

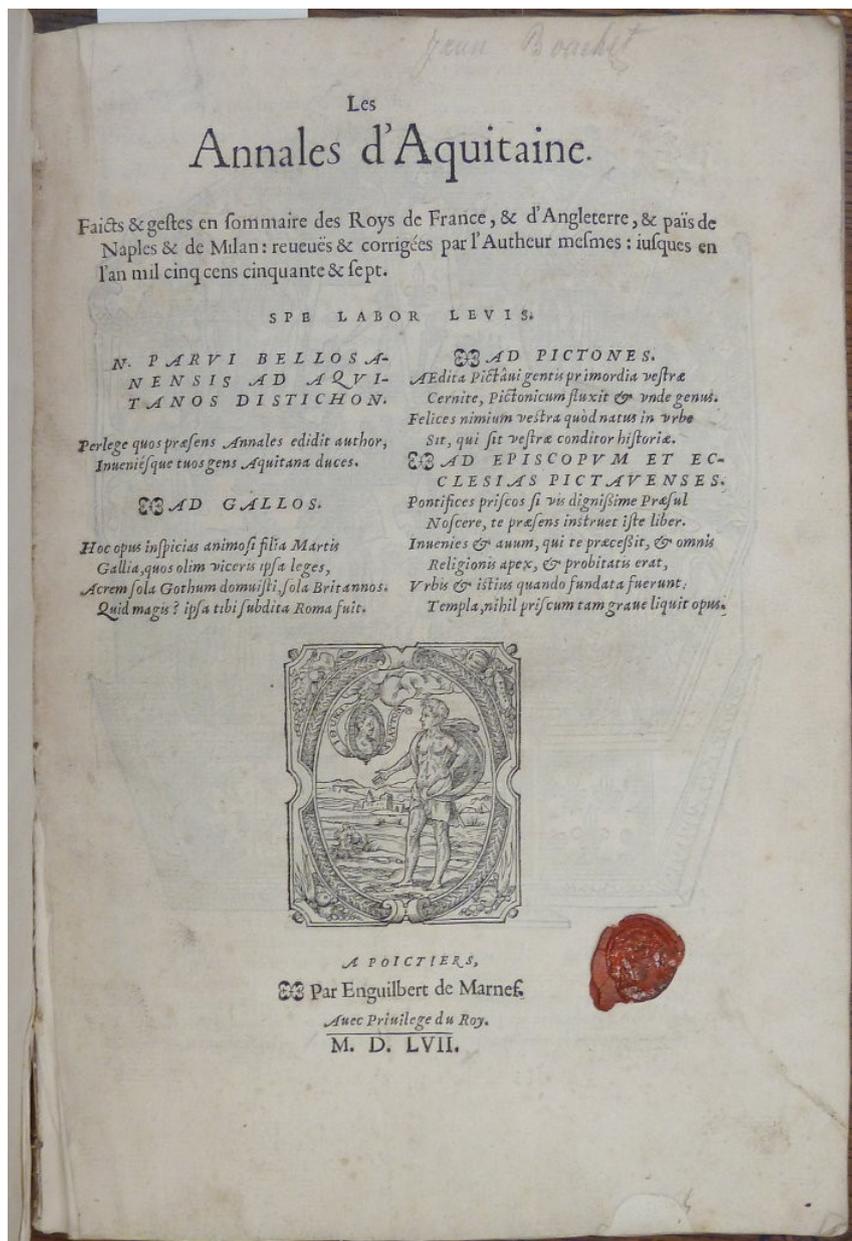
Firma electrónica

para principiantes

el cuentito matemático, conceptos, ejemplos,
uso cotidiano de la firma (electrónica)

Daniel Viñar Ulriksen
dvinar@csic.edu.uy
daniel@uruguayos.fr

La firma y el sello



- La firma identifica a una persona, la compromete con el documento, a una fecha
- El sello autentica, además de la firma a una persona que posee algo difícil de imitar



La firma y el sello - 2



- El sello puede otorgar autoría, autenticidad, integridad, confidencialidad, no divulgación
- En este caso, la no divulgación depende del respeto no violento del sello

Necesidad de ocultar el mensaje

- No divulgación:
necesidad de
“encriptación”



Escítala



Máquina criptográfica
franacesa, Henri II, Siglo XVI

Máquinas criptográficas

Enigma



Lorenz Cipher



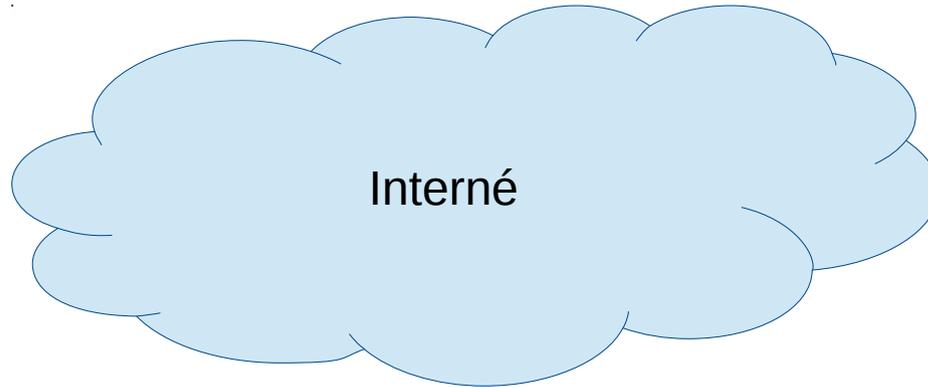
Red
Máquina japonesa



Encriptado (o cifrado) simétrico



Pepe

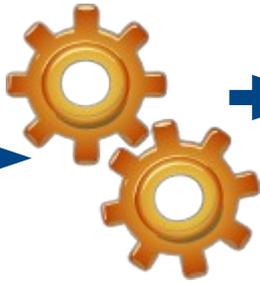


Interné

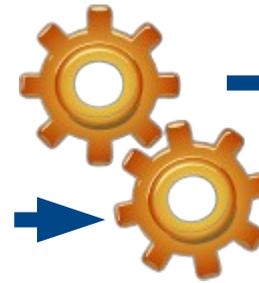


Lucía

Las
zanahorias
están
cocidas



VkIDSU9TIEVMRUNUU
k9OSUNPUzEdMBsGA1
UEAwwUQ29ycmVvIFVy
dWd1YXlvc0gQ0ECEH
BwiKirx5klUd8AAmumr+
gwDQYJKoZlhvcNAQEB
BQAEggEAKRUKCqFGy
pj60VEvDSy0UzNhExnt



Las
zanahorias
están
cocidas



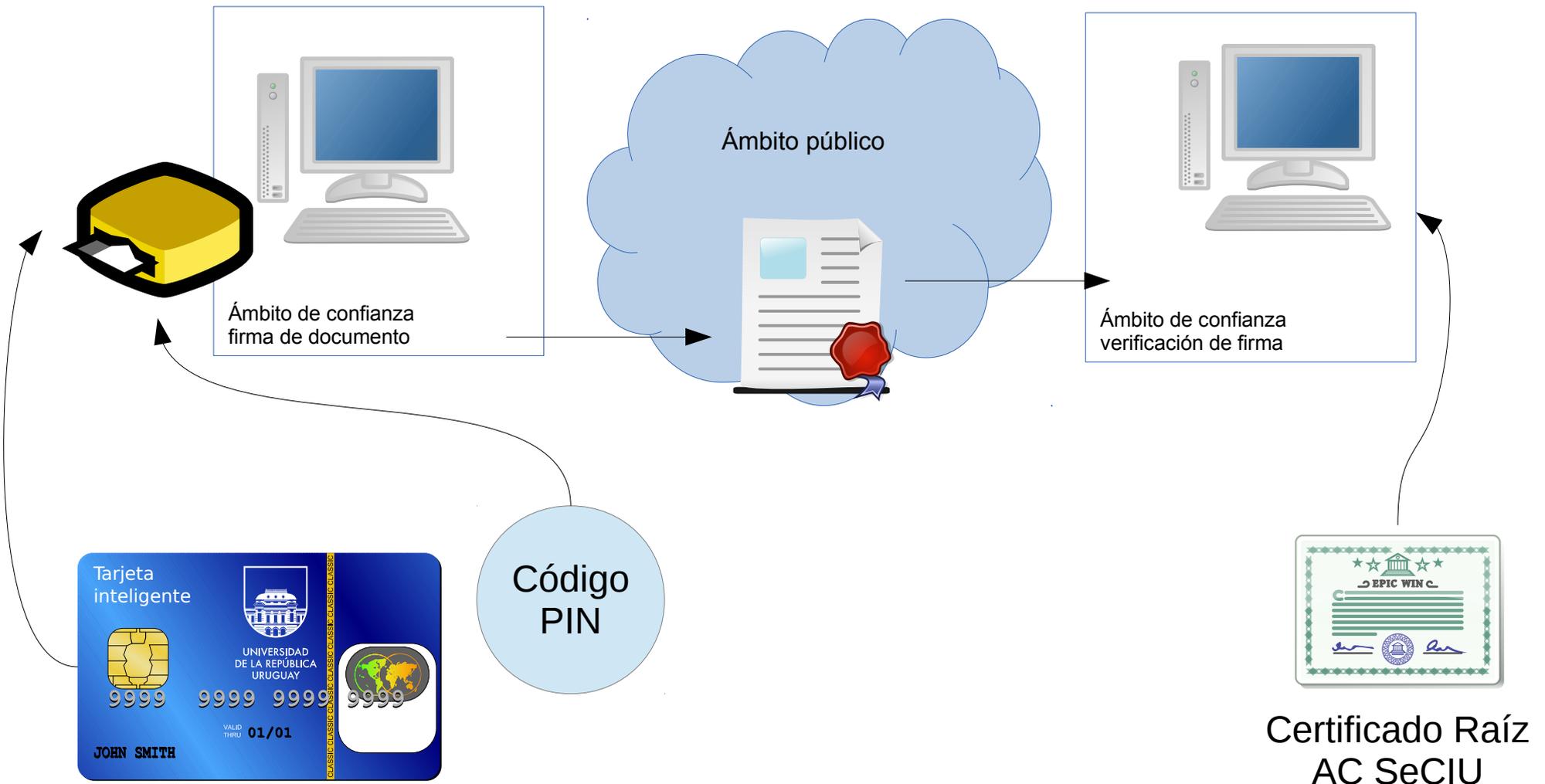
Clave secreta compartida

Evolución de la legislación

- El encriptado es considerado arma de guerra
- Fue prerrogativa de los estados durante la segunda mitad del siglo XX
- El internet se convirtió en una “red de redes”, que enruta y transporta información, pero insegura
- En los 2000, se liberó el encriptado para permitir el comercio electrónico por internet

Integridad de los certificados

Confidencialidad de la clave



Mensaje firmado

Esto es una prueba de mensaje firmado - Icedove

Archivo Editar Ver Ir Mensaje Herramientas Ayuda

Recibir mensajes Redactar Chat Direcciones Etiquetar

Responder Reenviar Archivar Basura Borrar

De Daniel Viñar Ulriksen

Asunto **Esto es una prueba de mensaje firmado** 17:48

A Daniel Viñar Ulriksen

Otras acciones

Este mensaje está firmado.

--
Daniel Viñar Ulriksen
CCI

1 mensaje borrado de Papelera 98%

- Ver -> Fuente del Mensaje: datos de la firma (diapositiva siguiente)

El mensaje está firmado

Este mensaje incluye una firma digital válida. El mensaje no ha sido manipulado desde que se envió.

Firmado por: DANIEL VIÑAR ULRIKSEN
Dirección de correo: dvinar@cci.edu.uy
Certificado emitido por: Correo Uruguayo - CA

[Ver certificado de firma](#)

El mensaje no está cifrado

Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.

[Aceptar](#)

General Detalles

El certificado ha sido verificado para los usos siguientes:

- Certificado del firmante del correo
- Certificado de correo del destinatario

Expedido a

Nombre Común (CN)	DANIEL VIÑAR ULRIKSEN
Organización (O)	<No forma parte del certificado>
Unidad Organizacional (OU)	<No forma parte del certificado>
Número de serie	70:70:88:A8:AB:C7:99:25:51:DF:00:02:6B:A6:AF:E8

Expedido por

Nombre Común (CN)	Correo Uruguayo - CA
Organización (O)	ADMINISTRACION NACIONAL DE CORREOS
Unidad Organizacional (OU)	SERVICIOS ELECTRONICOS

Validez

Expedido el	11/07/13
Expira el	11/07/14

Huella digital

Huella SHA-1	FC:B1:E2:22:8F:24:3E:1A:42:BB:57:68:2B:CB:2B:97:ED:7F:71:5C
Huella MD5	00:C8:62:39:56:FA:7D:D3:BE:09:A1:5A:A8:CA:54:3D

Contenido de un mensaje firmado

Date: Sun, 28 Jul 2013 17:48:38 -0300
From: =?ISO-8859-1?Q?Daniel_Vi=F1ar_Ulriksen?= <dvinar@cci.edu.uy>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20130704 Icedove/17.0.7
MIME-Version: 1.0
To: =?ISO-8859-1?Q?Daniel_Vi=F1ar_Ulriksen?= <dvinar@csic.edu.uy>
Subject: Esto es una prueba de mensaje firmado
Content-Type: multipart/signed; protocol="application/pkcs7-signature"; micalg=sha1;
boundary="-----ms020307020103070104030007"

Este es un mensaje firmado criptográficamente en formato MIME.

-----ms020307020103070104030007
Content-Type: text/plain; charset=ISO-8859-1; format=flowed
Content-Transfer-Encoding: quoted-printable

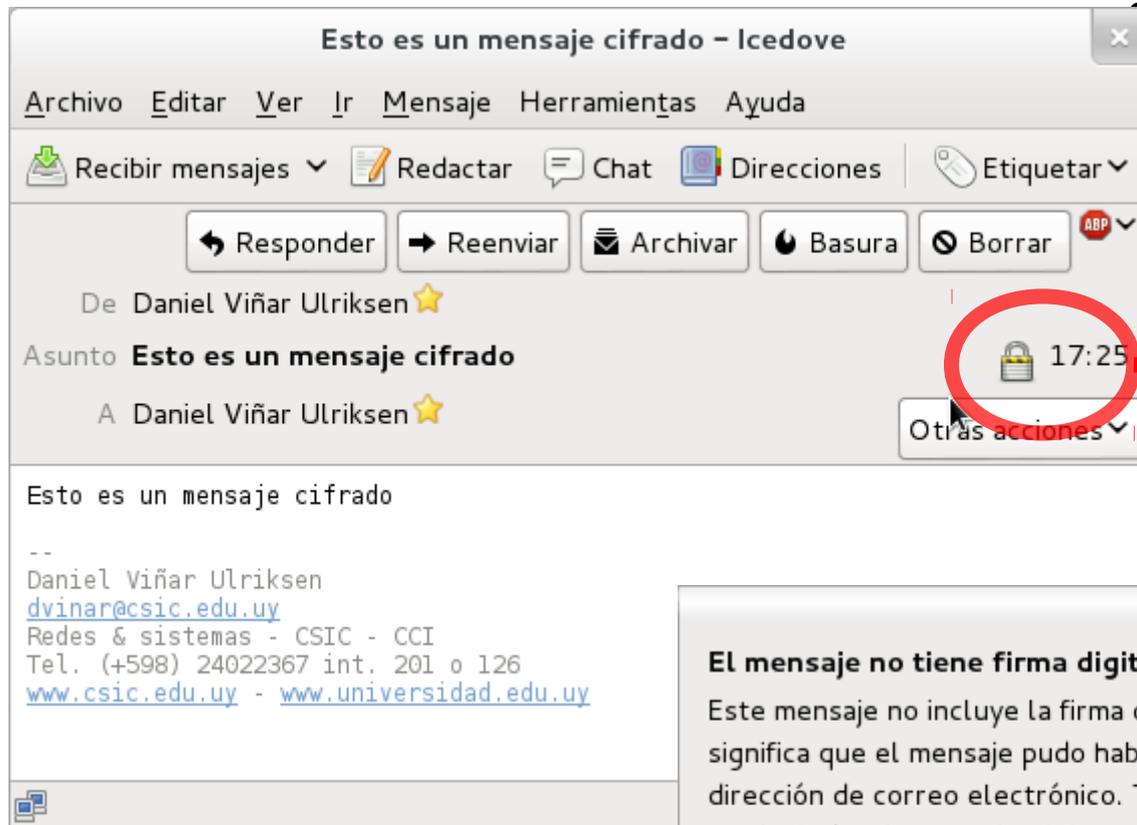
Este mensaje está firmado.

--=20
Daniel Vi=F1ar Ulriksen
CCI

-----ms020307020103070104030007
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: Firma criptográfica S/MIME

MIAGCSqGSIb3DQEHAQCAMIACAQExCzAJBgUrDgMCGGUAMIAGCSqGSIb3DQEHAQAoIIMUDCC
BcwggO0oAMCAQICEHBwiKirx5kIUd8AAmumr+gwDQYJKoZIhvcNAQEFBQAwEjELMAkGA1UE
BhMCMCVVxkZApBgNVBAoMIkFETUIOSVNUUkFDSU90IE5BQ0IPTkFMIERFIENPUIJFT1MxHzAd
(...)
1IXCsU3n4eMXB8WG0V+aZzzAW+5TMmynGNAIOKNR/pxhrYn5yQCLQx5De61B9hSAmkMzDNYq
J88+cmRnyhbF8ejyS++dHToetup5vyv9UjntSPUy/1+E3keh6XKBVUxL2uYofEL8uKTa4HoG
uGEg7Kr3hjCooVWUuWOZ+mMhdAVnAAAAAAA
-----ms020307020103070104030007--

Ver un mensaje decifrado en thunderbird



Ver -> Fuente del Mensaje: datos encriptados (diapositiva siguiente)

El mensaje no tiene firma digital

Este mensaje no incluye la firma digital del remitente. La ausencia de una firma digital significa que el mensaje pudo haber sido enviado por alguien que finge tener esta dirección de correo electrónico. También es posible que el mensaje haya sido manipulado mientras circulaba por la red. Sin embargo, es poco probable que haya ocurrido alguna de estas posibilidades.

El mensaje está cifrado

Este mensaje fue cifrado antes de ser enviado. El cifrado hace muy difícil que otras personas puedan ver información mientras ésta viaja por la red.

Aceptar

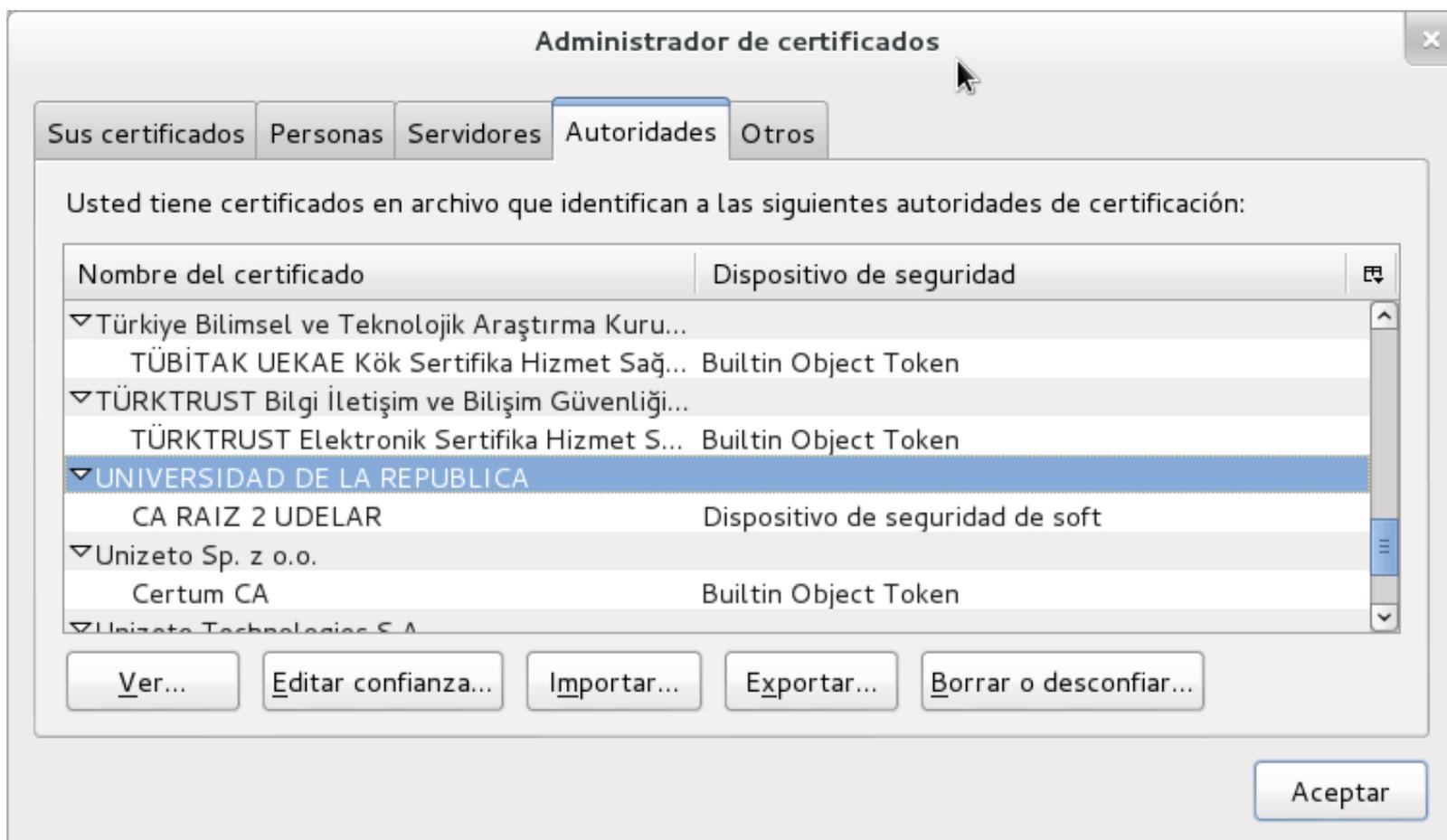
Un verdadero mensaje encriptado

Message-ID: <51F57E2B.4090700@csic.edu.uy>
Date: Sun, 28 Jul 2013 17:25:15 -0300
From: =?ISO-8859-1?Q?Daniel_Vi=F1ar_Ulriksen?= <dvinar@csic.edu.uy>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:17.0) Gecko/20130704 Icedove/17.0.7
MIME-Version: 1.0
To: =?ISO-8859-1?Q?Daniel_Vi=F1ar_Ulriksen?= <dvinar@cci.edu.uy>
Subject: Esto es un mensaje cifrado
Content-Type: application/pkcs7-mime; name="smime.p7m"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7m"
Content-Description: Mensaje cifrado S/MIME

MIAGCSqGSIb3DQEHA6CAMIACAQAxggGrMIIBpwIBADCBjjB6MQswCQYDVQQGEwJVWTErMCKG
A1UECgwiQURNSU5JU1RSQUJ04gTkFDSU9OQUwgREUgQ09SUkVPUzEfMB0GA1UECwwWU0VS
VklDSU9TIEVMRUNUUK9OSUNPUzEdMBsGA1UEAwwUQ29ycmVvIFVydWd1YXlvc0gQ0ECEHBw
iKirx5klUd8AAumr+gwDQYJKoZIhvcNAQEBBQAEggEAKRUKCqFGypj60VEvDSy0UzNhExnt
9c3JF6yqvh+uWjFLf6XZ3BLM1lk3C1cfWlISEBXvbBz18ADQe0MPICG82OIAxaqInWLDUleW
VHIEts0Ot90qWS0HcvflwN5rKgfHEJ8y7UqBEQu8+tBBSG2Lr7eb1hhKfTcUZVW08HRwgjyh
3FYrjPUyycamj2MDOMfu+W+yf/qjwca+jG0UZbkDPuaNa/euNTEaRy9QXQ18VSXc019dnp5v
wbBRL2EE6hmQ4KIJK6iVDrPnW3xeKcGUkRwj050vdykvsdY18UFjk7WDA/n7WNSjkd2IFc+7
iFEDddrczFmSBJPfE1JmE2KMUTCABgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECKjljT/B+wtU
oIAEggEwpwM+XiTT8Q+/rugOOIZ4cSKgGVEGViiuhHfd7A3CeLZwMxM6+R2cyadjNjCMRSHr
HqLE6OV5kqmuCKfTu2U+df7DCW7I9HTIkxbYdJIXEfPepZNwnAk7o1LRCp22p7zjzsyJcRs
FmNYUj50nQgWkxIRcc10o8R7XigkzTWvZxXupoJamaxh22p33kMQFLDYpvgRku7iB8kFDdXm
0lmcHILsv2/PylYoJUA/5V8LNklsSkVwTXEUgNyw6megJg6ZoAzrrTe4pQtQcxCID0VCD5xK
WmgheqsShHobSeAxj2+27OG1mE5L3Tsyw2ZQSW68luSmR0asPHrb4k8w0PU9twXVhFY+xCdK
qxCAcsw5bVxHVeeEPFFR5IXc+hHErO1/j4S5Urw5lhQ/csEYiycA7wQIYLioRiKbqHkAAAAA
AAAAAAAA

Certificado raíz de SeCIU

Conviene obtener el certificado de una fuente segura y verificar su huella



Huella SHA1 del Certificado Raíz de SeCIU

05 E9 C9 B7 5F 42 BF DB AC 27 29 9E 4D F2 7F F6 DC 2B A2 0B

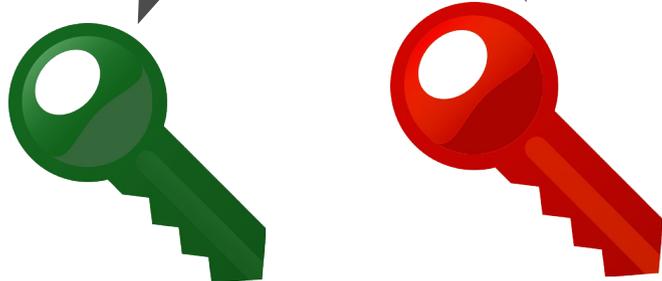
criptografía asimétrica



Jim

Número aleatorio
elevado

Algoritmo de
generación de clave



Clave pública

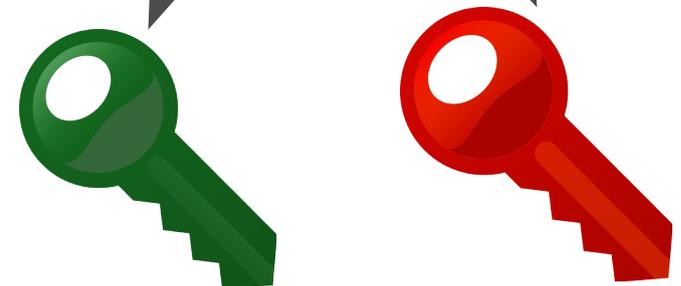
Clave privada



Andy

Número aleatorio
elevado

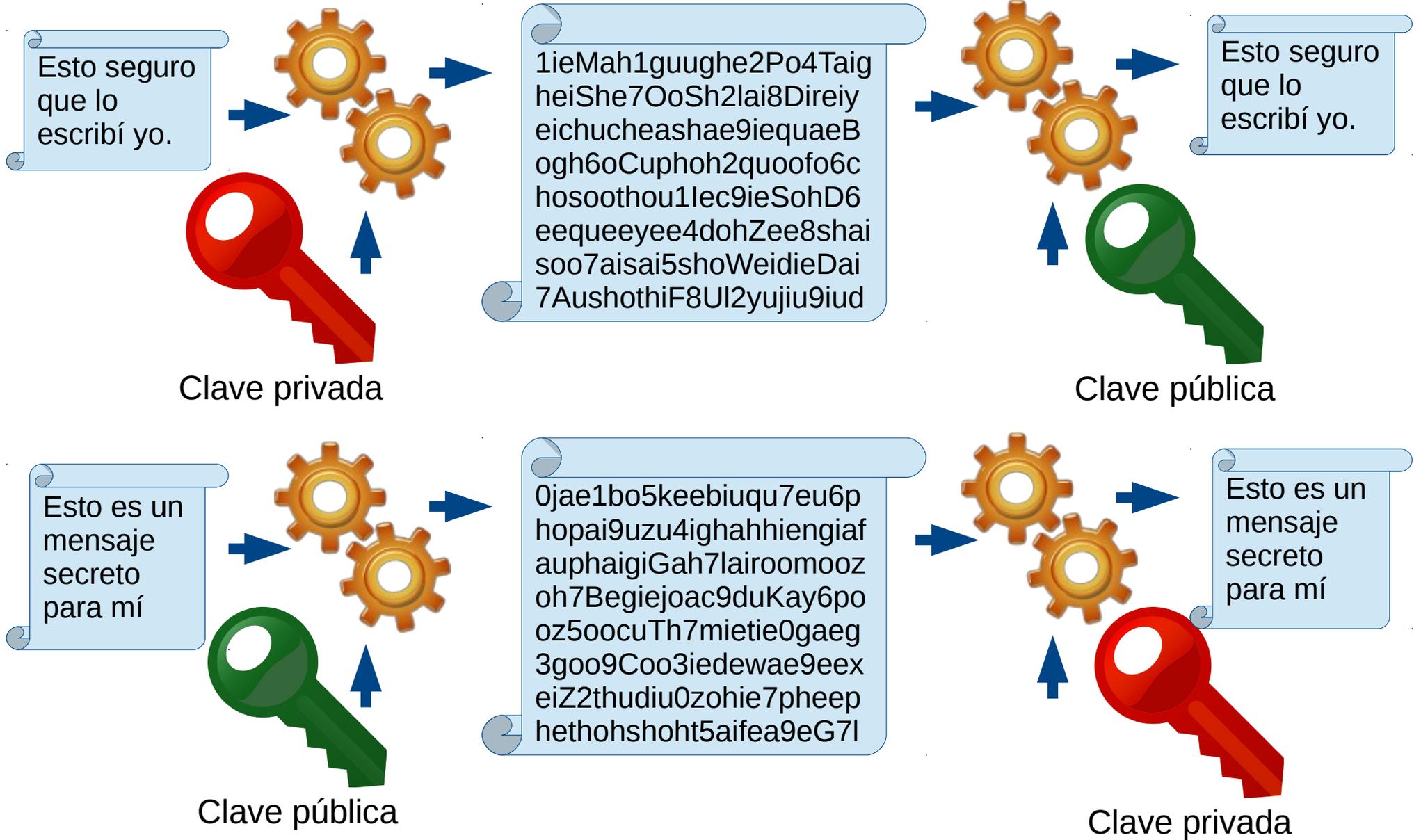
Algoritmo de
generación de clave



Clave pública

Clave privada

Asocioación asimétrica de las claves



Una herramienta matemática: el hashtag: da la integridad

Un amigo es aquel que te da la libertad de ser tú mismo. Soy el Rey Lagarto, puedo hacer lo que sea. Los espectadores de cine son vampiros callados. El amor no puede salvarte de tu propio destino. Quien controla los medios de comunicación, controla las mentes. Creo un largo y prolongado y ordenado transtorno de los sentidos hasta llegar a obtener lo desconocido. De hecho, no recuerdo haber nacido, debió haber ocurrido durante una de mis borracheras.

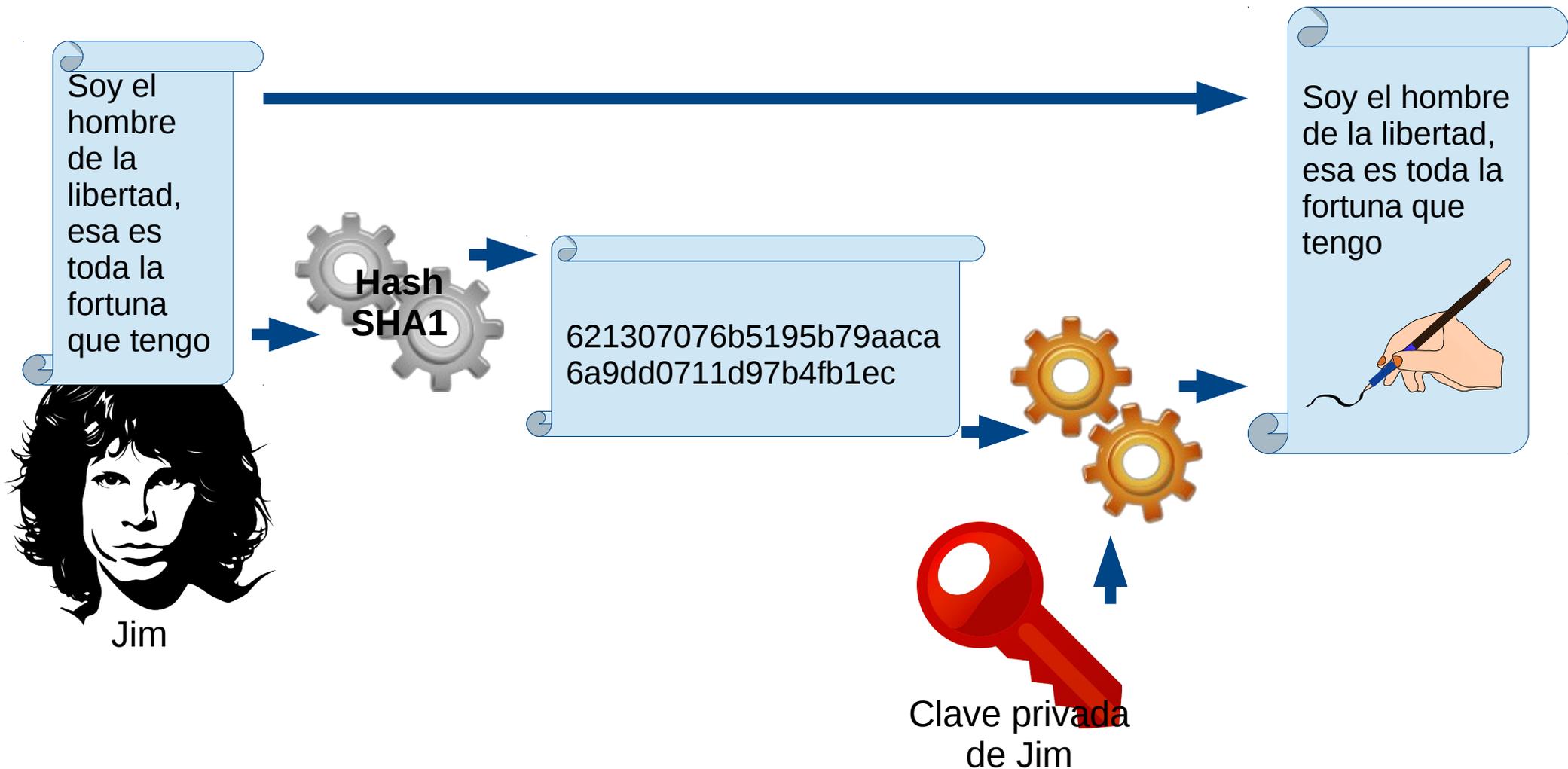


67c41270a1e91f494894b54d
26f62814535ed9a3 jim.txt

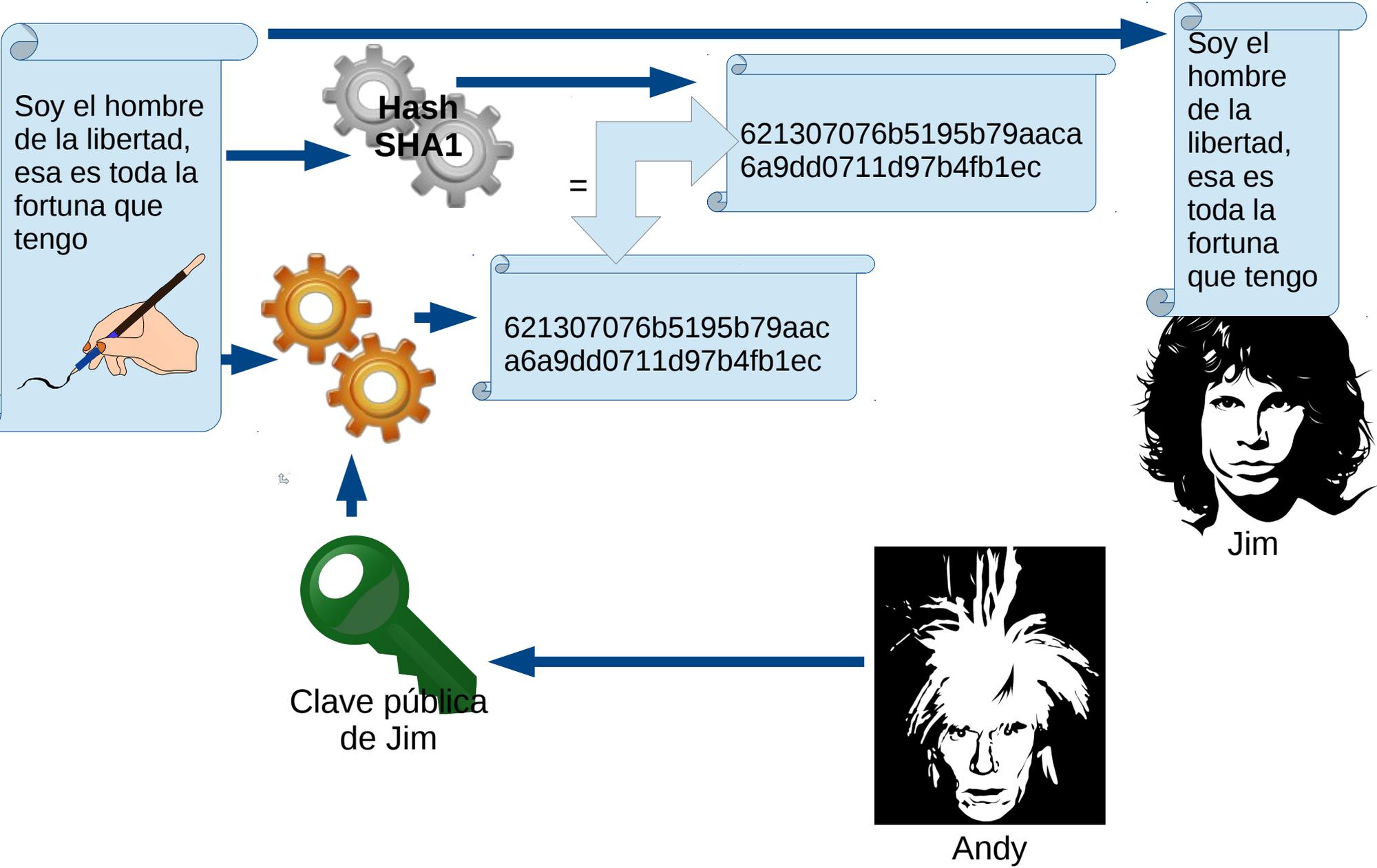


Otro mensaje arbitrario

Jim firma



Andy reconoce la firma de Jim



Jim le escribe un mensaje confidencial a Andy

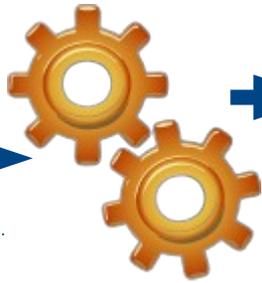
Hay cosas conocidas y cosas desconocidas, y en el medio están The Doors...



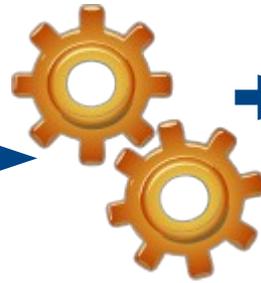
Jim



Clave pública de Andy



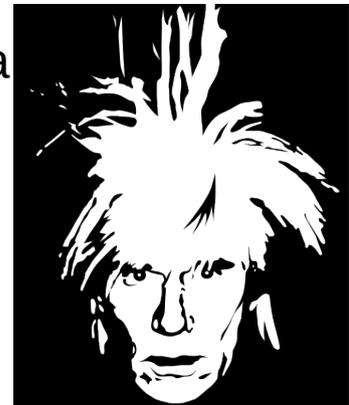
ite8ieweishi6Zaa2jaic5gu
xae2AhNoh0pieph1ahhai
shie0thaephoe8laup8ote
eshi3eeGequieghibahbei
Queiz1eishu1upohneiw0
iepeixie5ouMep7waj5ina
7eikai9quaikutieCh1Xep
9Joo2huT5phiyeiyeesa5



Hay cosas conocidas y cosas desconocidas, y en el medio están The Doors...

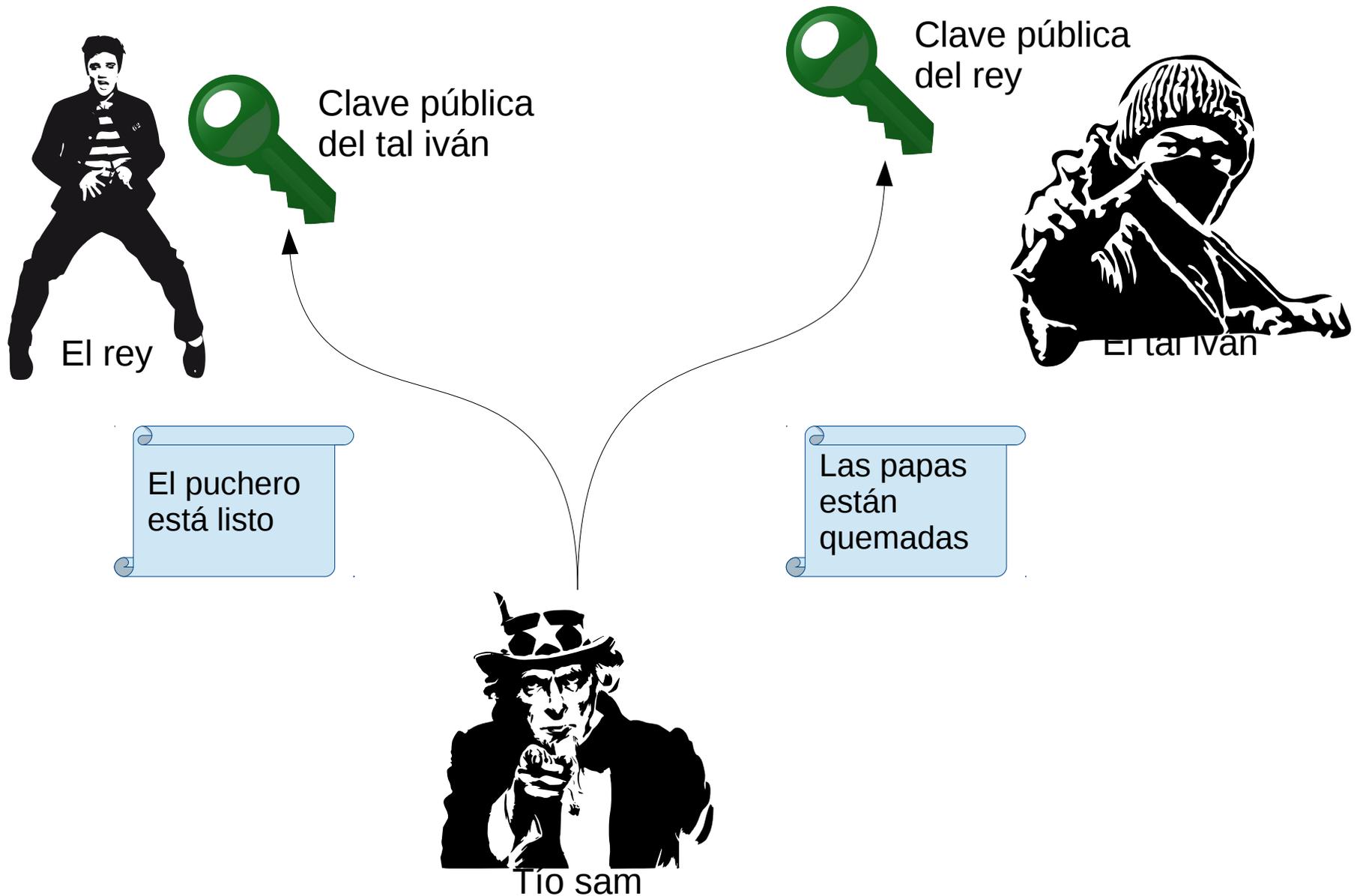


Clave privada de Andy

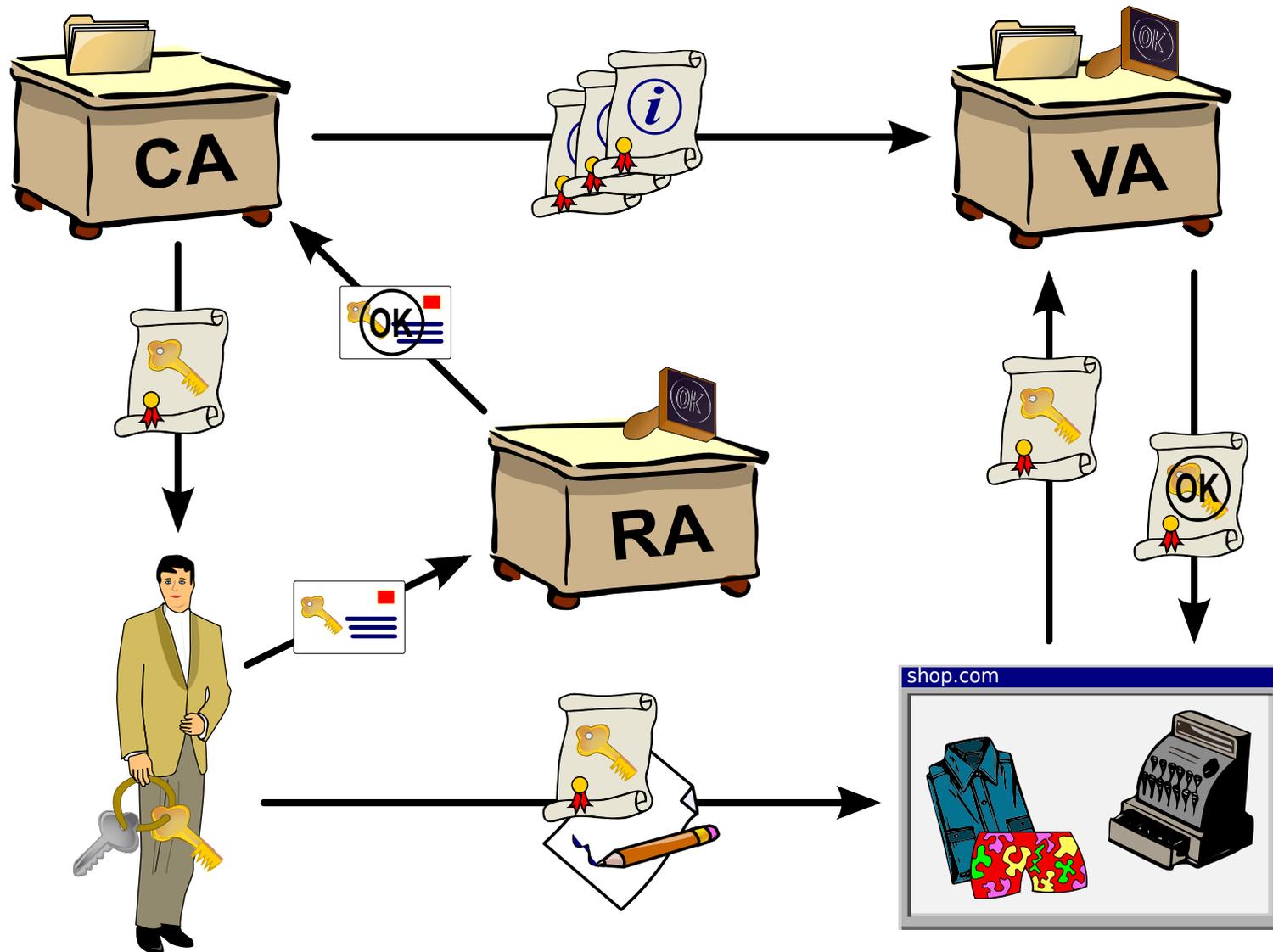


Andy

El problema del *hombre en el medio*



La infraestructura de clave pública



Infraestructura de clave pública (PKI)