

Firmas y Certificados digitales: conceptos y contextos

Autor: Pedro Castilla del Carpio

INSTITUTO NACIONAL
DE DEFENSA DE LA
COMPETENCIA Y DE LA
PROTECCIÓN DE LA
PROPIEDAD INTELECTUAL



La SUNAT está implementando los libros contables electrónicos y la factura electrónica.

El Poder Judicial está implementando la notificación electrónica en los procesos judiciales laborales y contencioso administrativos. Además, junto con el IFB, el PP.JJ. tiene un proyecto de implementación del “expediente electrónico” en los Juzgados Comerciales para reducir drásticamente la duración de los procesos.

La SUNARP está incorporando procedimientos en vía electrónica para la inscripción de diversos títulos legales.

El RENIEC ha construido una infraestructura electrónica para generar certificados digitales a todos los funcionarios del Estado y, eventualmente, para todos los ciudadanos que se relacionen administrativamente con Entidades del Estado.

La CONASEV utiliza hace 5 años vías electrónicas como vehículo de sus relaciones oficiales con las empresas supervisadas.

Estos son algunos ejemplos **en el ámbito del gobierno electrónico**. Todos ellos, en algún punto, se sustentan en aquello que se llama “el Certificado Digital”.

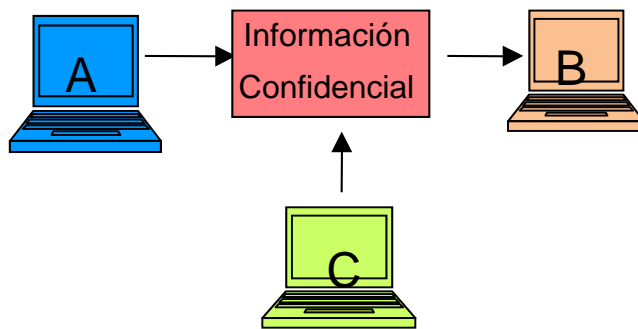
En el marco del comercio electrónico, y en todo el planeta:

- Cada compraventa que se hace con tarjeta de crédito a través de internet,
 - Cada transferencia bancaria hecha por vía electrónica,
 - Cada portal o website asegurados contra imposturas y suplantaciones,
- están basados en “Certificados Digitales”.

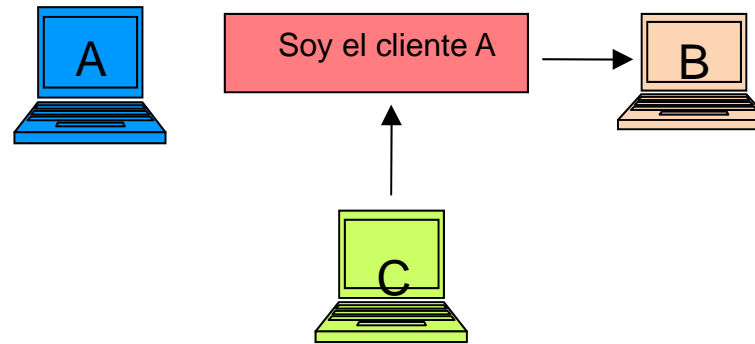
En conclusión: vale la pena conocer **cómo funciona** y **por qué funciona** la certificación digital.

Cuatro escenarios inseguros en las vías electrónicas de comunicación

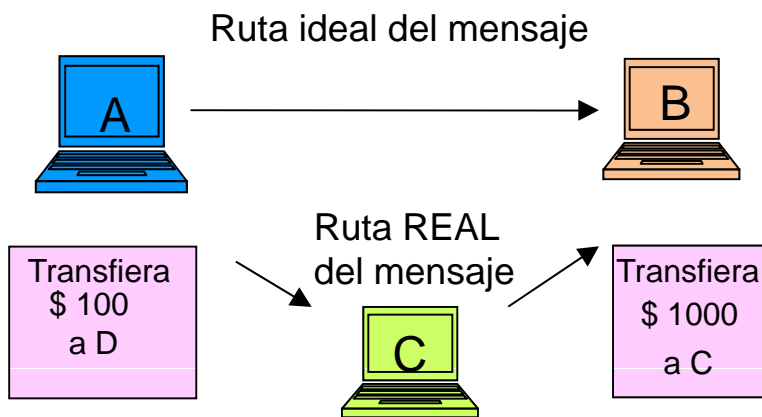
1. Espionaje



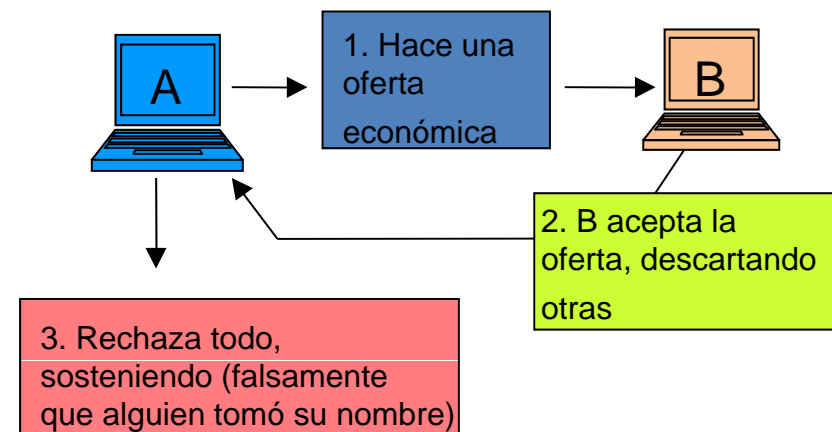
2. Suplantación de identidad



3. Adulteración de los documentos



4. Negación maliciosa de documento propio



¿ Cómo hacemos para evitar dichos escenarios?

Felizmente, existen herramientas con las cuales podemos asegurar cuatro cosas:

➔ 1. La verdadera identidad de los remitentes de documentos electrónicos.

➔ 2. La imposibilidad de que más tarde dichos remitentes quieran desconocer los compromisos asumidos por vía electrónica.

➔ 3. La privacidad de los documentos, negando su lectura a quienes no sean los destinatarios.

➔ 4. La imposibilidad de que alguien (emisor, receptor o tercero) adultere el contenido de los documentos sin ser notado.

El arte-ciencia que nos da las herramientas necesarias se denomina criptografía.

“En Internet, nadie sabe que eres un perro”



"On the Internet, nobody knows you're a dog."

Soluciones Criptográficas

Un documento construido con un sistema de signos que conocemos, tiene carácter comprensible. La criptografía es la técnica que permite eliminar (cifrar) el carácter comprensible de un documento, y después recuperarlo (descifrarlo). Los procesos de cifrado y descifrado utilizan un “algoritmo” y una o más “claves”.

Un algoritmo consiste en una secuencia de operaciones dirigidas a cierto objetivo (es una guía de instrucciones). Ejemplos: el procedimiento para obtener una raíz cuadrada. El procedimiento para obtener el máximo común divisor de dos números.

Por lo general los algoritmos criptográficos son públicamente conocidos. No existe misterio respecto a cuáles son las operaciones que deben realizarse. El secreto consiste en los números específicos que deben insertarse en ellas. A esos números se les denomina las claves.

Un algoritmo muy simple, llamado “Julio César” como uno de sus primeros usuarios, consiste en sustituir cada letra por la que viene tres lugares después en el abecedario:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z
d	e	f	g	h	i	j	k	l	m	n	ñ	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

Con este método, la frase “**General, ataque por el norte a las cinco de la mañana**” se convierte en:

Jhphuñ, dwdtxh
sru hñ pruw h d
ñdv flpfr gh ñd
odqdpd.

Julio César,
dibujo de Goscinny:



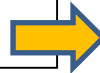
Este es un ejemplo de la relación entre algoritmo y clave.

Este es el algoritmo XOR

Input 1	Input 2	Output
0	0	0
0	1	1
1	0	1
1	1	0

Como clave secreta, usemos el número 10010101

Texto: "Pague 1000 a Juan"
Lo paso a formato binario



01011100

Aquí se introduce la clave secreta



+ 10010101

Los 2 números se suman siguiendo el algoritmo XOR



11001001

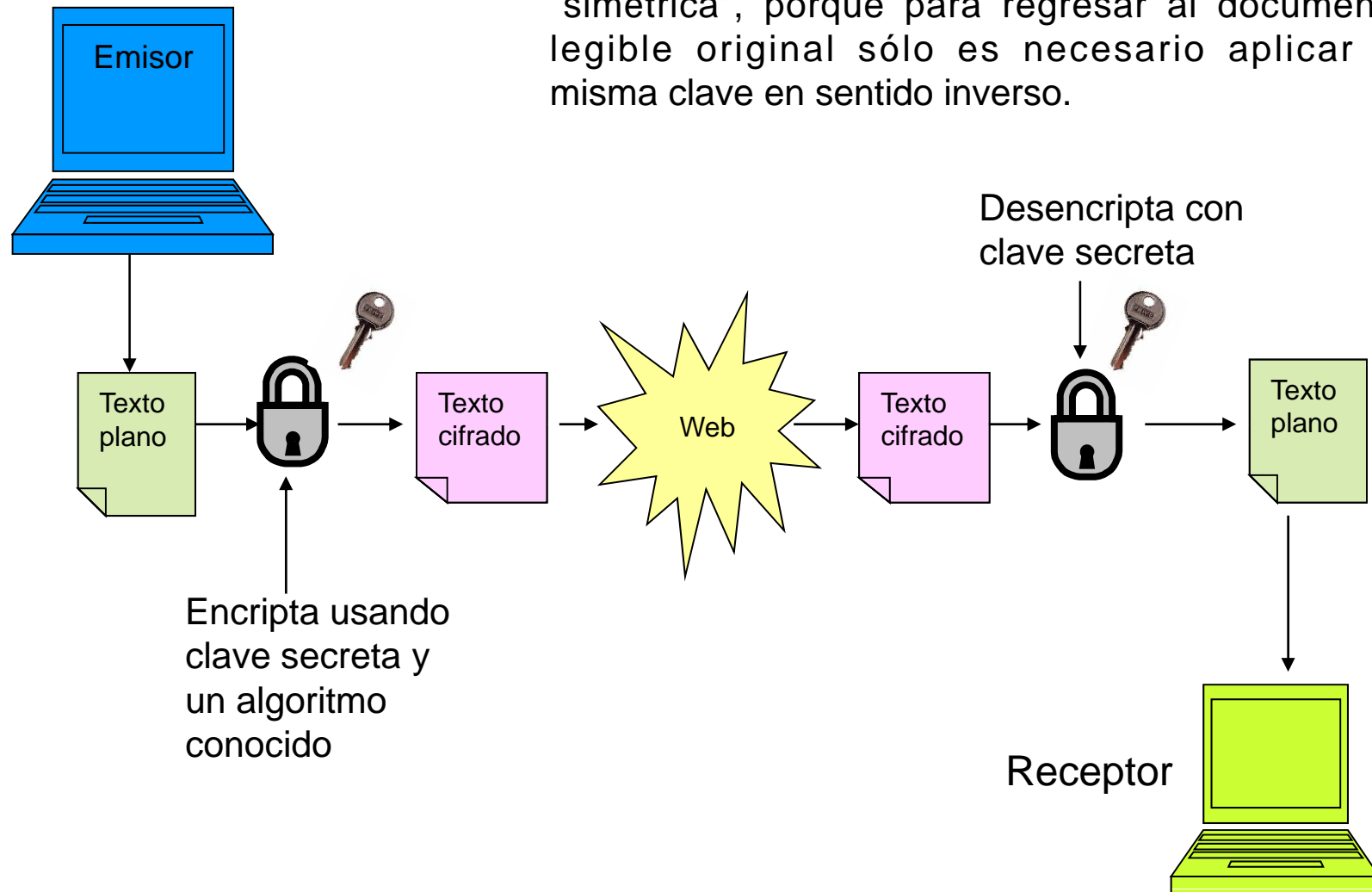


En formato de texto: ZTU91%^



Un espía podría obtener el número 11001001, pero como no sabe la clave secreta no puede deducir el número equivalente al mensaje. (En este ejemplo, los números que se usan son pequeñísimos, y con algunos minutos de "prueba y error" se agotarían todas las combinaciones posibles y se descubriría el texto).

A una clave como la anterior se le denomina “simétrica”, porque para regresar al documento legible original sólo es necesario aplicar la misma clave en sentido inverso.



Criptografía de clave asimétrica

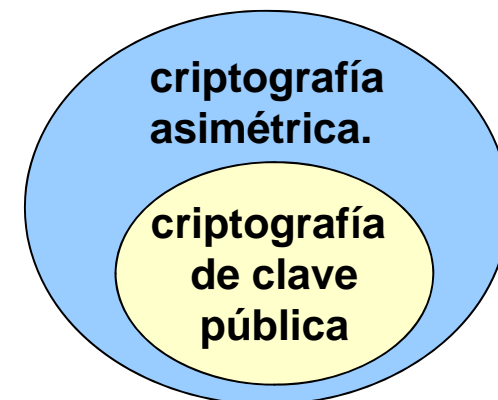
En la criptografía de clave asimétrica, no se usa la misma clave para cifrar y descifrar, sino que tenemos dos claves relacionadas matemáticamente entre sí de modo tal que una descifra lo que la otra cifró. Lo que parece extraño al profano es que:

*“Ninguna otra clave puede desencriptar el mensaje, **¡ni siquiera la clave original!** (Hay razones matemáticas que aseguran esto).*

La belleza de este esquema es que cada persona sólo necesita una pareja de claves para comunicarse con cualquier número de interlocutores. Una vez que alguien obtiene su par de claves, puede comunicarse con cualquier otra persona”. (Un grupo de 1000 personas sólo necesitaría 2,000 claves).

(Atul Kahate, “Cryptography and Network Security”).

La criptografía de clave pública (en donde una de las claves es de conocimiento público y la otra es de conocimiento exclusivo del titular del par de claves) es una sub-clase (la más utilizada) de la criptografía asimétrica. Será objeto de estudio en esta presentación.



La criptografía de clave pública nos provee con dos mecanismos o procesos:

- Uno para lograr privacidad e integridad. (“Proceso 1”)
- Otro para lograr autenticidad, “no repudio” e integridad. (“Proceso 2”).

Aplicando el segundo proceso sobre el resultado del primer proceso, obtenemos todo.

Esquema del resto de esta presentación:

1. Descripción del proceso 1.
2. Descripción del proceso 2.
3. Descripción de la combinación de ambos procesos para obtener todo simultáneamente (proceso 3).
4. El Talón de Aquiles del sistema y mecanismos para superarlo.
5. Anexo: se estudiara el algoritmo mas empleado en la criptografia de clave publica.

Un paréntesis:



Para nuestros ejemplos usaremos a Pierre Fermat (1601 – 1665) y Leonhard Euler (leer “Oiler”) (1707 – 1783)



Usamos sus nombres pues algunos de sus aportes a la Teoría de Números son básicos para la comprensión matemática del algoritmo más utilizado en los programas de criptografía pública (el método RSA).



En lo sucesivo, usaremos imágenes de llaves para expresar que estamos encriptando / “cerrando” un documento (volviéndolo ilegible) o desencriptandolo / abriéndolo (volviéndolo legible). En realidad las llaves son números. Los documentos tambien los convertimos en números. Asi, las llaves y los documentos seran “inputs” que introduciremos en las formulas de cierto algoritmo.

Proceso 1. Objetivo: Privacidad e Integridad en las comunicaciones

Primer paso.

1º se aplica una sencilla "tabla de conversión" de letras a números.

Dr. Fermat



Exámenes Serológicos de Euler

A = 01
B = 02
C = 03
(...)

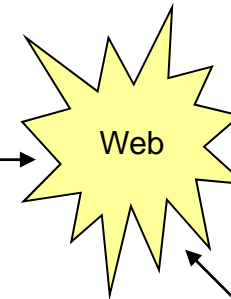
El mensaje se convierte en un número:

0572958
4837501
9283...
5789

Luego Fermat ENCRIPTA, v.d. ejecuta la primera parte de un algoritmo asimétrico públicamente conocido, usando dos números como inputs: 1) el mensaje, y 2) la clave pública de Euler.

El resultado es otro número:

7354628
98750



7354628
98750



Euler

Clave privada Clave pública



Si Cain intercepta el documento, para descifrarlo necesitaría la clave privada de Euler, que no tiene. Quizá pueda borrarlo, pero no leerlo.



Segundo paso.

Euler DESENCRIPTA: ejecuta la segunda parte del mismo algoritmo, usando dos números como inputs: 1) el documento cifrado que recibió, y 2) su clave privada.



7354628
98750

La clave privada REVIERTE lo que la clave pública hizo:

0572958
4837501
9283...
5789

Luego Euler aplica la "tabla de conversión" de letras a números.

A = 01
B = 02
C = 03
(...)

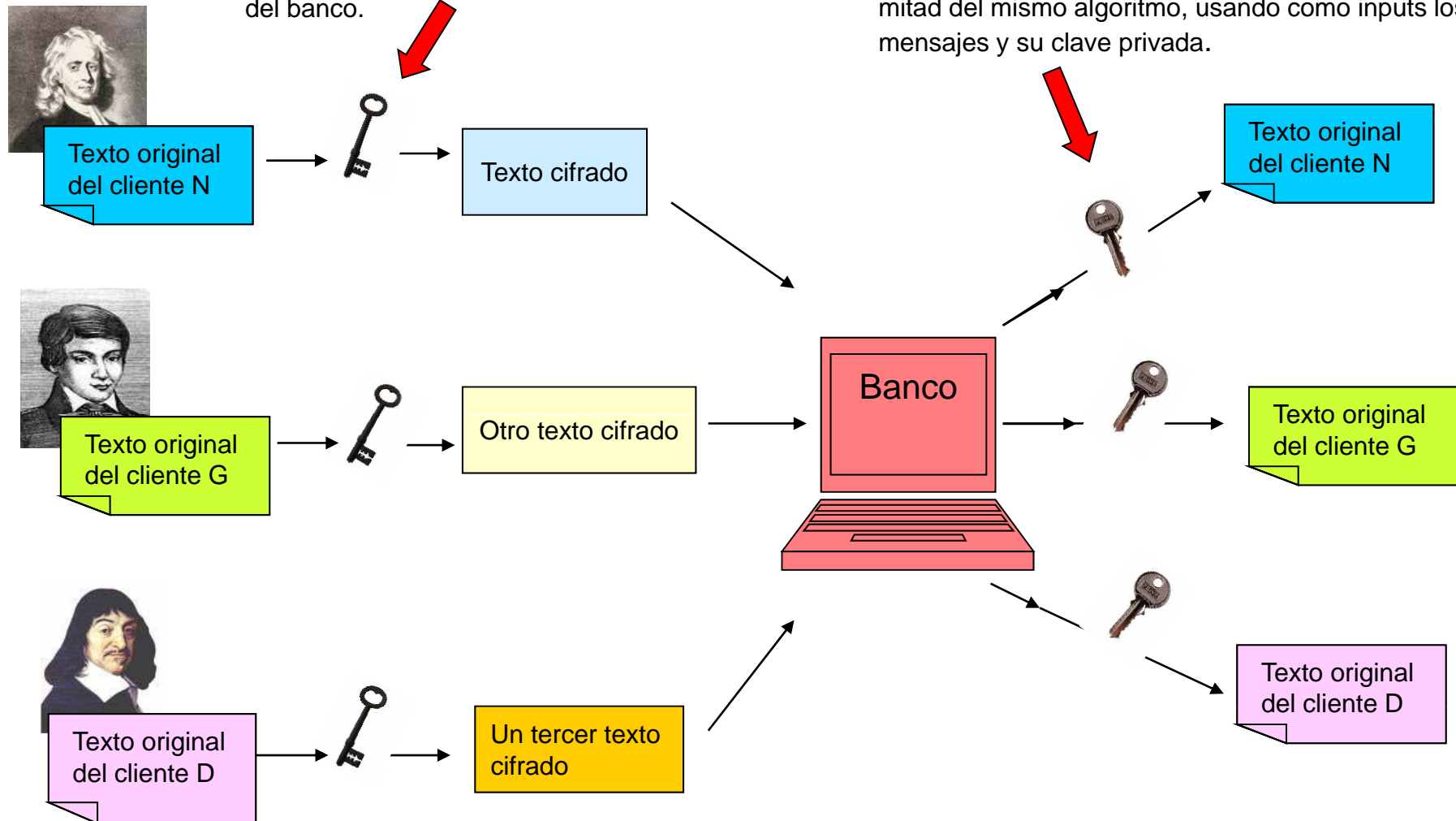
Exámenes Serológicos de Euler

Observe: todos, incluso Caín, conocen el algoritmo. Los algoritmos son PUBLICOS. También los inputs que se vacían en las formulas del algoritmo son conocidos, MENOS UNO. La clave privada de Euler es ese input secreto.

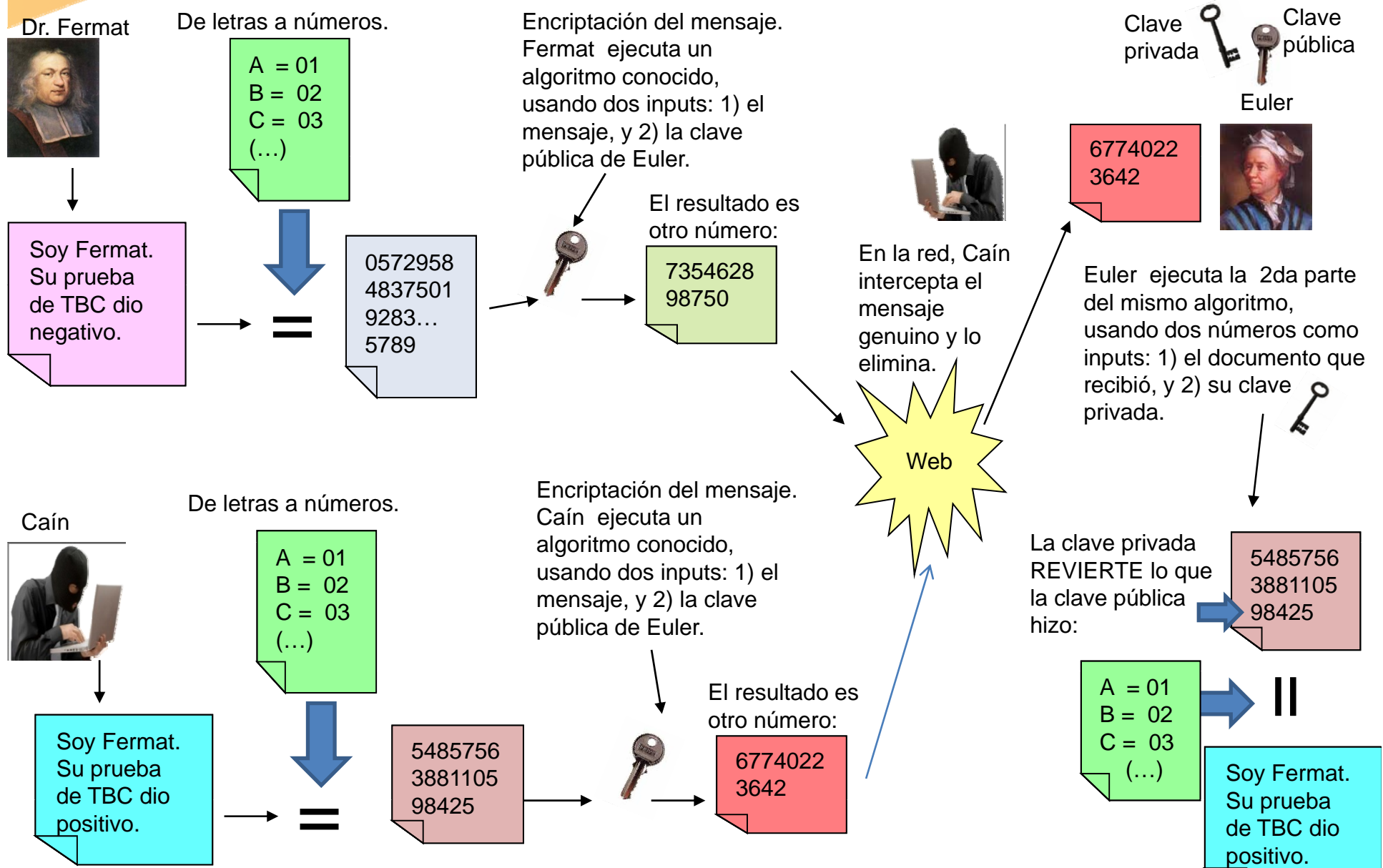
Nota 1: además de garantizar privacidad e integridad, el mecanismo es económico. Una persona sólo necesita un par de claves para recibir información confidencial de “ n ” contactos a través de un medio inseguro (internet)

1. Los clientes cifran sus mensajes ejecutando un algoritmo conocido y usando, como inputs, sus mensajes y la clave publica del banco.

2. El banco descifra los mensajes ejecutando la 2a mitad del mismo algoritmo, usando como inputs los mensajes y su clave privada.



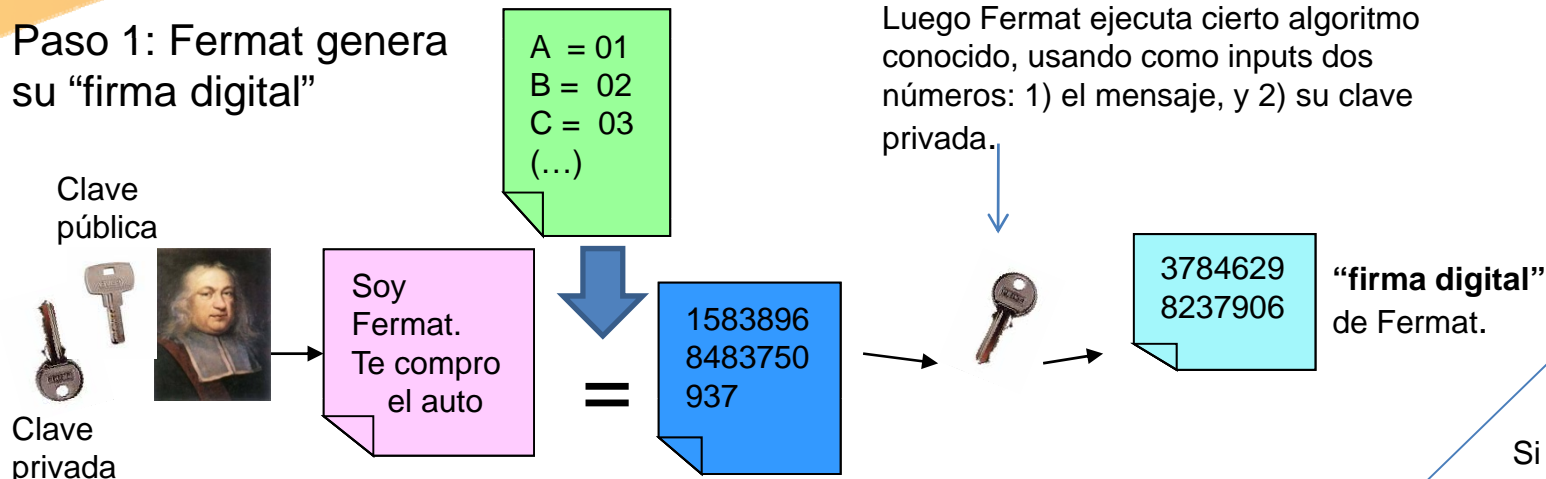
Nota 2: el proceso 1 no pretende garantizar la autenticidad del documento recibido



Si Euler solo se apoya en el proceso 1, puede ser víctima de un engaño

Proceso 2. Objetivo: autenticidad, integridad y carácter no repudiable del documento

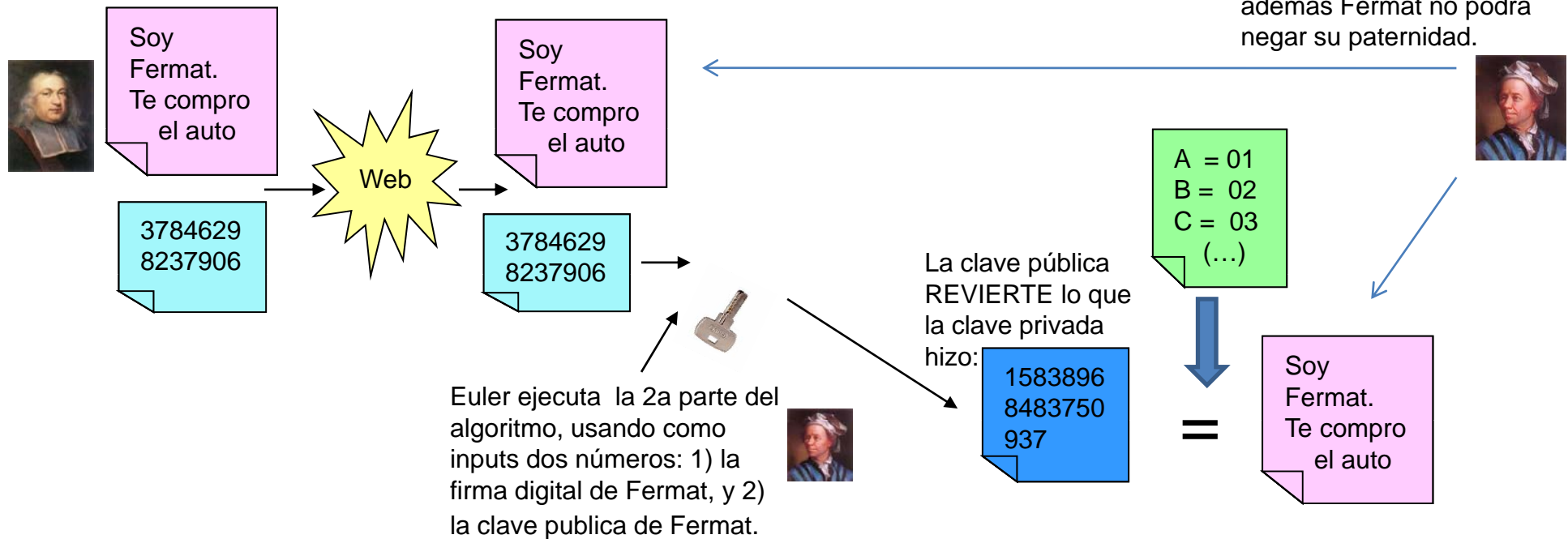
Paso 1: Fermat genera su "firma digital"



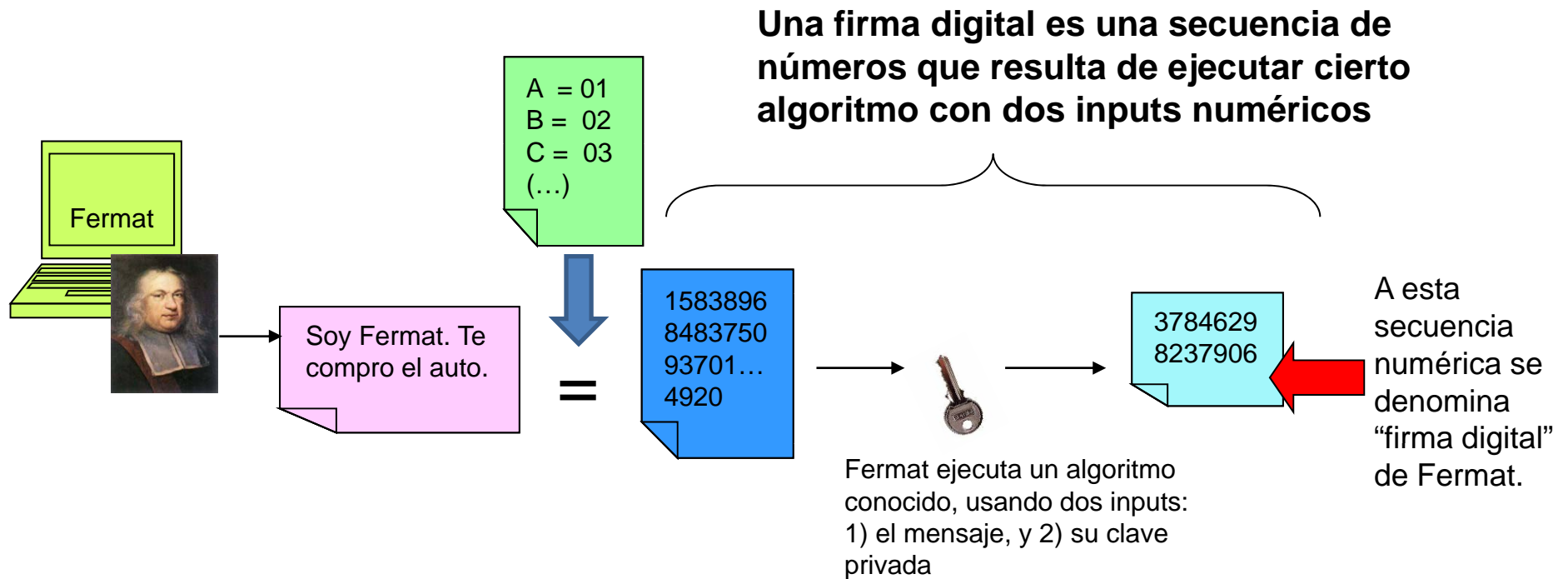
FINAL

Si los dos coinciden, Euler sabe que la firma digital fue generada con la clave privada de Fermat, y que además Fermat no podrá negar su paternidad.

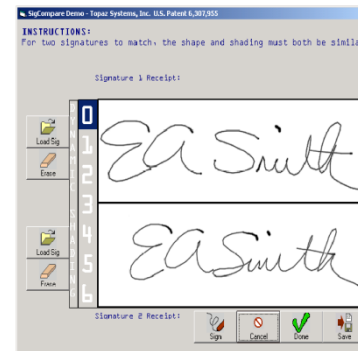
Paso 2: Fermat envía dos cosas: el texto legible y la "firma digital"



Notas sobre el Proceso 2. Nota 1: la firma digital NO es una reproducción de la firma gráfica manuscrita

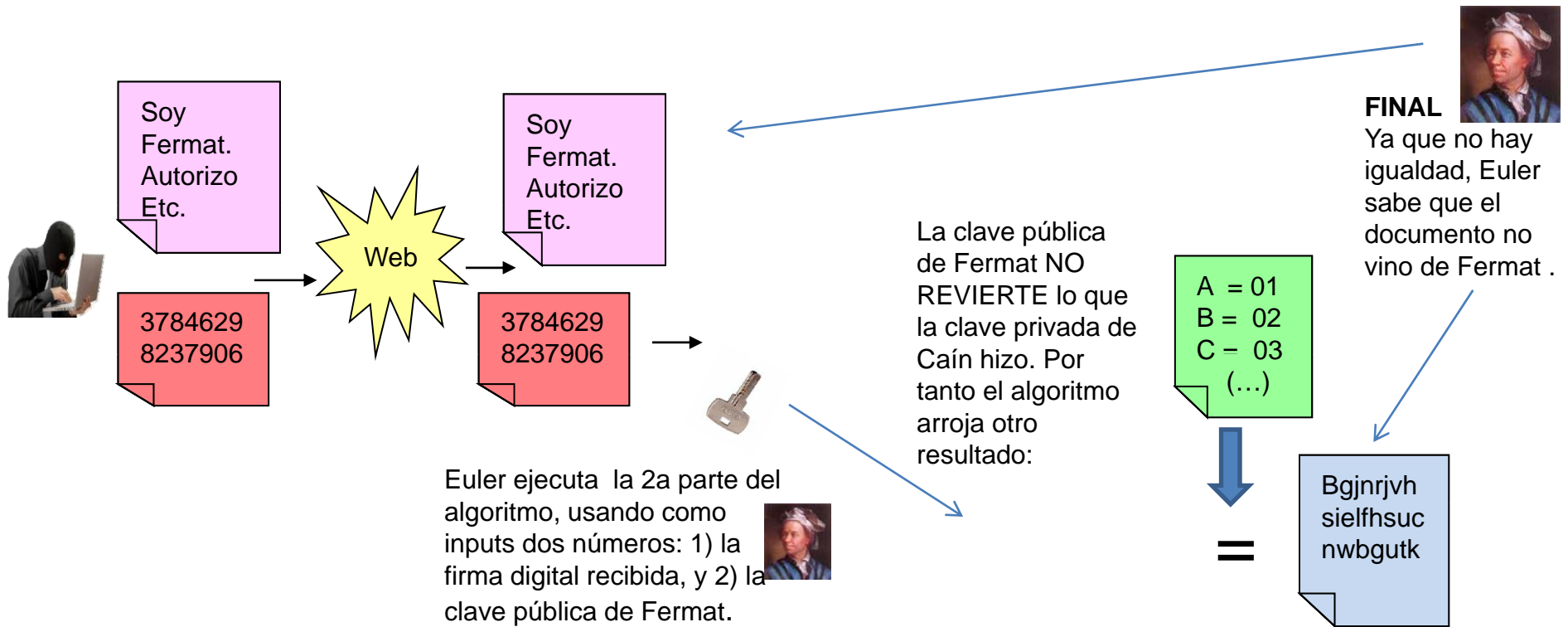
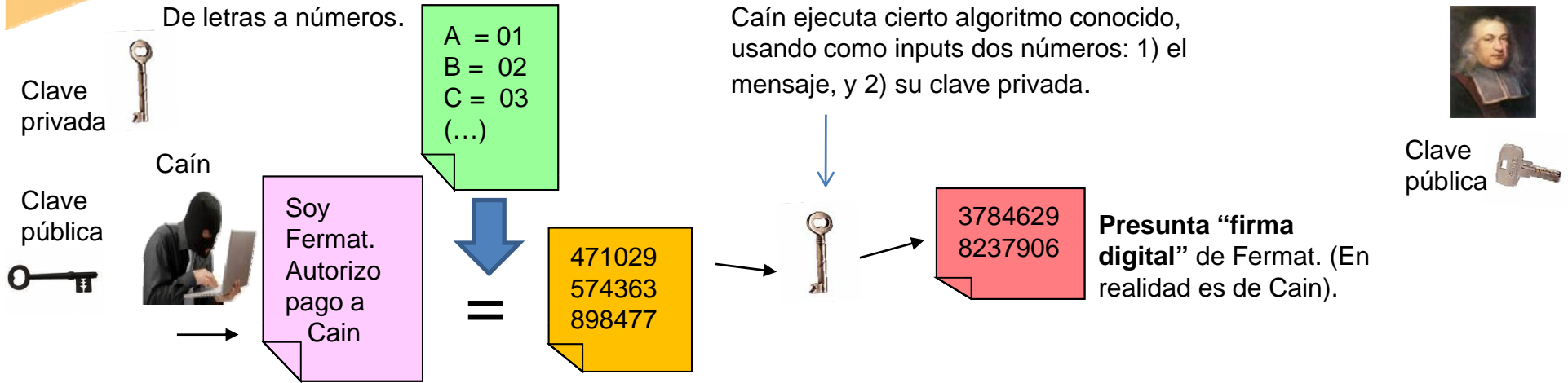


Así pues, una firma digital NO es una firma “escaneada” o “digitalizada”. Estas últimas son otras modalidades de **firma electrónica**. El nombre de “firma digital” se reserva para la secuencia numérica resultante del proceso criptográfico arriba descrito.

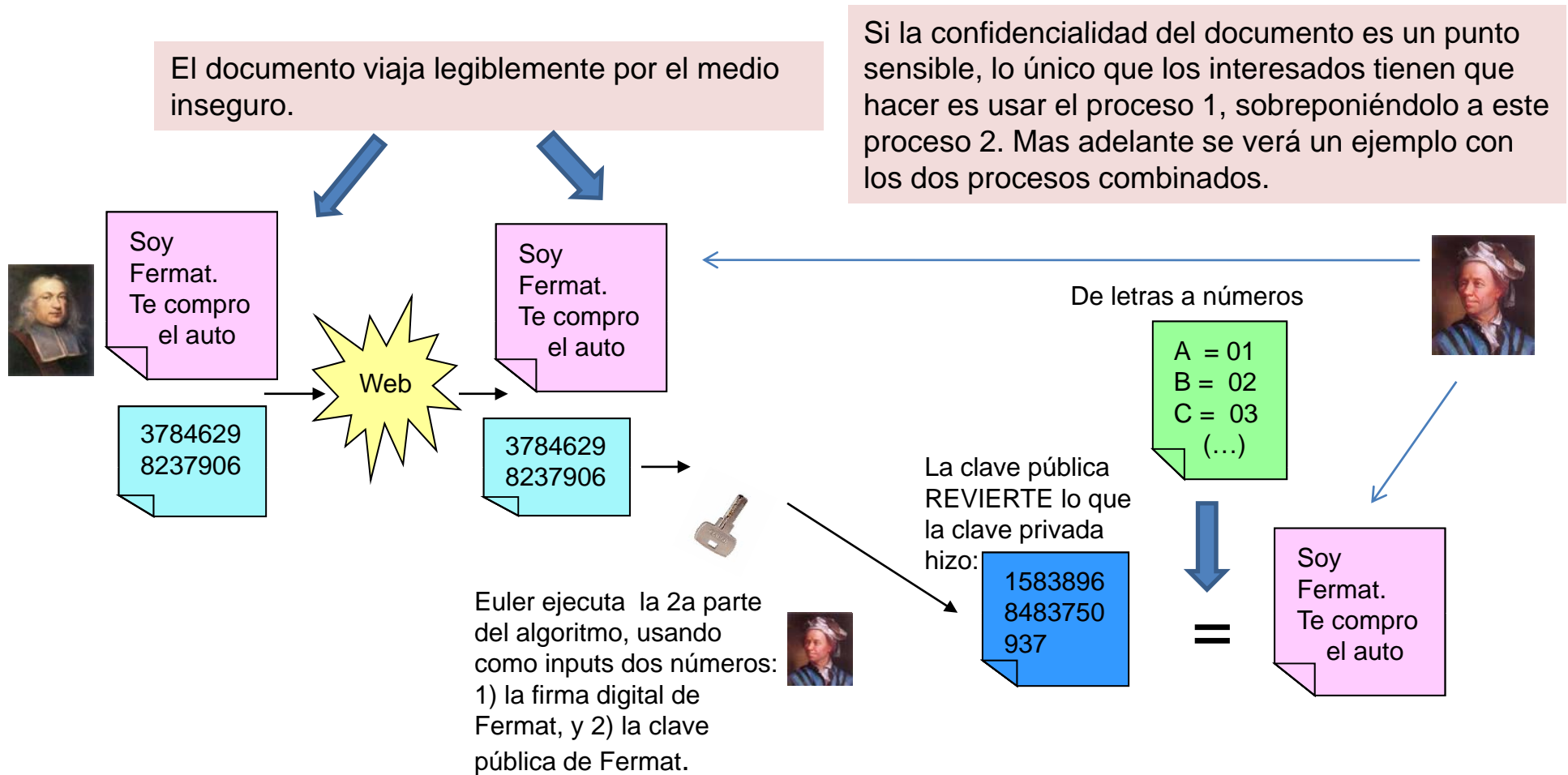


Dos modalidades de firmas electrónicas que **no** son firmas digitales.

Nota 2 sobre el proceso 2: permite detectar suplantaciones

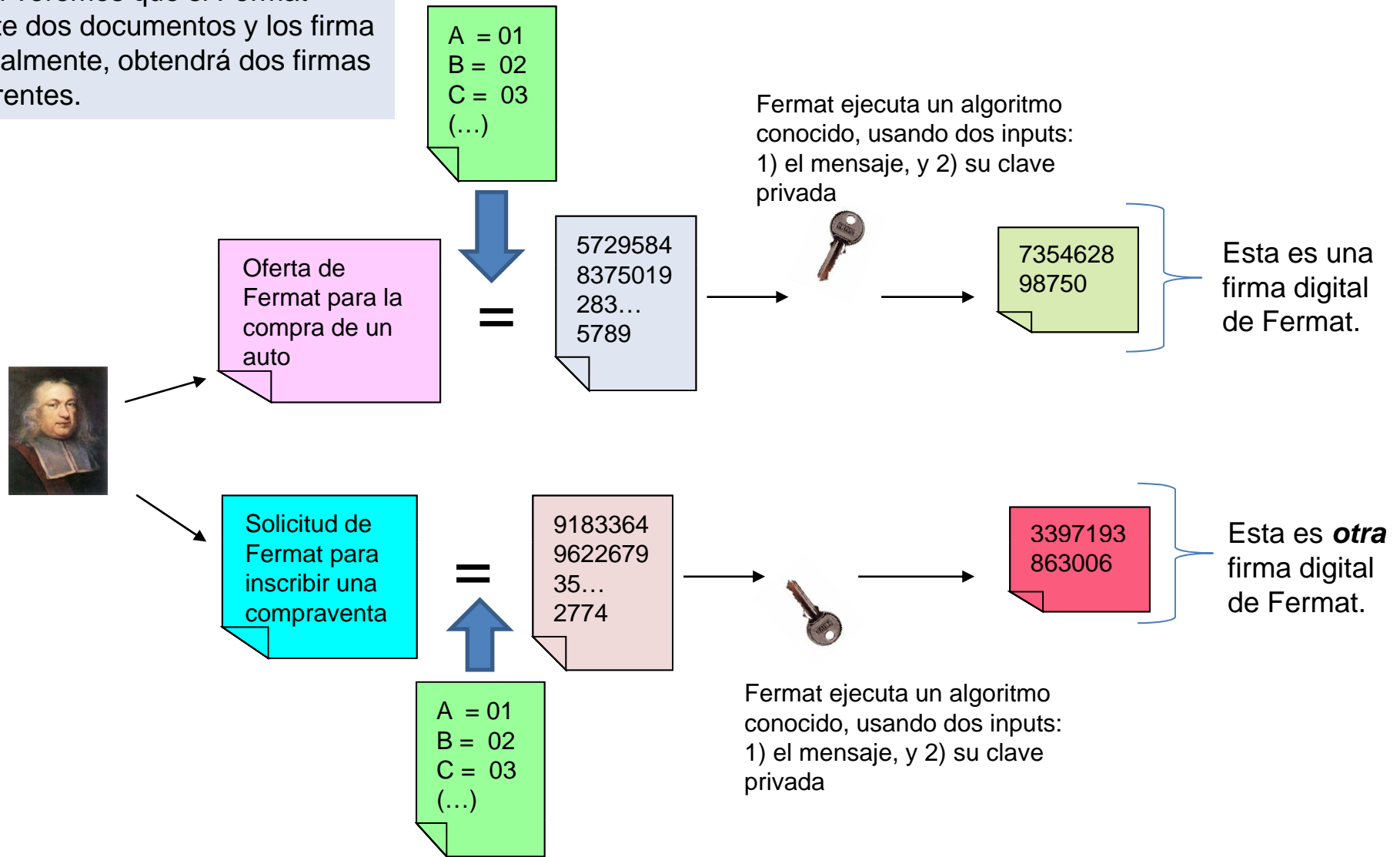


Nota 3 sobre el Proceso 2: no pretende garantizar la confidencialidad de la información transmitida



Nota 4 sobre el Proceso 2: a diferencia de la firma manuscrita, la “firma digital” de Fermat NO es un elemento constante, sino que cambia con cada documento que Fermat produce.

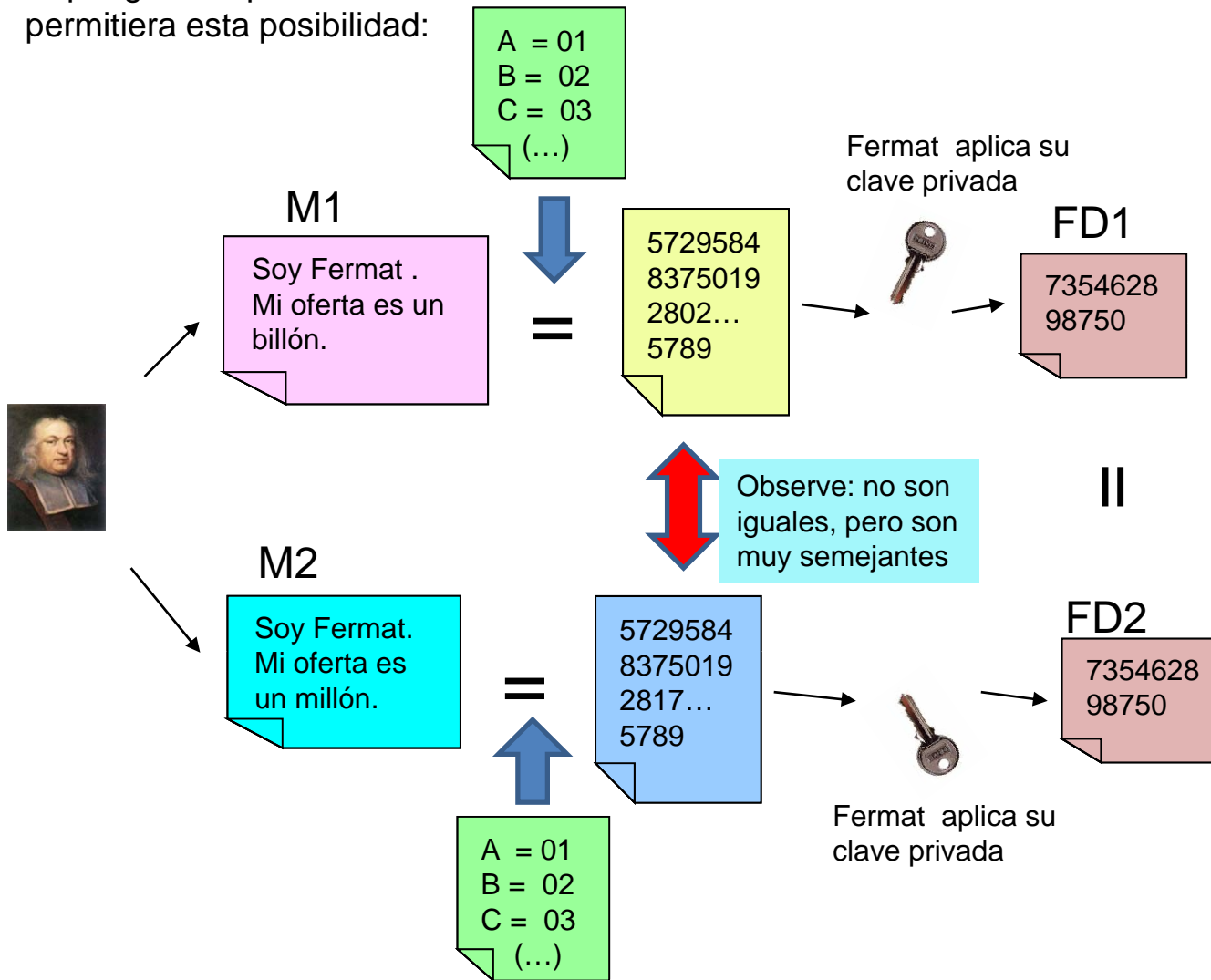
Aquí veremos que si Fermat emite dos documentos y los firma digitalmente, obtendrá dos firmas diferentes.



Lo que sí es constante, lo que no cambia es el par de claves que Fermat tiene.

Nota 5. Consecuencias muy negativas de una eventual colisión de dos firmas digitales de Fermat

Supongamos que el sistema permitiera esta posibilidad:

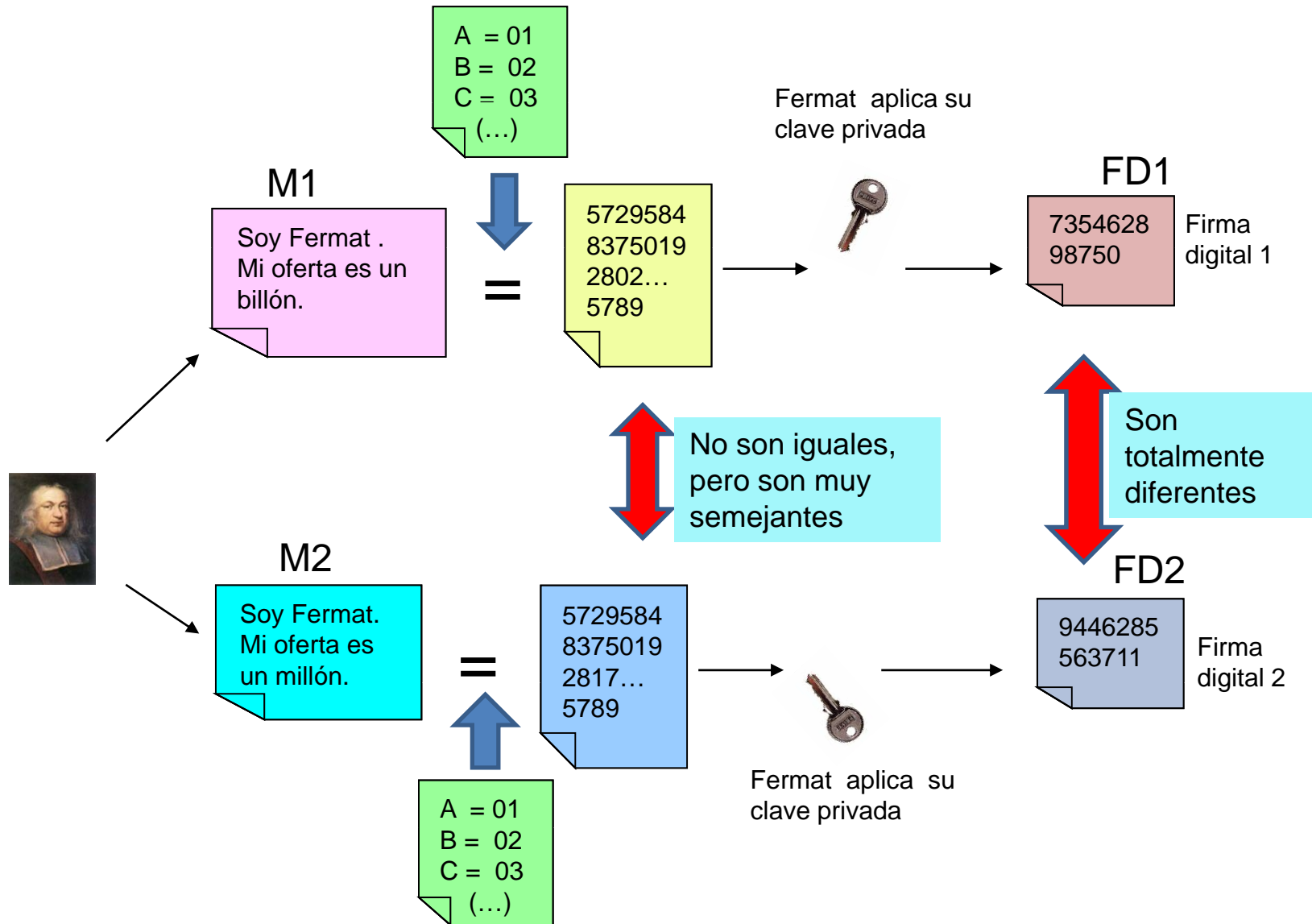


Secuencia de hechos.

1. Fermat envía M1 con FD1.
2. Fermat se arrepiente de M1.
3. Fermat envía M2, que tiene FD2 igual a FD1.
4. Euler le exige cumplir M1.
5. Fermat dice que sólo envió M2.
6. Euler demuestra ante el Juez que, aplicando la clave pública de Fermat sobre FD1, se obtiene M1.
7. Fermat demuestra ante el Juez que, aplicando su clave pública sobre FD1, también se obtiene M2 (la única oferta que el reconoce).

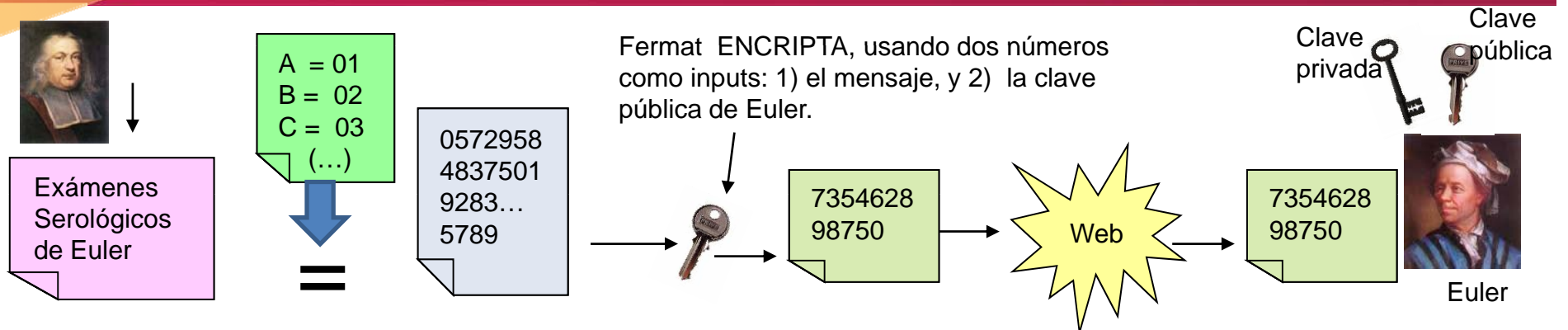
8. El Juez no tendría forma de saber si Fermat envió M1 y M2 o si (como el dice) sólo envió M2. Y por tanto no podría obligarlo a cumplir M1.

Nota 5 (continuación).- Afortunadamente la matemática detrás de la criptografía asimétrica tiene como consecuencia que, aun cuando dos números M1 y M2 (los mensajes originales) estén muy próximos el uno al otro, los valores resultantes FD1 y FD2 (las firmas digitales) serán muy diferentes.



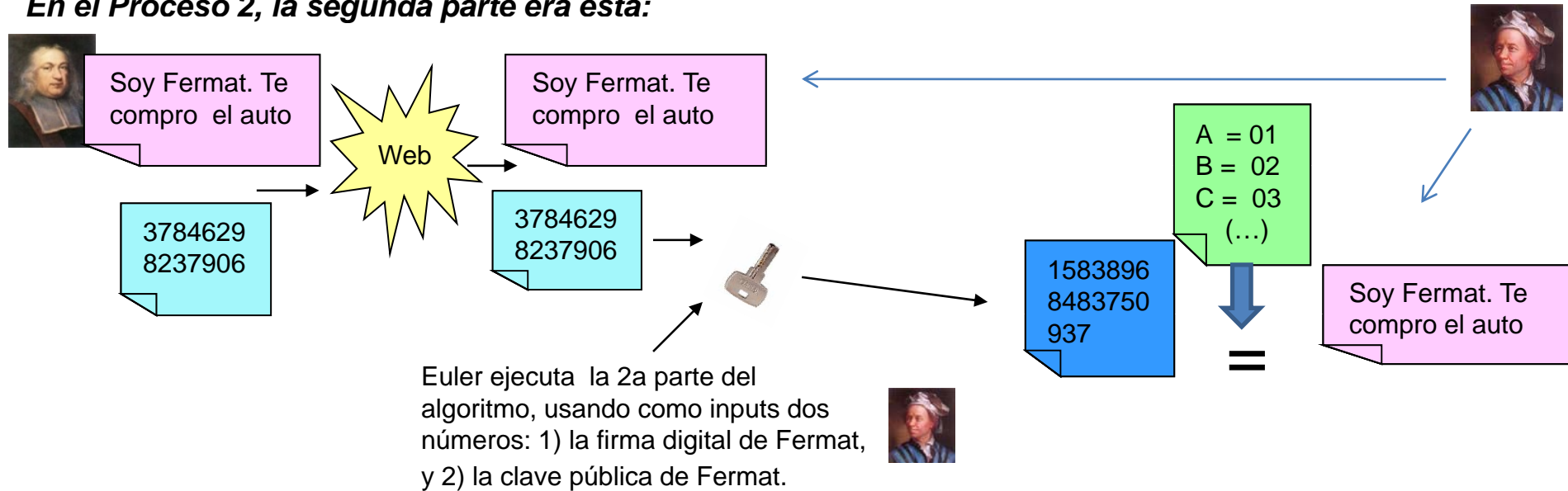
¿Todo bien hasta aquí ?

En el Proceso 1, la primera parte era esta:



Pregunta fundamental: ¿Cómo sabe Fermat que esa clave pública efectivamente pertenece a Euler?

En el Proceso 2, la segunda parte era esta:



Pregunta fundamental: ¿Cómo sabe Euler que esa clave pública efectivamente pertenece a Fermat?

El ataque del "hombre en el medio"

Fermat.
Clave pública = 20.



Caín.
Clave pública = 17.



Euler.
Clave pública = 13.



1. Hola, Euler, soy Fermat.
Manda tu clave pública.
La mía es 20.

Mensaje interceptado

Cambiaré el mensaje.
2. "Hola, Euler, soy Fermat.
Manda tu clave pública.
La mía es 17".

3. Hola, Fermat. Recibí
tu mensaje. Mi
clave pública es 13.

Mensaje interceptado

¡Bien!
Ahora
engañaré a
Fermat

4. "Hola, Fermat, aquí
Euler. Mi clave pública es 17".

5. Fermat encripta un
mensaje privado
con 17.

Mensaje interceptado

6. Caín descifra el
mensaje, lee y lo vuelve
a encriptar, pero con 13.

7. Euler descifra el
mensaje. Crea respuesta
privada y la encripta
con 17.

Mensaje interceptado

8. Caín descifra el
mensaje, lee y vuelve a
encriptar, pero con 20.

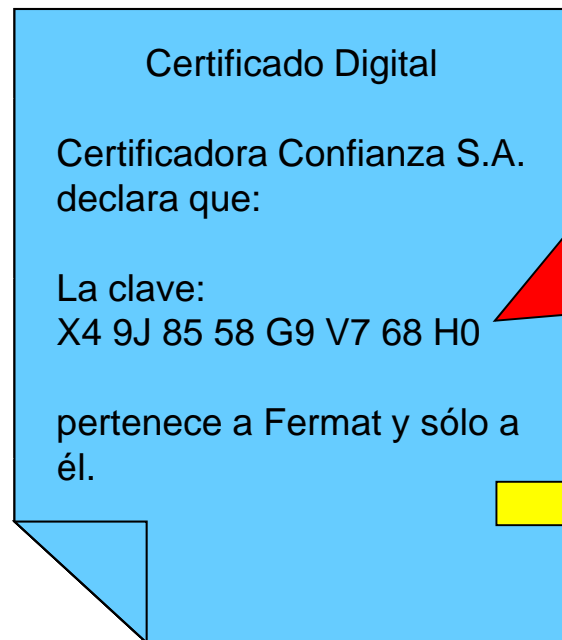
Concepto de "certificado digital"

Un certificado digital es un archivo electrónico en donde una organización digna de confianza declara que cierta clave (un número) está asignado exclusivamente a cierta persona específica.



(La clave privada está alojada en la PC de F. y bajo su control exclusivo)

Clave privada de Fermat:
59 J4 P3 41 86 81 M7.



Vinculación matemática entre las dos claves

En otras palabras:

Declaración de Confianza S.A.

La clave pública de Fermat, con la cual se podrá verificar la autoría de los documentos que emita y hacerle responder por ellos, es la siguiente:

X4 9J 85 58 G9 V7 68 H0

Generación del certificado digital

1. Euler genera sus dos claves con un programa idóneo



Clave privada:
"clave 1".



Clave pública:
"clave 2".

2. Euler envía 3 cosas a una entidad de registro:

clave 2



Documento 1:

Solicitud para obtener un certificado digital

Documento 2:

La misma solicitud, cifrada con la clave 1, y por tanto sólo descifrable con la clave 2.

Entidad de registro ER



3. La ER aplica la clave 2 al documento 2 para verificar si fue cifrado con la clave 1:



Solicitud cifrada

4. Resultado:

Solicitud para obtener un certificado digital

Al obtener un texto igual al documento 1, la ER verificó que Euler tiene la única clave que hace juego con la clave 2.

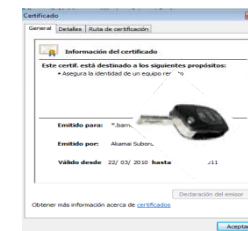
Por otra parte, la ER también verifica que el recurrente no sea un impostor que se hace pasar por Euler.

5. La ER informa a la Entidad certificadora que la solicitud de Euler es atendible.

Entidad de certificación EC



6. La EC genera un certificado digital donde da fe que la clave 2 es la clave pública de Euler.



Declaración de Confianza S.A.

La clave pública de Fermat, con la cual se podrá verificar la autenticidad y el carácter no repudiable de sus firmas digitales, es la siguiente:

X4 9J 85 58 G9 V7 68 H0

¿Cómo podemos obligar a la certificadora Confianza S.A. a responder por esta declaración suya?



¿Cómo podemos eliminar la posibilidad de que más tarde desconozca su declaración?

Respuesta: exigiendo que la firme digitalmente:

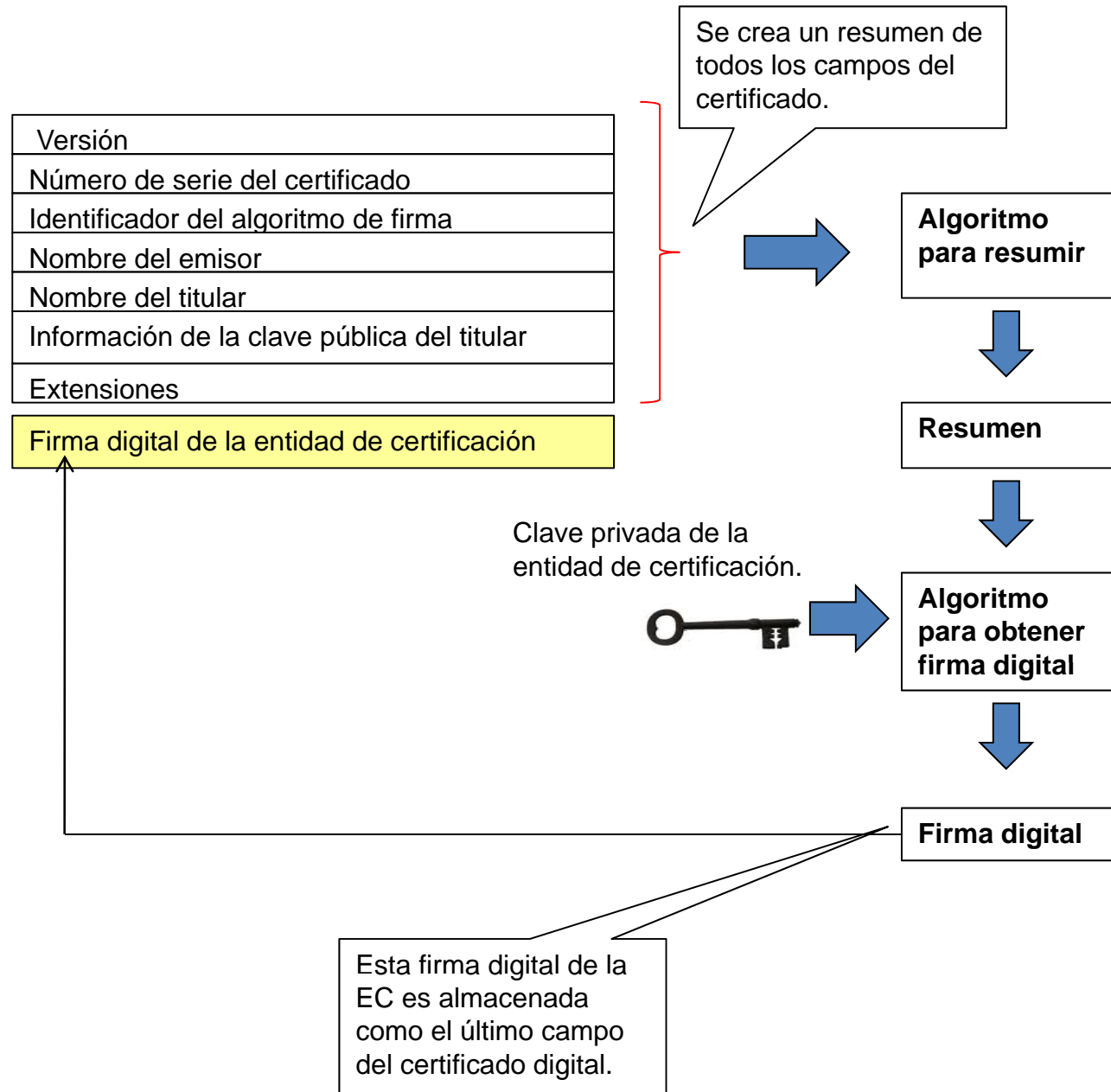
Declaración de Confianza S.A.

La clave pública de Fermat, con la cual se podrá verificar la autenticidad y el carácter no repudiable de sus firmas digitales, es la siguiente:

X4 9J 85 58 G9 V7 68 H0

Yo, Confianza S.A., lo firmo:
58 9E 59 7B 5S I2 90

Creación de la firma digital de la certificadora en un certificado



Contenido del certificado digital

En la presentación del certificado en la pantalla (versión 3 del X.509) la firma de la certificadora NO queda a la vista de los usuarios finales. Los principales campos visibles del certificado son los siguientes:

Algoritmo de Firma.- Indica cuál es el proceso matemático seguido por la certificadora para cifrar este certificado con su clave privada (ver RFC 2459).

Entidad certificadora que lo emite

Período de validez

Nombre del titular del certificado
(en este caso, una página web)

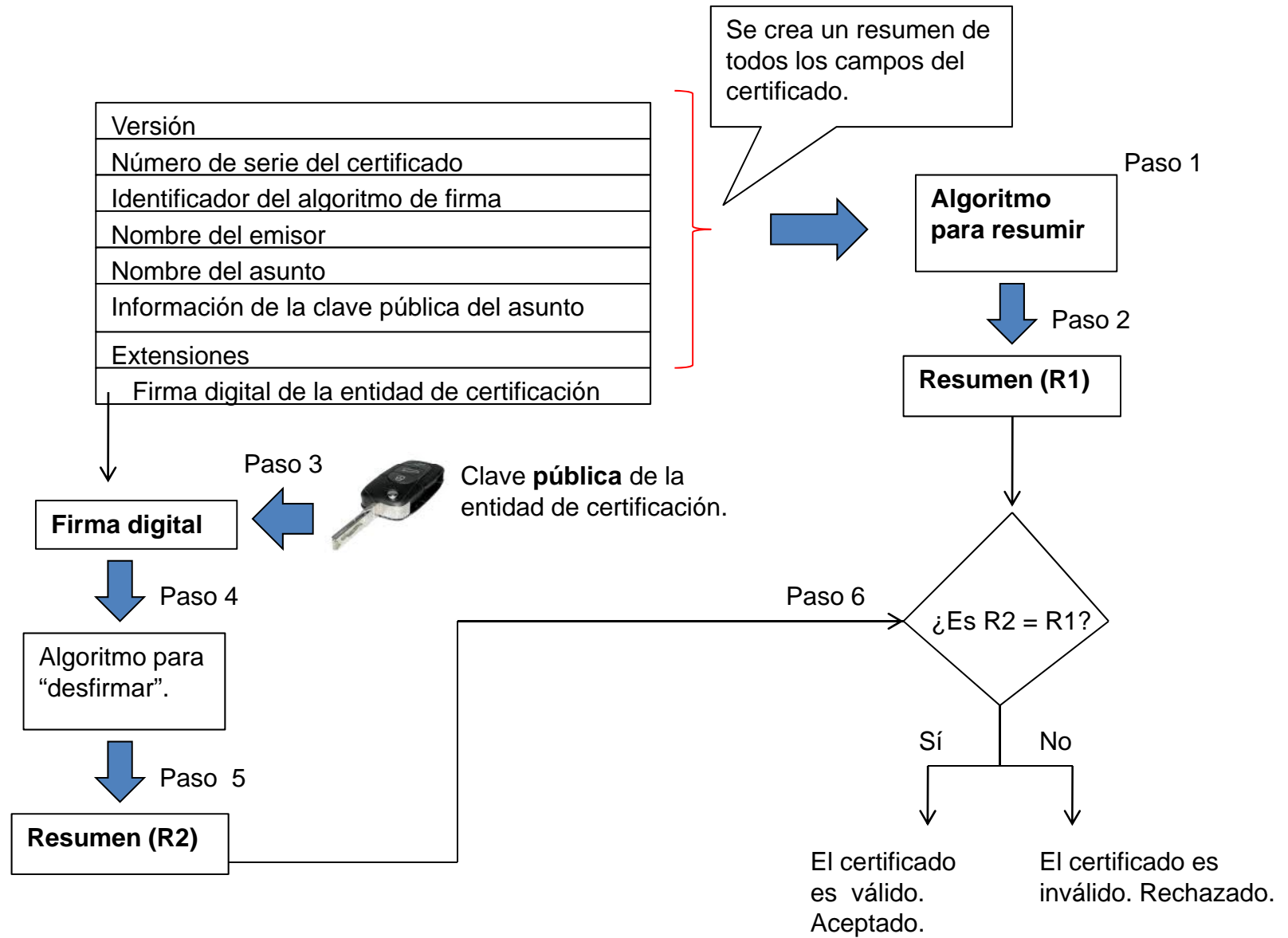
Vía de acceso a la Lista de
Certificados Revocados.

Clave pública del titular

Campo	Valor
Número de serie	01 00 00 00 00 01 27 86 1e 9f...
Algoritmo de firma	sha1RSA
Emisor	Akamai Subordinate CA 3, Aka...
Válido desde	Lunes, 22 de Marzo de 2010 0...
Válido hasta	Martes, 22 de Marzo de 2011 ...
Asunto	*.barnesandnoble.com, NEW ...
Clave pública	RSA (1024 Bits)
Puntos de distribución CRL	[1]Punto de distribución CRL: ...

```
30 81 89 02 81 81 00 ba 2a 55 07 b7 26 4d
3c 4d b8 01 d6 70 7b a5 b0 bd 72 0d b8 e2
c2 83 55 4a 24 64 58 8c ce f0 f2 0e af 97
74 1c 10 9e 8b f3 6a 46 62 9a a8 94 c5 e1
ef 10 d4 52 9d 73 80 61 5b 73 55 29 29 96
89 a2 c5 a3 76 2e 9c 22 cb 95 cb ce f9 b7
4e 88 15 34 ea a0 3c f1 cd ce 2e 6d 9b bd
d2 72 42 f8 42 a1 41 8a c0 d4 ac a4 87 1b
f4 a8 5c b9 b9 30 1e 74 af 54 e5 d7 e7 15
```

Verificación de la firma digital de la certificadora en un certificado

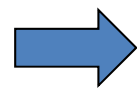


Verificación de la firma de la certificadora en un certificado

1. Aquí hay algo en donde debemos detenernos:

Versión
Identificador del certificado
Algoritmo de firma
Nombre del asunto
Información de la clave pública del asunto
Extensiones
Firma digital de la entidad de certificación

Se crea un resumen de todos los campos del certificado.



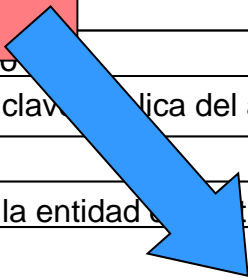
Algoritmo para resumir

Paso 1



Paso 2

Resumen (R1)



Firma digital

Paso 3




Paso 4

Algoritmo para "desfirmar".



Paso 5

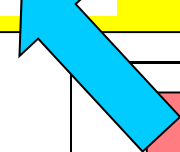
Resumen (R2)

 **Clave pública de la entidad de certificación.**

Paso 6

¿Es R1 = R2?

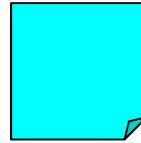
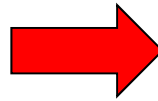
2. ¿Cómo nos consta que, en efecto, esta clave le pertenece a la entidad de certificación? ¿Cómo estar seguros de que no ocurrió "el ataque del hombre intermedio"?



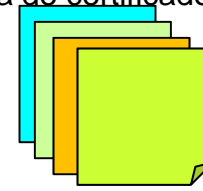
Verificación de la autenticidad de un certificado



Euler



Cadena de certificados digitales



Fermat

5 certificados: de Euler y de las certificadoras D, C, B y A.

El software navegador de Fermat revisa la cadena de certificados, hasta encontrar uno al cual reconozca.



D certifica que la clave pública de Euler es 493



C certifica que la clave pública de D es 199.



B certifica que la clave pública de C es 362.



A certifica que la clave pública de B es 104.



A certifica que la clave pública de A es 681.

La autenticidad de cada certificado es respaldada por un certificado anterior, cuya autenticidad, a su vez, es respaldada por otro anterior... hasta que llegamos a una organización que auto-genera su propio certificado.

Opciones posibles

1. Fermat usa un navegador que reconoce el certificado raíz de A.
2. El certificado de Fermat, o alguno de su propia cadena, fue emitido por alguna de las certificadoras D, C, B, A.
3. Fermat usa un navegador que no reconoce a la certificadora "A", y además su propia cadena de certificados no tiene ninguna certificadora en común con la de Euler.

→ El software navegador de Fermat reconocerá la autenticidad del certificado de Euler.

→ El software navegador de Fermat no reconocerá credibilidad al certificado de Euler.

Google - Windows Internet Explorer

http://www.google.com.pe/

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Google

Página Seguridad Herramientas

La Web [Imágenes](#) [Videos](#) [Noticias](#) [Libros](#) [Traductor](#) [Gmail](#) [Más](#)

[iGoogle](#) [Configuración de la búsqueda](#) [Acceder](#)

Google

Perú

Buscar con Google Voy a tener suerte

¡Nuevo! Explora [Google Flu Trends](#) para Perú

Google.com.pe ofrecido en: [Quechua](#)

[Programas de publicidad](#) [Soluciones Empresariales](#) [Todo acerca de Google](#) [Go](#)

© 2010 - [Privacidad](#)

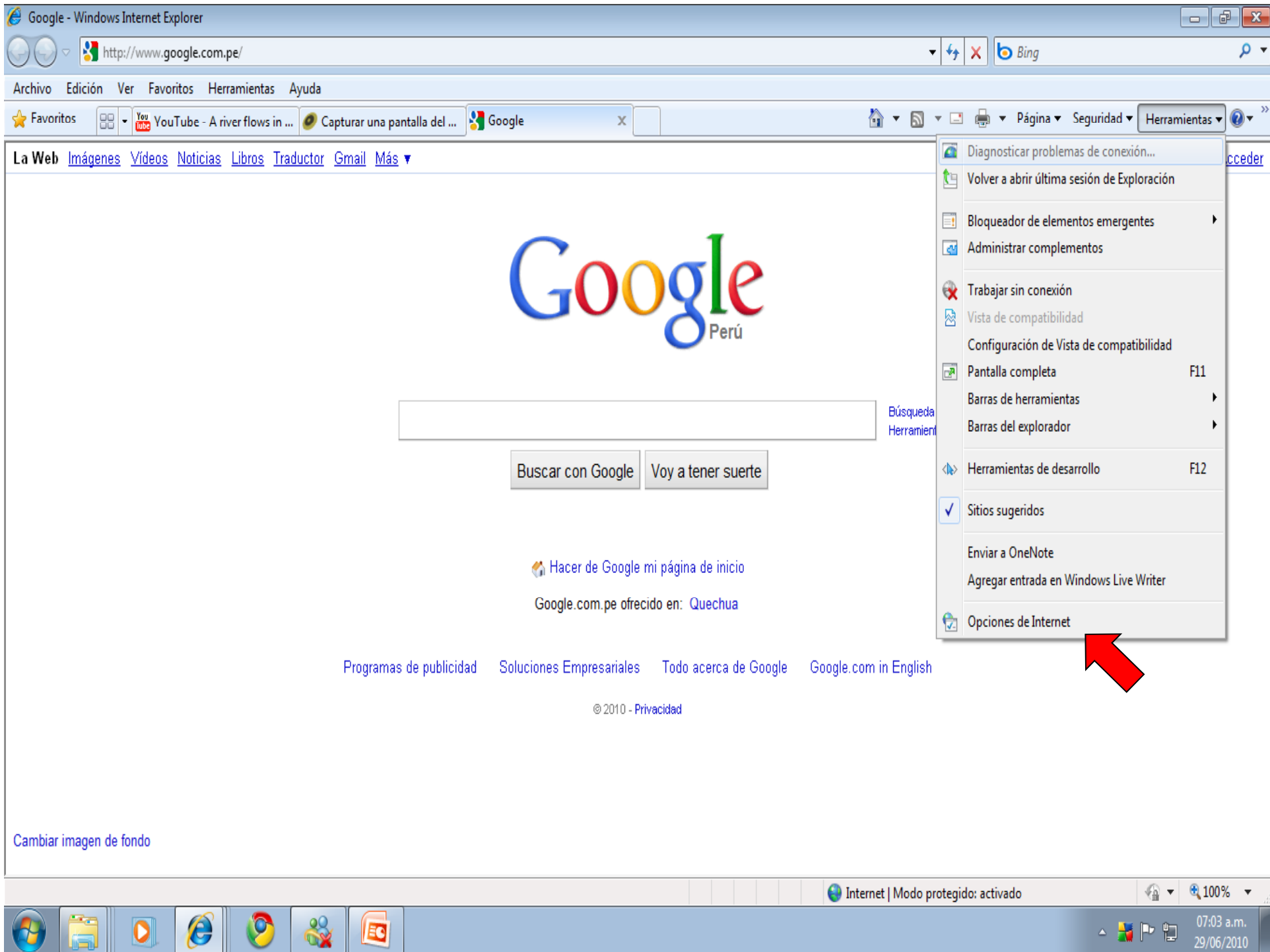
[Cambiar imagen de fondo](#)

Internet | Modo protegido: activado

100%

A modo de ejemplo, veamos el Directorio de “entidades de certificación intermedias” y de “entidades de certificación raíz” que forma parte del software navegador más usado, Internet Explorer.

Supongamos que Fermat está usando Internet Explorer. Cuando él reciba un certificado de Euler que, en última instancia, se sustente en alguna de las entidades registradas en aquel Directorio, el navegador reconocerá de inmediato a dicho certificado como veraz.



Google - Windows Internet Explorer

http://www.google.com.pe/

Archivo Edición Opciones de Internet

Conexiones Programas Opciones avanzadas

General Seguridad Privacidad Contenido

Página principal

Para crear pestañas de página principal, escriba cada dirección en una línea independiente.

<http://search.conduit.com/?SearchSource=10&ctid=>

Usar actual Usar predeterminada Usar página en blanco

Historial de exploración

Elimine archivos temporales, historial, cookies, contraseñas guardadas e información de formularios web.

Eliminar el historial de exploración al salir

Eliminar... Configuración

Búsqueda

Cambie las opciones predeterminadas de búsqueda. Configuración

Pestañas

Cambie la forma en que las páginas web se muestran en las pestañas. Configuración

Apariencia

Colores Idiomas Fuentes Accesibilidad

Aceptar Cancelar Aplicar

Google Perú

Búsqueda avanzada Herramientas del idioma

Buscar con Google Voy a tener suerte

Hacer de Google mi página de inicio

Google.com.pe ofrecido en: Quechua

Soluciones Empresariales Todo acerca de Google Google.com in English

© 2010 - Privacidad

Cambiar imagen de fondo

Internet | Modo protegido: activado

100%

07:09 a.m.
29/06/2010

Opciones de Internet

Conexiones | Programas | Opciones avanzadas

General | Seguridad | Privacidad | Contenido

Control parental

Controle el contenido de lo que se puede ver en Internet. [Control parental](#)

Asesor de contenido

Las clasificaciones le ayudan a controlar el tipo de contenido de Internet que se puede ver con este equipo.

[Habilitar...](#) [Configuración](#)

Certificados

Use certificados para las conexiones cifradas y para fines de identificación.

[Borrar estado SSL](#) [Certificados](#) [Editores](#)

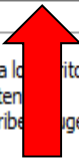
Autocompletar

Autocompletar almacena lo escrito en páginas web para intentar anticiparse a lo que escribe y sugerir posibles coincidencias. [Configuración](#)

Fuentes y Web Slices

Las fuentes y las Web Slices proporcionan contenido actualizado de sitios web, el cual puede leerse en Internet Explorer y en otros programas. [Configuración](#)

[Aceptar](#) [Cancelar](#) [Aplicar](#)



Búsqueda avanzada
Herramientas del idioma

con Google [Voy a tener suerte](#)

Explora [Google Flu Trends](#) para Perú

gle.com.pe ofrecido en: [Quechua](#)

[Empresariales](#) [Todo acerca de Google](#) [Google.com in English](#)

© 2010 - [Privacidad](#)

[Cambiar imagen de fondo](#)

Opciones de Internet

Conexiones Programas Opciones avanzadas
General Seguridad Privacidad Contenido

Control parental

SSL Certificados Editores

Configuración

Configuración

Aceptar Cancelar Aplicar

Certificados

Propósito planteado: <Todos>

Personal Otras personas Entidades de certificación intermedias Entidades de certificación

Emitido para	Emitido por	Fecha de...	Nombre descriptivo
Microsoft Certificat...	Microsoft Root Certifi...	02/04/2019	<ninguno>
Microsoft Internet ...	GTE CyberTrust Globa...	19/02/2011	<ninguno>
Microsoft Secure S...	Microsoft Internet Au...	19/02/2011	<ninguno>
Microsoft Windows ...	Microsoft Root Authority	31/12/2002	<ninguno>
MSN Content Auth...	MSN Content PCA	24/02/2010	<ninguno>
MSN Content Auth...	MSN Content PCA	09/02/2017	<ninguno>
MSN Content PCA	Microsoft Root Certifi...	09/02/2017	<ninguno>
Root Agency	Root Agency	31/12/2039	<ninguno>
VeriSign Class 3 Co...	Class 3 Public Primary ...	20/05/2019	<ninguno>

Importar... Exportar... Quitar Opciones avanzadas

Propósitos planteados del certificado

Firma de listas de confianza de Microsoft, Firmante de listas de raíz

Ver

Obtener más información acerca de [certificados](#)

Cerrar

Estos los certificados raíces que el navegador de Windows (Internet Explorer) reconoce como totalmente confiables.



¡Te veré en la Corte!

1. Fermat envía una oferta económica a Euler, firmada digitalmente.



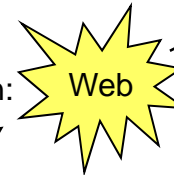
T.L.

F.D.

2. Euler recibe los documentos, los graba y comunica su aceptación.



3. Fermat recibe y conoce la aceptación: se perfecciona el contrato



F.D.



4. Fermat informa a Euler, en texto legible y en texto cifrado con su clave privada, que recibió su aceptación.

5. Tiempo después, Fermat pretende evadir sus obligaciones

¡Todo es nulo!



6. Euler recurre al Juez y presenta los documentos electrónicos que recibió de Fermat.



Fermat niega la autoría o el contenido o el acuse de recibo.



7. A requerimiento del Juez, la certificadora le envía el certificado digital de Fermat.



Clave Pública De Fermat



F.D.



clave pública de Fermat

Texto legible

F.D.



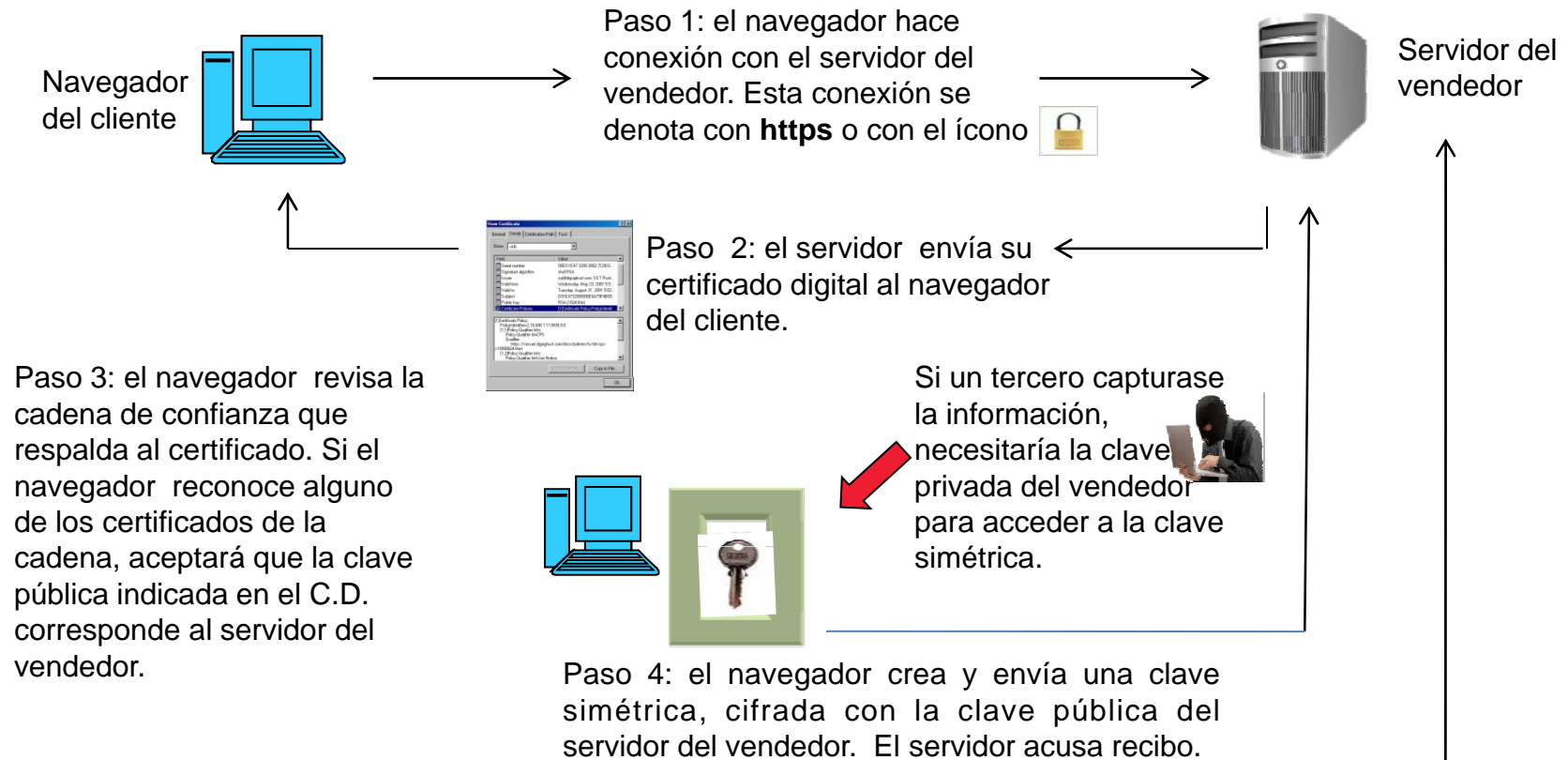
T.L.

8. El juez aplica la clave pública de Fermat a las dos firmas digitales y consigue descifrarlas. Esto demuestra que: (1) la oferta y el acuse de recibo de la aceptación de la oferta fueron cifrados con la clave privada de Fermat; (2) ninguno de dichos documentos fue alterado por Euler o por terceros.

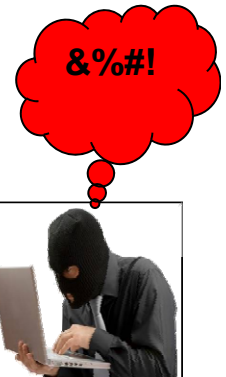
¡Así que todo es válido!



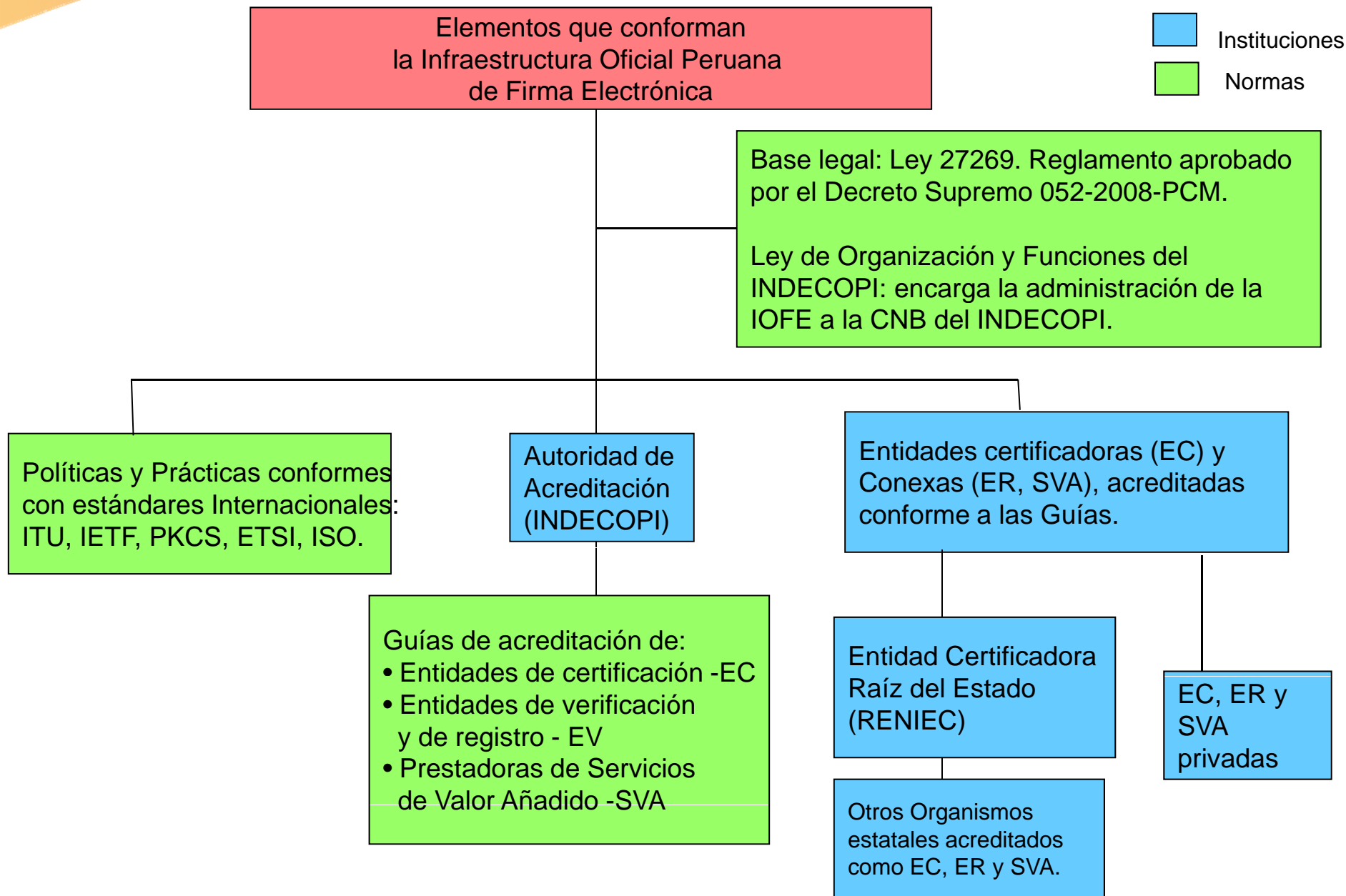
Secure Socket Layer (SSL): sustento de toda compra por Internet



¿Por qué en el Paso 4 el navegador del cliente crea una clave simétrica que será transmitida cifrada con la clave pública del servidor, en lugar de usar directamente dicha clave pública para transmitir, cifrada, la información privada del cliente? Por eficiencia (ver la técnica del "sobre digital").

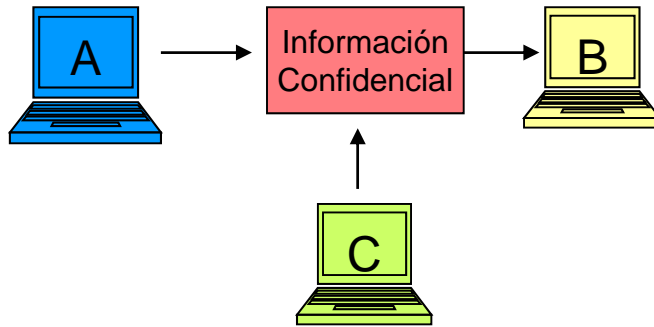


Marco legal para la certificación digital en el Perú



Recordemos los cuatro problemas identificados al principio

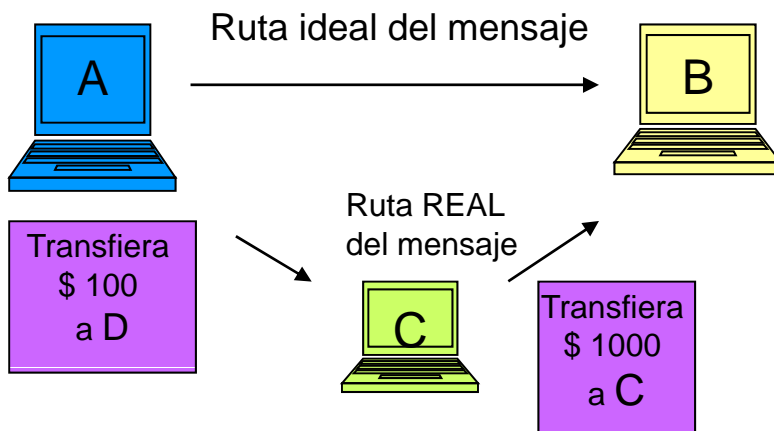
1. Espionaje



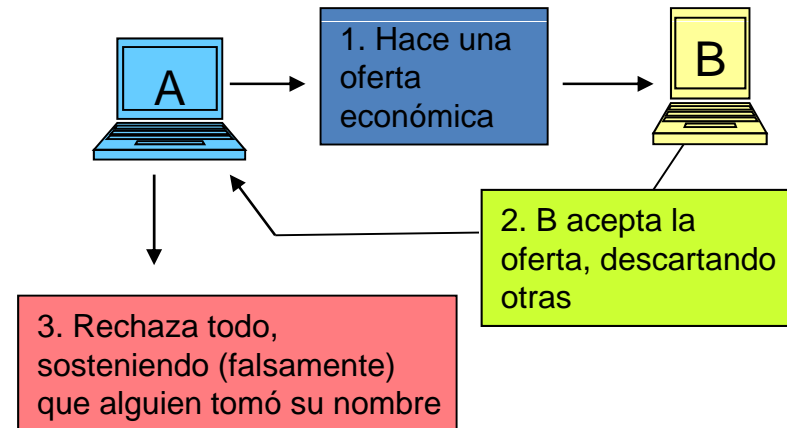
2. Suplantación de identidad



3. Adulteración de los documentos

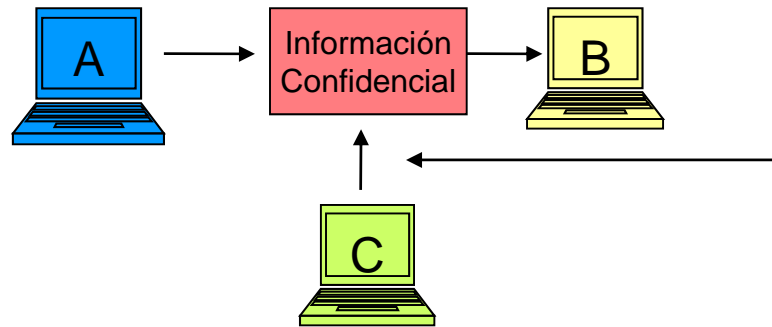


4. Negación maliciosa de documento propio



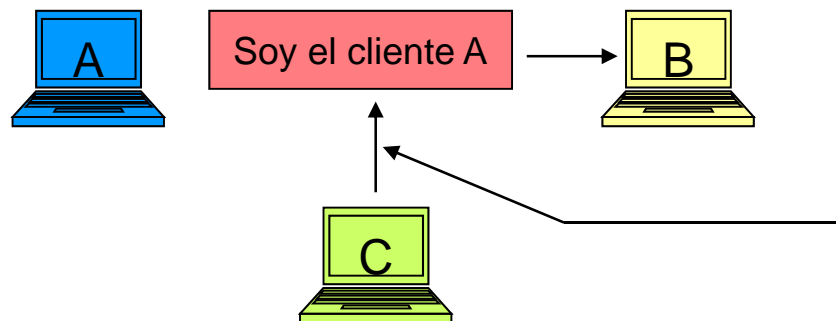
Solución a los problemas identificados al principio

1. Espionaje



Si "A" envía la información cifrada con la clave pública de "B", "C" no puede acceder a ella. Sólo podría descifrarla con la clave privada de "B".

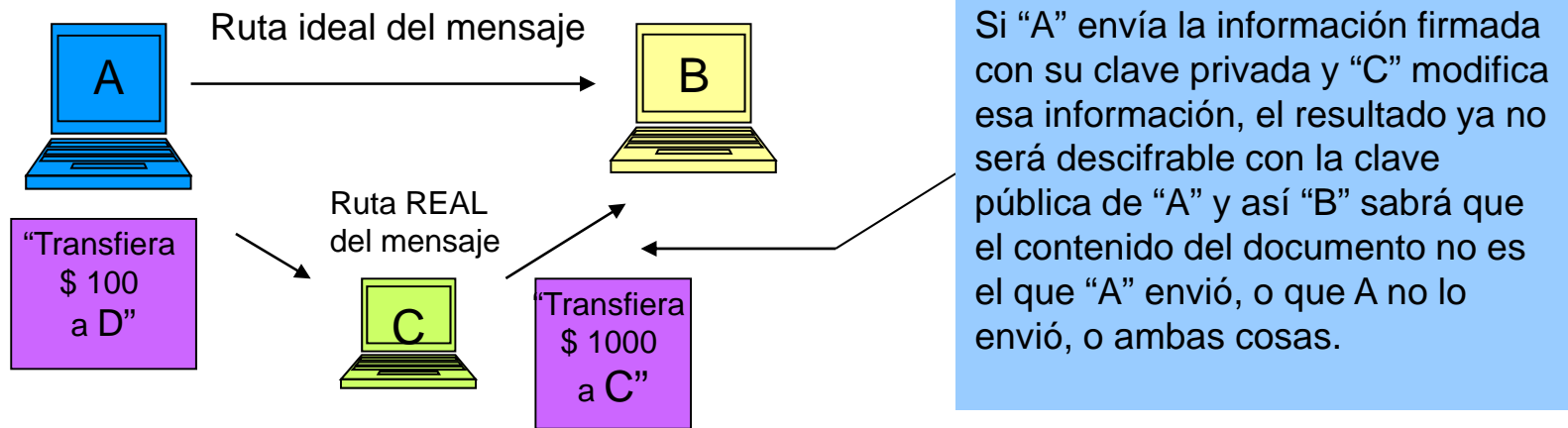
2. Suplantación de identidad



Si "B" exige a sus interlocutores que sus documentos lleven "firma digital" como garantía de autenticidad, "C" no puede hacerse pasar por "A" porque, para firmar digitalmente como si fuese "A", necesitaría la clave privada de "A".

Solución a los problemas identificados al principio (continuación)

3. Adulteración de los documentos



4. Negación maliciosa de documento propio

Si “A” envió su documento firmado digitalmente (vale decir, cifrado con su clave privada), “A” no podrá desentenderse del mismo ni atribuirlo a un tercero, pues la única clave que podrá descifrarlo será la clave pública de “A”, lo cual demostrará que fue cifrado con la clave privada de “A”.

