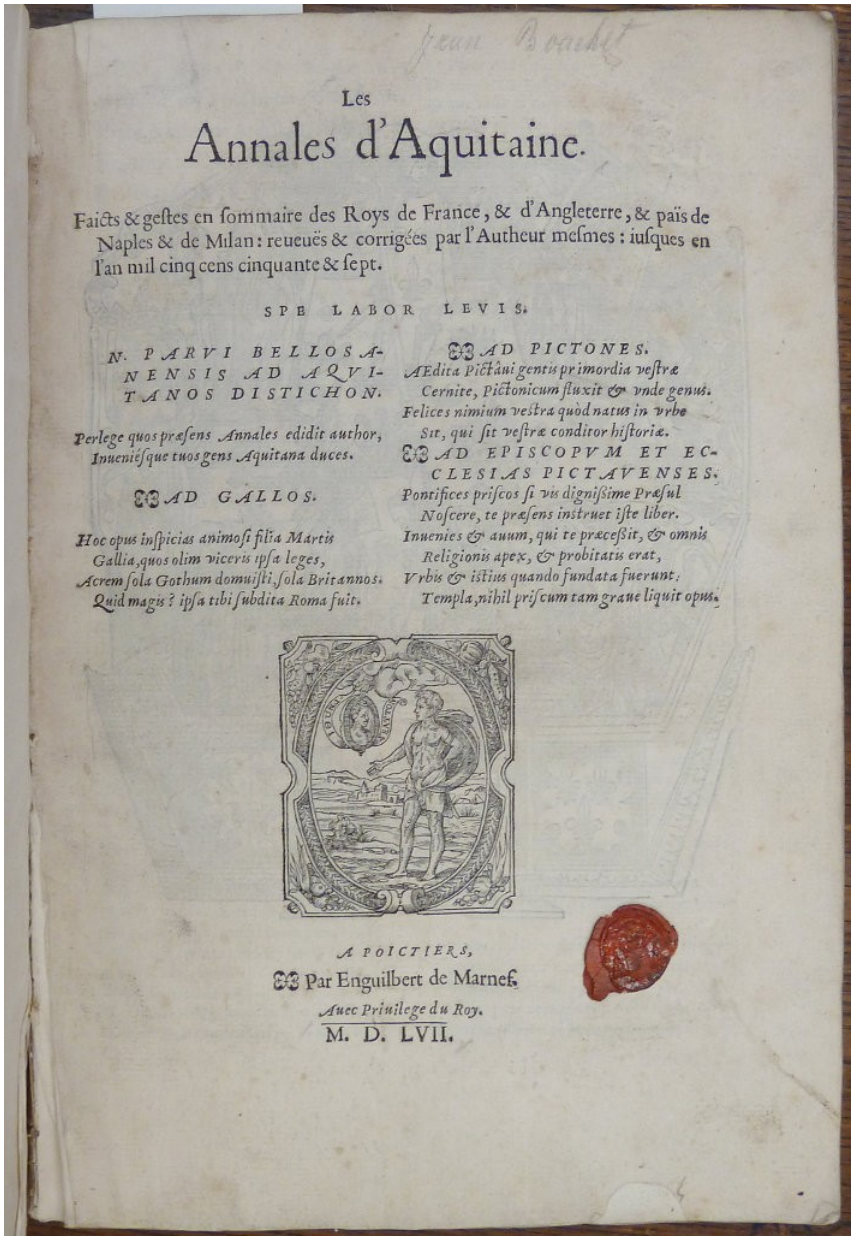
Firma electrónica

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



Les

Annales d'Aquitaine.

Faicts & geſtes en ſommaire des Roys de France, & d'Angleterre, & païs de Naples & de Milan: reueuës & corrigées par l'Autheur meſmes: iuſques en l'an mil cinq cens cinquante & ſept.

SPE LABOR LEVIS.

N. PARVI BELLOSANENSIS AD AQVITANOS DISTICHON.

Perlege quos præſens Annales edidit author,
Inueniéſque tuos gens Aquitana duces.

AD GALLOS.

Hoc opus inſpicias animoſi filia Martis
Gallia, quos olim viceris ipſa leges,
Acrem ſola Gothum domuiſti, ſola Britannos.
Quid magis? ipſa tibi ſubdita Roma fuit.

AD PICTONES.

AEdita Pictáui gentis primordia veſtræ
Cernite, Pictonicum fluxit & vnde genus.
Felices nimium veſtræ quòd natus in vrbe
Sit, qui ſit veſtræ conditor hiſtoriæ.

AD EPISCOPVM ET ECCLESIAS PICTAVENSES.

Pontifices priſcos ſi vis digniſsime Præſul
Noſcere, te præſens inſtruet iſte liber.
Inuenies & auum, qui te præceſsit, & omnis
Religionis apex, & probitatis erat,
Vrbis & iſtius quando fundata fuerunt,
Templa, nihil priſcum tam graue liquit opus.

A POICTIERS,

Par Enguilbert de Marnef.

Auec Priuilege du Roy.

M. D. LVII.

- 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

VklDSU9TIEVMRUNUUk9OSUNPUzEdMBsGA1UEAwwUQ29ycmVvIFVydWd1YXlvIC0gQ0ECEHBwiKirx5klUd8AAmumr+gwDQYJKoZIhvcNAQEBBQAEggEAKRUKCqFGypj60VEvDSy0UzNhExnt

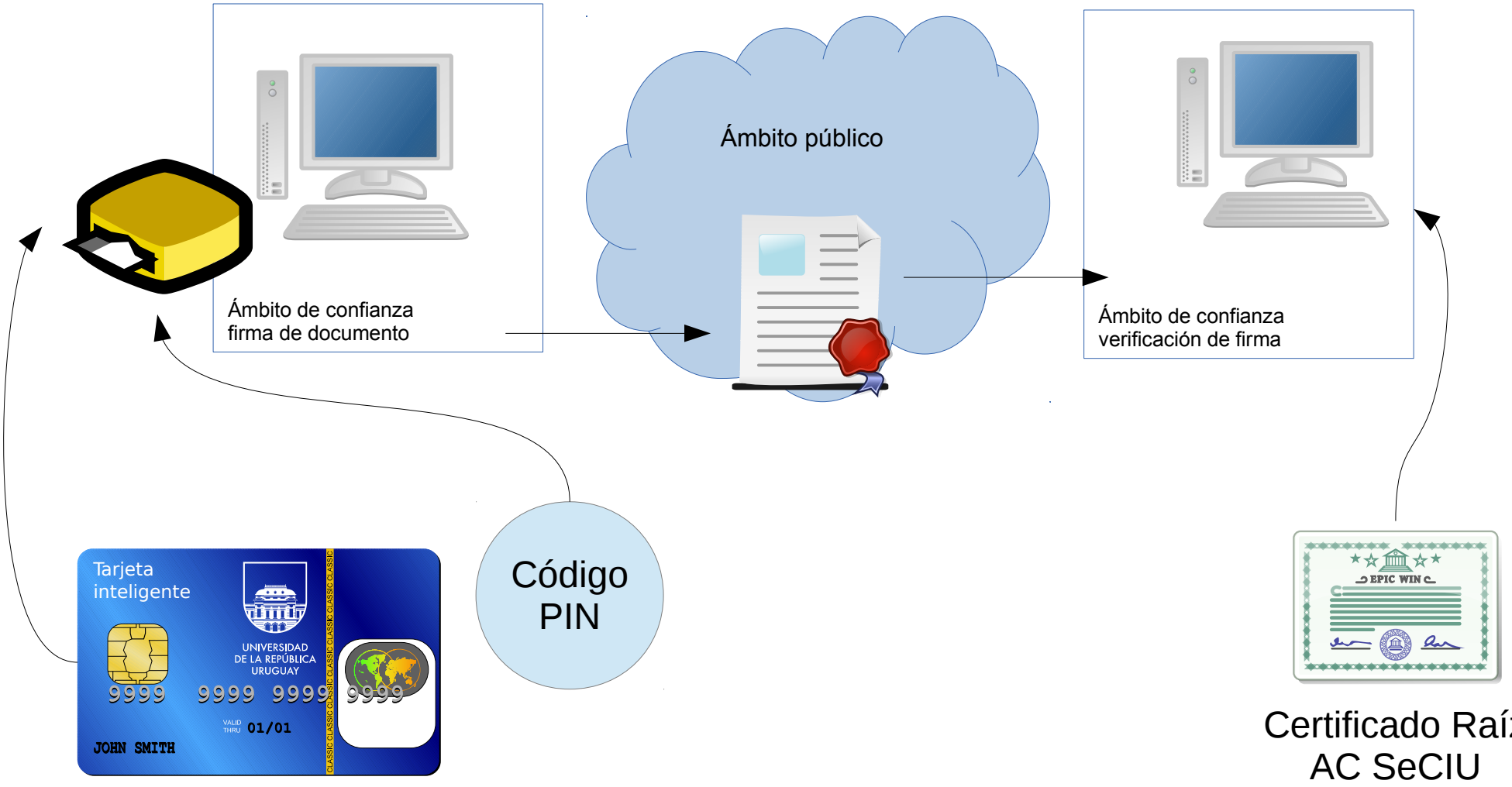
Las zanahorias están cocidas

Clave secreta compartida

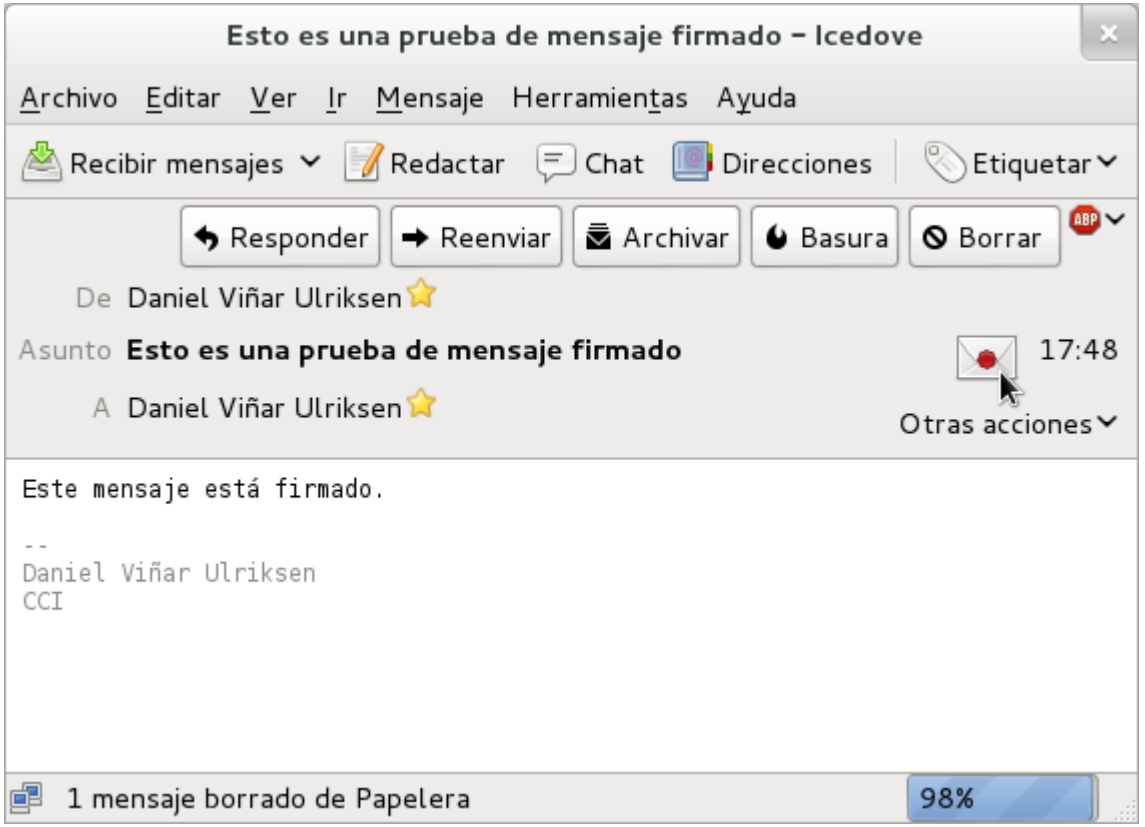
Evolución de la legislación

- 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



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

Contendido 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"

Ã‰ste es un mensaje firmado criptogrÃ¡ficamente en formato MIME.

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

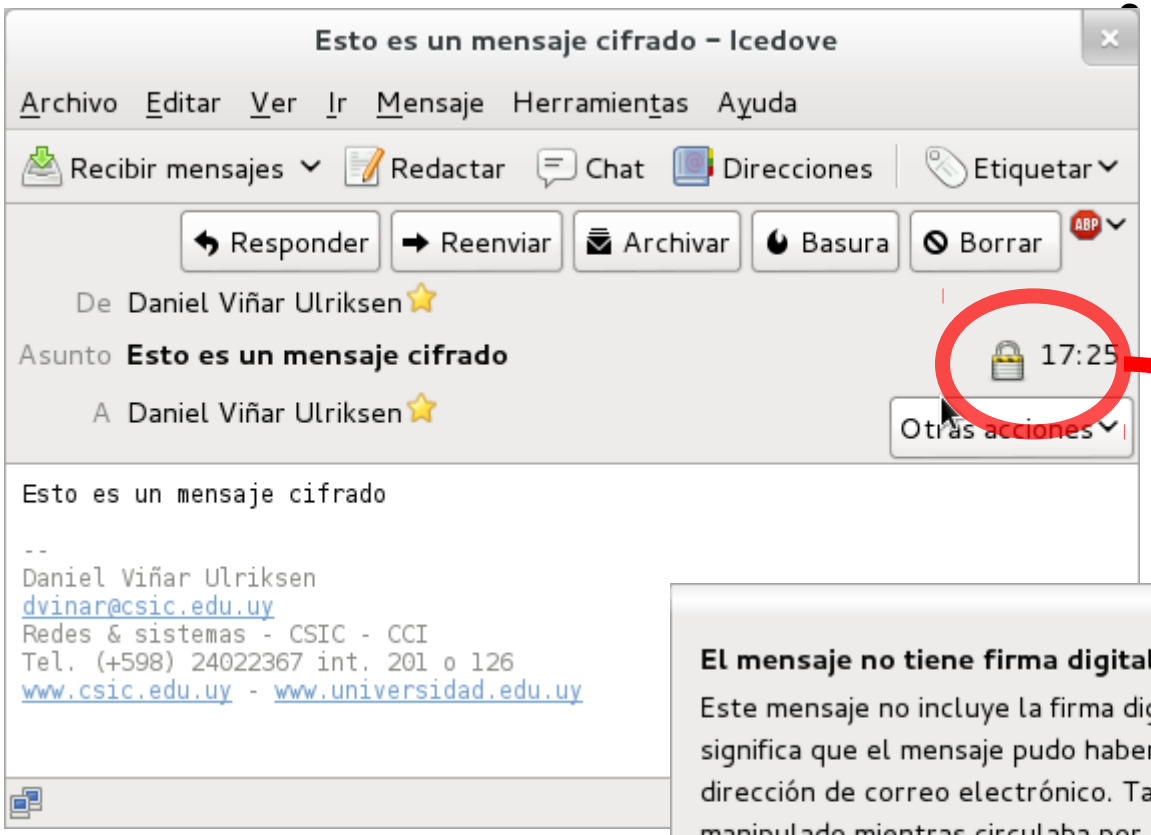
Este mensaje est=E1 firmado.

--=20
Daniel Vi=F1ar Ulriksen
CCI

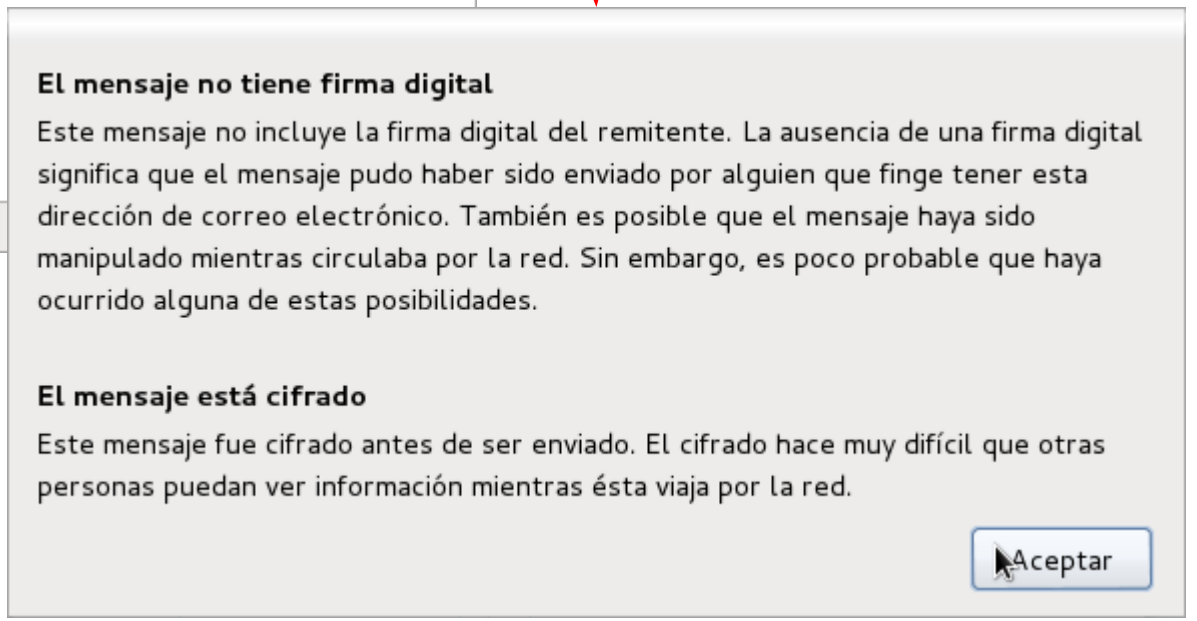
--------------ms020307020103070104030007
Content-Type: application/pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: Firma criptogrÃ¡fica S/MIME

MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIIMUDCC
BcwwggO0oAMCAQICEHBwiKirx5klUd8AAmumr+gwDQYJKoZIhvcNAQEFBQAwejELMAkGA1UE
BhMCVVkxKzApBgNVBAoMIkFETUlOSVNUUkFDSU9OIE5BQ0lPTkFMIERFIENPUlJFT1MxHzAd
(...)
1IXCsU3n4eMXB8WG0V+aZzzAW+5TMmynGNAIOKNR/pxhrYn5yQCLQx5De61B9hSAmkMzDNYq
J88+cmRnyhbF8ejyS++dHToetup5vyv9UjntSPUy/1+E3keh6XKBVUxL2uYofEL8uKTa4HoG
uGEg7Kr3hjCooVWUuWOZ+mMhdAVnAAAAAAAA
--------------ms020307020103070104030007--

Ver un mensaje decifrado en thunderbird



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



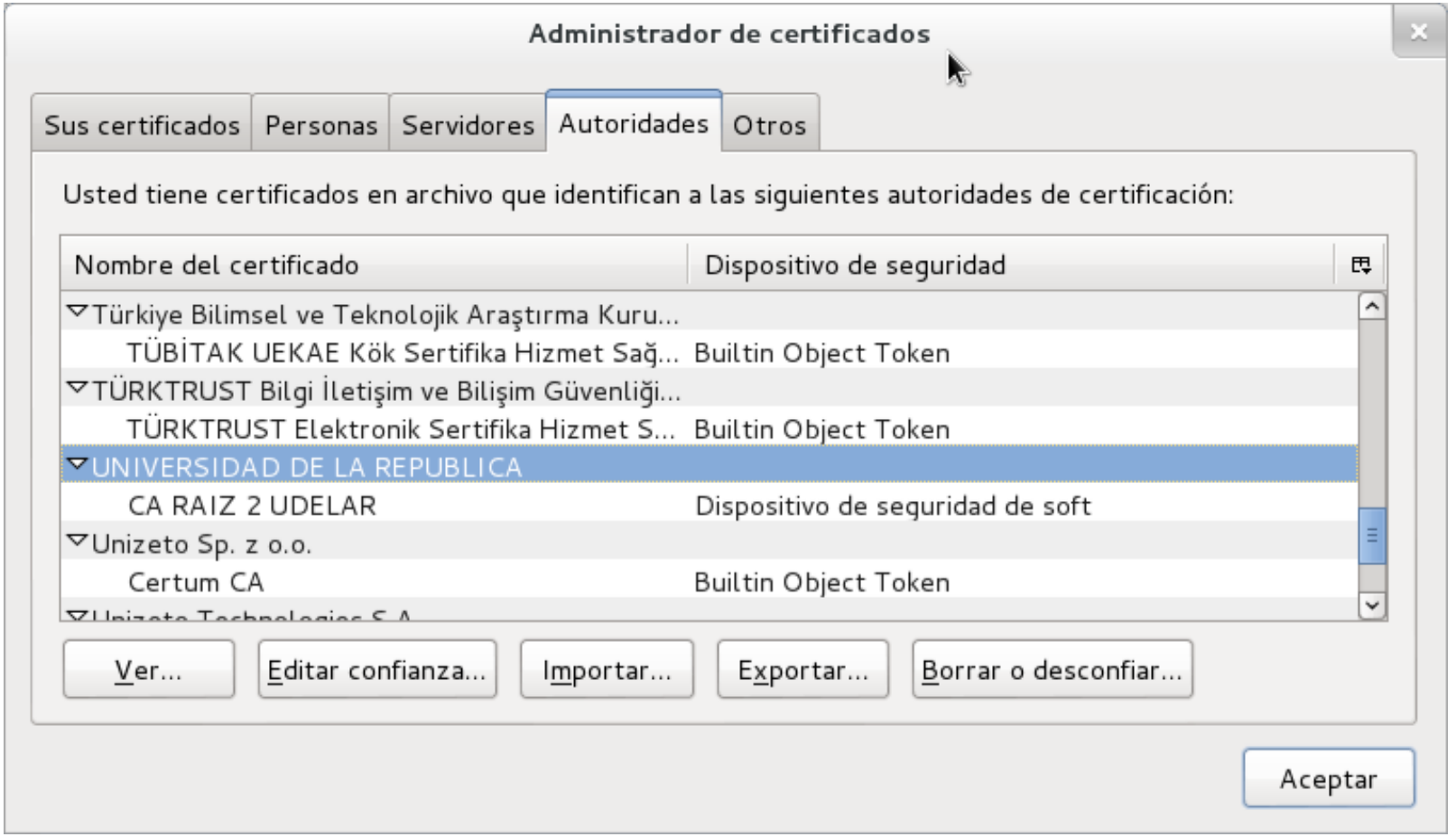
Un verdadero mensaje encriptado

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
A1UECgwiQURNSU5JU1RSQUNJT04gTkFDSU9OQUwgREUgQ09SUkVPUzEfMB0GA1UECwwWU0VS
VklDSU9TIEVMRUNUUk9OSUNPUzEdMBsGA1UEAwwUQ29ycmVvIFVydWd1YXlvIC0gQ0ECEHBw
iKirx5klUd8AAmumr+gwDQYJKoZIhvcNAQEBBQAEggEAKRUKCqFGypj60VEvDSy0UzNhExnt
9c3JF6yqvh+uWjFLf6XZ3BLM1lk3C1cfWllSEBXVbBz18ADQe0MPICG82OlAxaqInWLdUleW
VHIEts0Ot90qWS0HcvflwN5rKgfHEJ8y7UqBEQu8+tBBSG2Lr7eb1hhKfTcUZVW08HRwgjyh
3FYrjPUyycamj2MDOMfu+W+yf/qjwcA+jG0UZbkDPuaNa/euNTEaRy9QXQ18VSXc019dnp5v
wbBRL2EE6hmQ4KIJK6iVDrPnW3xeKcGUkRwj050vdykvsdY18UFjk7WDA/n7WNsjkd2lFc+7
iFEDddrczFmSBJPfE1JmE2KMUTCABgkqhkiG9w0BBwEwFAYIKoZIhvcNAwcECKjljT/B+wtU
oIAEggEwpwM+XiTT8Q+/rugOOlZ4cSKgGVEGViiuhHfd7A3CeLZwMxM6+R2cyadjNJcMRSHr
HqLE6OV5kqmuCKfTu2U+df7DCW7I9HTlkbxIYdJIXEfPepZNwnAk7o1LRCp22p7zjzsyJcRs
FmNYUj50nQgWkxlRcc10o8R7XigkzTWvZXxupoUamaxh22p33kMQFLDYpvgRku7iB8kFDdXm
0lmcHlLsv2/PylYoJUA/5V8LNkIsSkVwTXEUgNyw6megJg6ZoAzrrTe4pQtQcxClD0VCD5xK
WmgheqsShHobSeAxj2+27OG1mE5L3Tsyw2ZQSW68IuSmR0asPHrb4k8w0PU9twXVhFY+xCdK
qxCAcsw5bVxHVeeEPFFR5IXc+hHErO1/j4S5Urw5lhQ/csEYiycA7wQIYLIoRiKbqHkAAAAA
AAAAAAAA

Certificado raíz de SeCIU

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



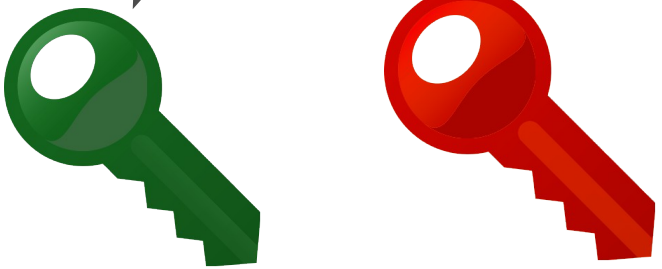
Huella SHA1 del Certificado Raíz de SeCIU
05 E9 C9 B7 5F 42 BF DB AC 27 29 9E 4D F2 7F F6 DC 2B A2 0B

criptografía asimétrica

Jim

Número aleatorio elevado

Algoritmo de generación de clave



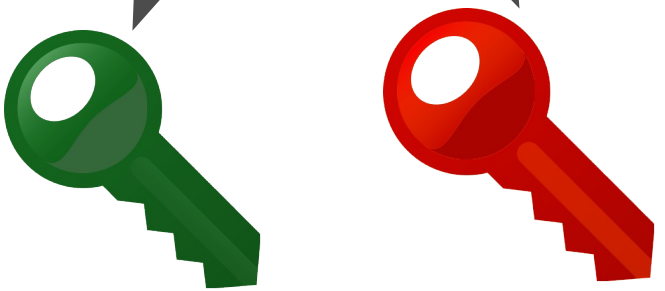
Clave pública

Clave privada

Andy

Número aleatorio elevado

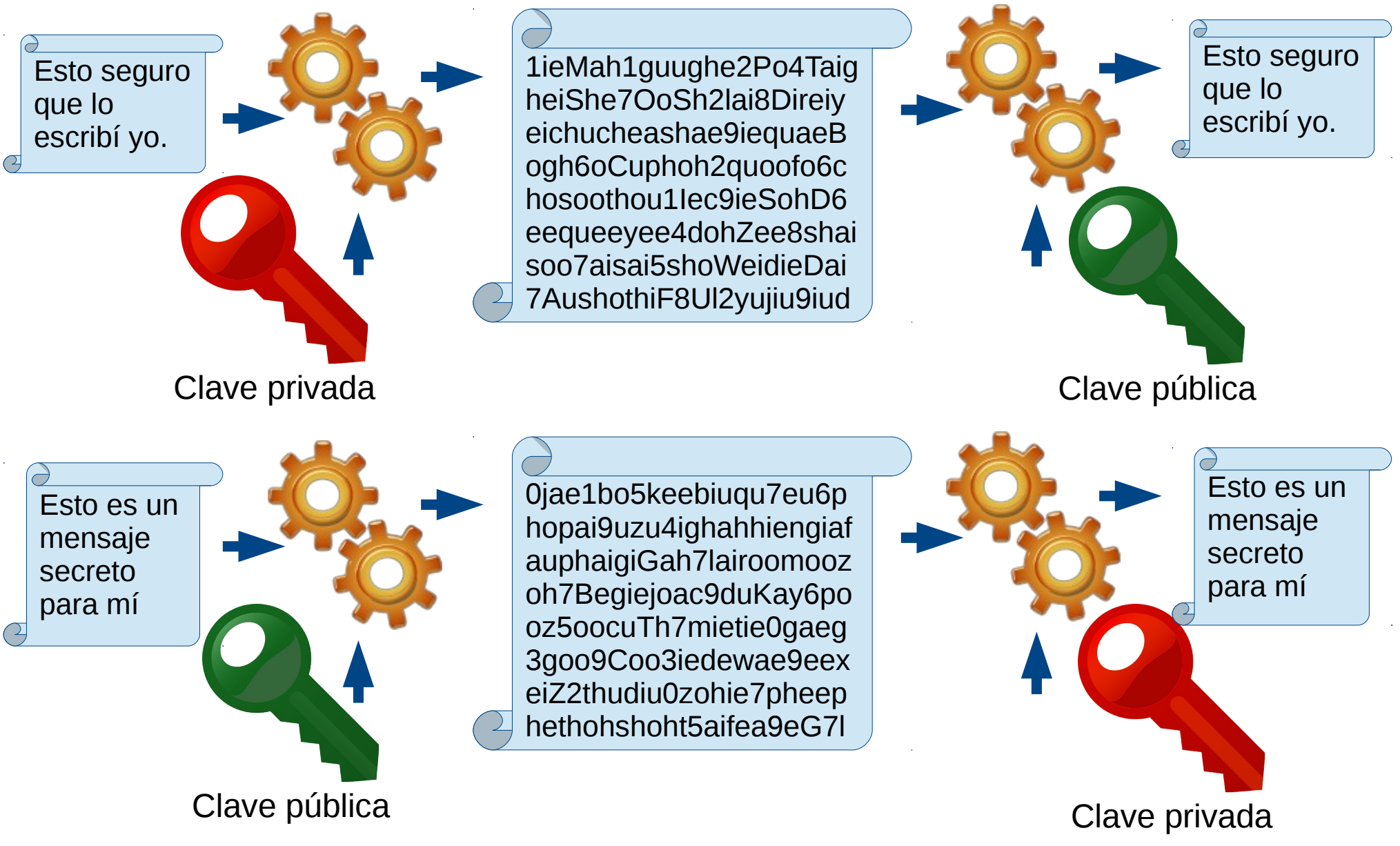
Algoritmo de generación de clave



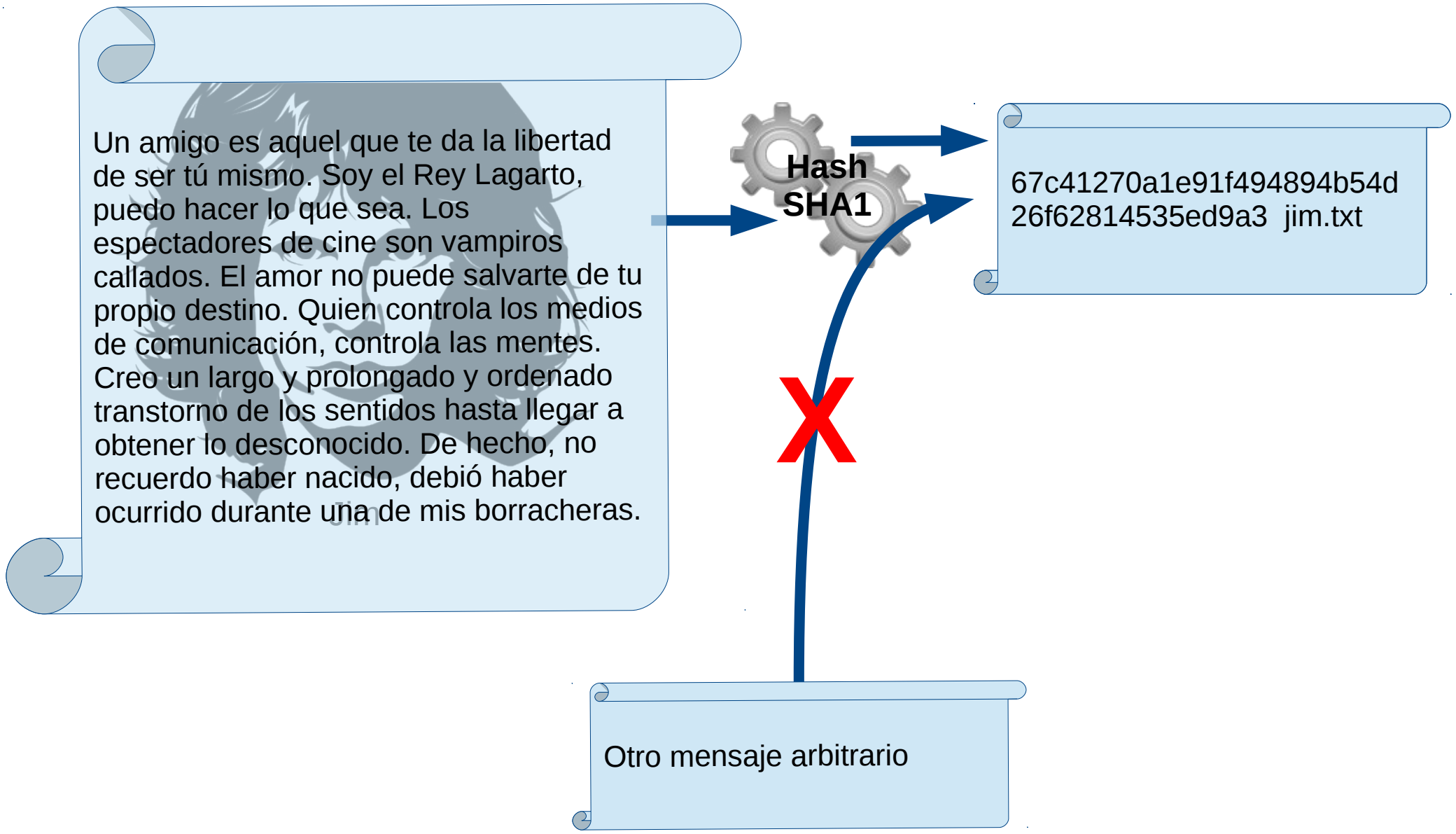
Clave pública

Clave privada

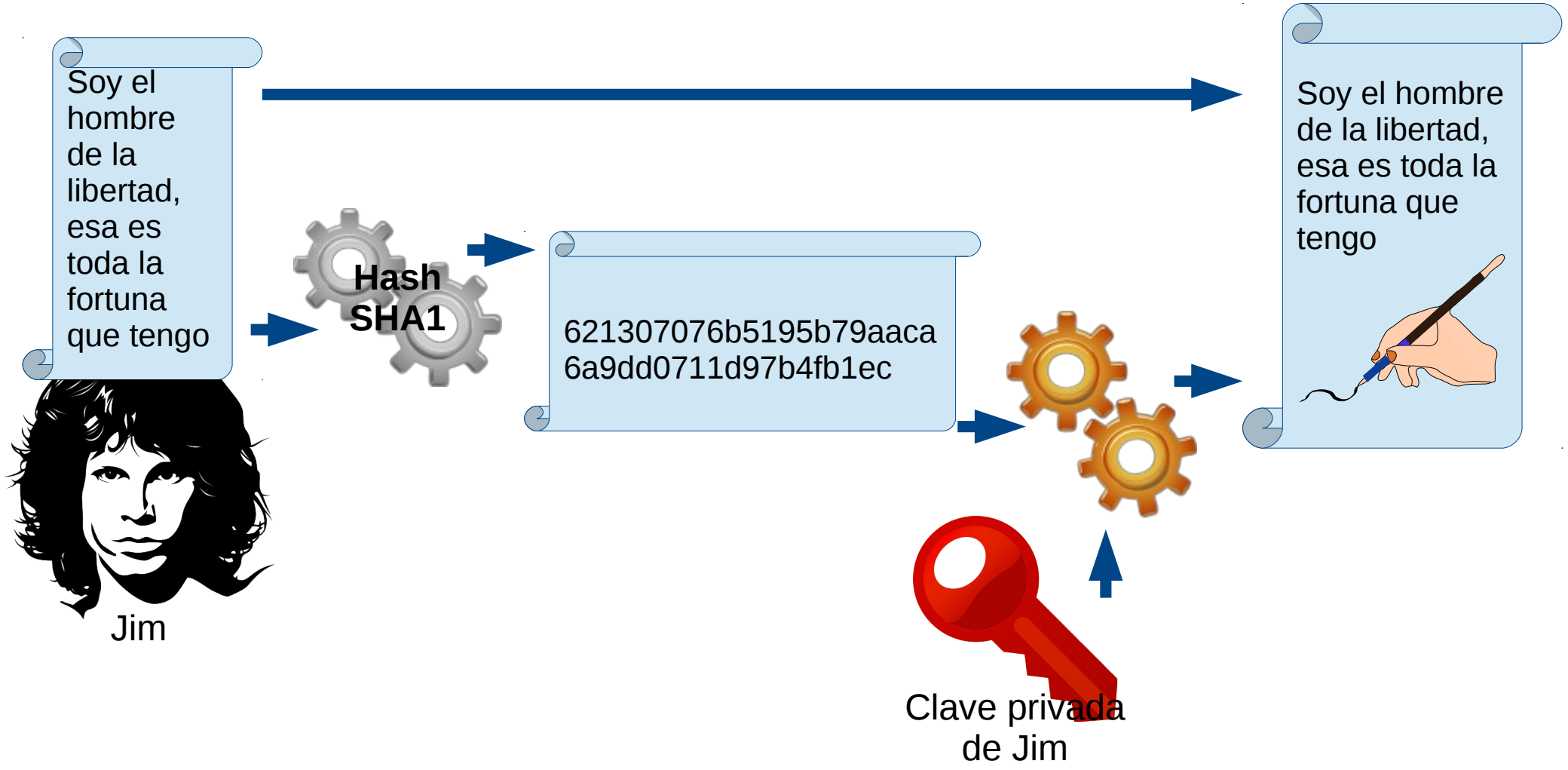
Asocioación asimétrica de las claves



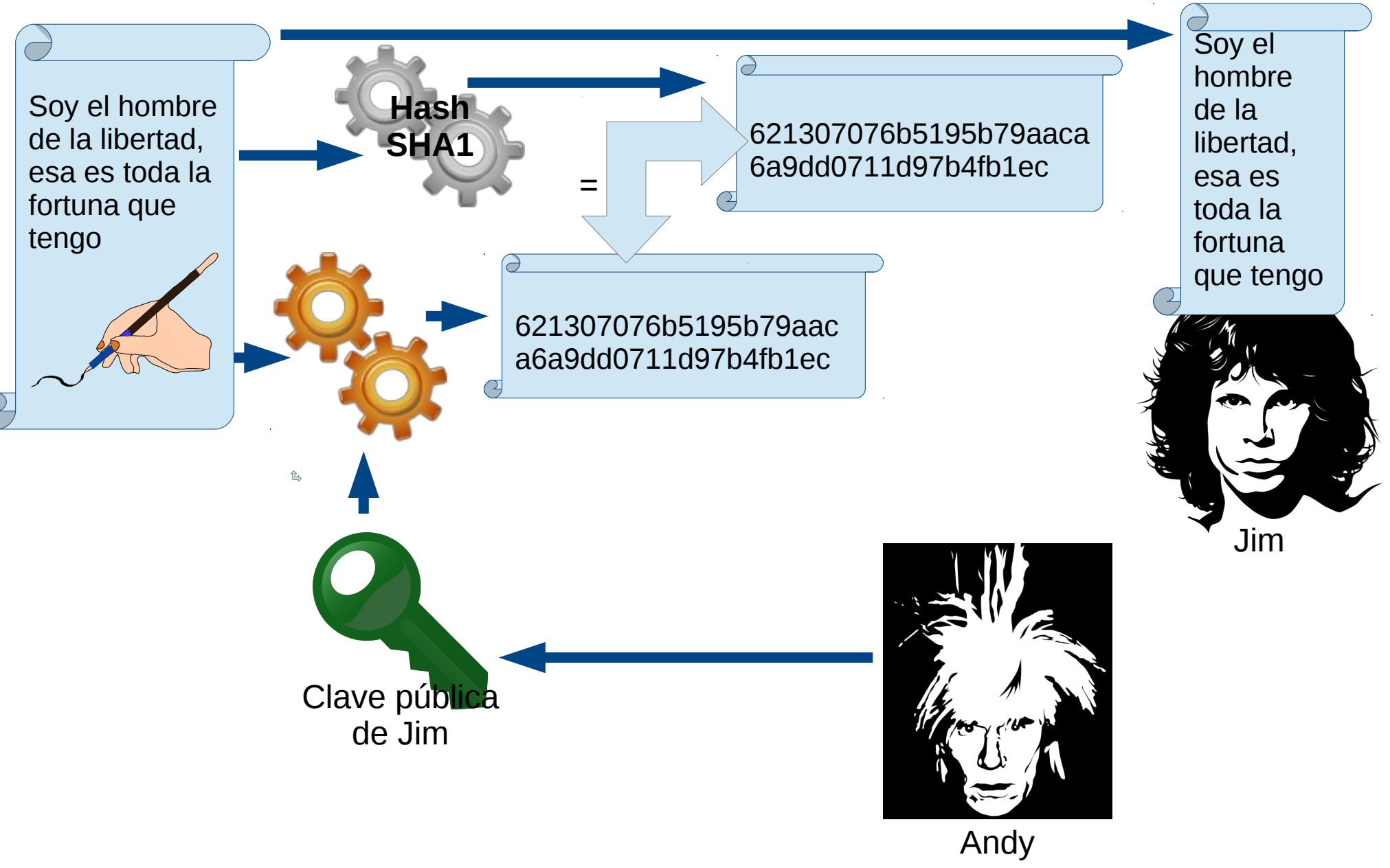
Una herramienta matemática: el hashtag: da la integridad



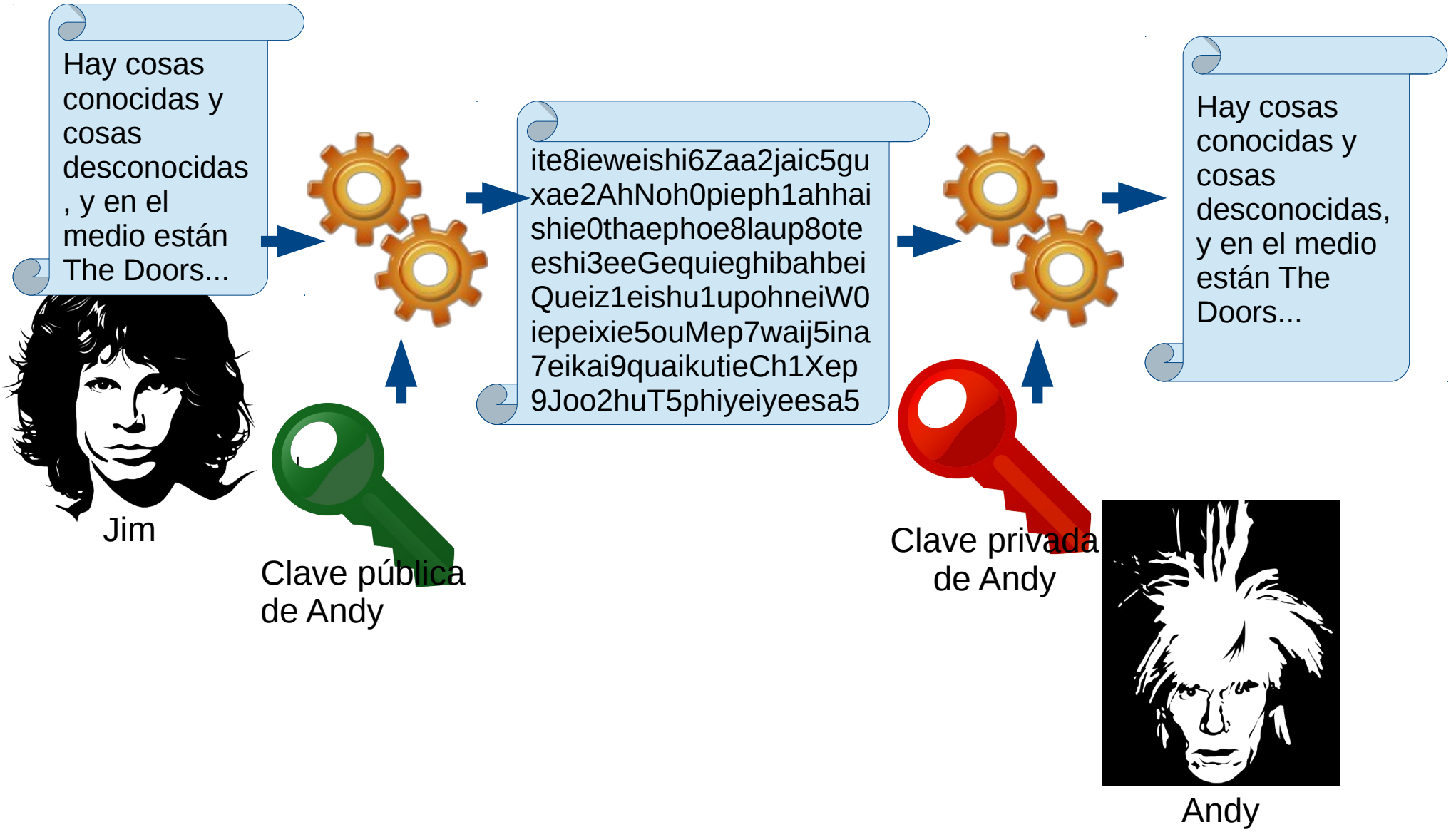
Jim firma


Soy el hombre de la libertad, esa es toda la fortuna que tengo
Hash SHA1
621307076b5195b79aaca6a9dd0711d97b4fb1ec
Soy el hombre de la libertad, esa es toda la fortuna que tengo
Jim
Clave privada de Jim

Andy reconoce la firma de Jim



Jim le escribe un mensaje confidencial a Andy



El problema d*el hombre en el medio*

El rey

Clave pública
del tal iván

Clave pública
del rey

El tal Iván

El puchero
está listo

Las papas
están
quemadas

Tío sam

La infraestructura de clave pública