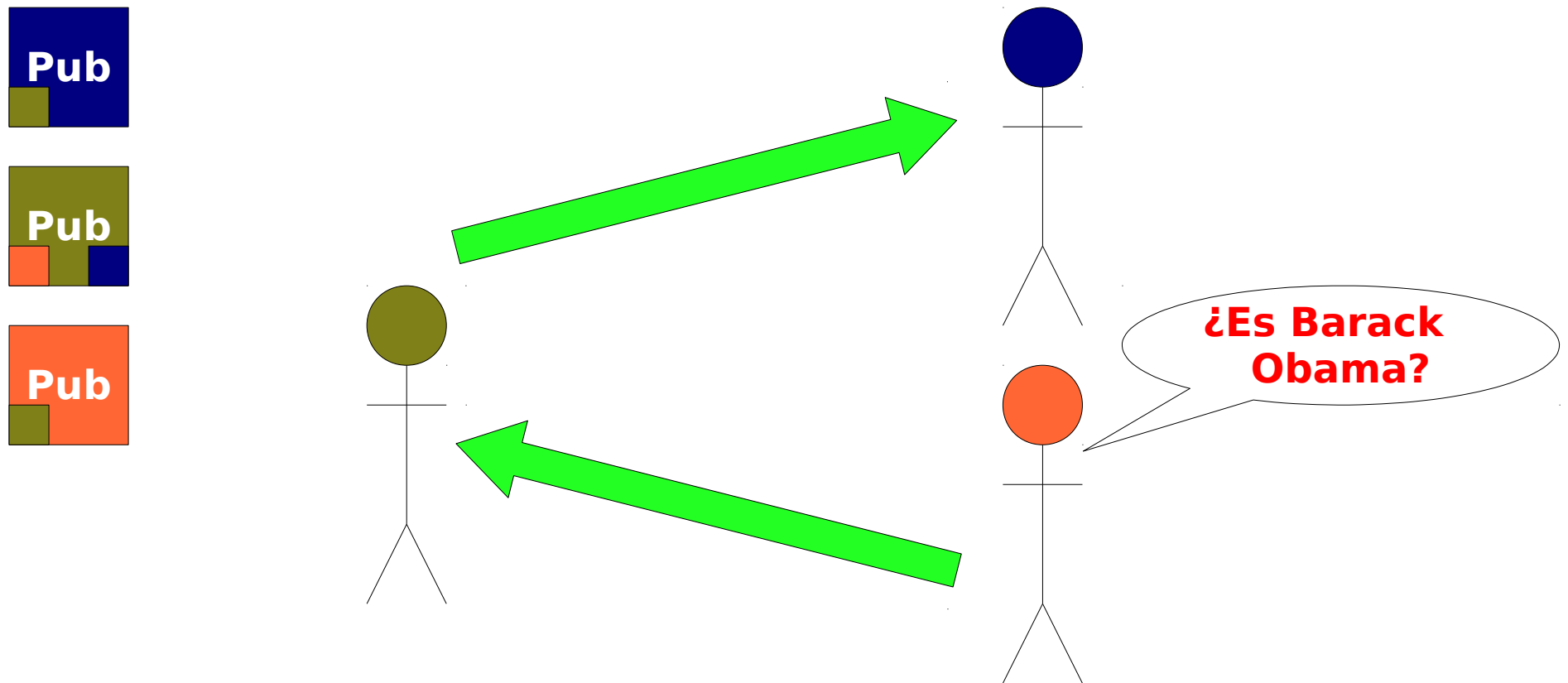
<http://xkcd.com/364/>

Firma de claves públicas



Firma de claves públicas

- La cadena de confianza asegura la identidad de terceros con los que nunca se ha tenido contacto físico



Ejercicio

Comprueba la
identidad de un
compañero

Firma y sube su
clave pública