

# Seguridad y Alta Disponibilidad: Criptografía II



IES Gonzalo Nazareno  
**CONSEJERÍA DE EDUCACIÓN**

Jesús Moreno León

jesus.moreno.edu@  
juntadeandalucía.es

Septiembre 2012

---

Transparencias adaptadas del material del libro:  
Redes de computadores: un enfoque  
descendente basado en Internet,  
2ª edición. Jim Kurose, Keith Ross

Copyright 1996-2002.  
J.F Kurose y K.W. Ross.  
Todos los derechos reservados.



# Objetivos de la seguridad informática

---

- Confidencialidad
- Disponibilidad
- Integridad
- No repudio

¿Puede ayudarnos la criptografía a conseguir estos objetivos?

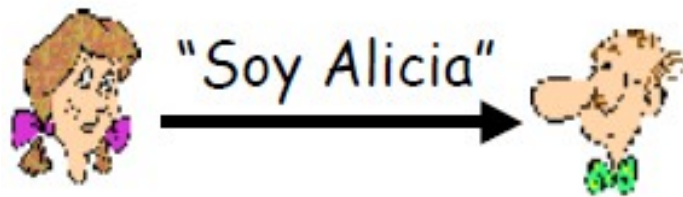


# Autenticación

---

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa1.0:** Alicia dice “Soy Alicia”



¿Escenario de fallo?



# Autenticación

---

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa1.0:** Alicia dice “Soy Alicia”



En una red Roberto no  
puede *ver* a Alicia  
Gertrudis simplemente dice  
que ella es Alicia



# Autenticación

---

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa2.0:** Alicia dice “Soy Alicia” en un paquete IP que contiene su dirección IP origen



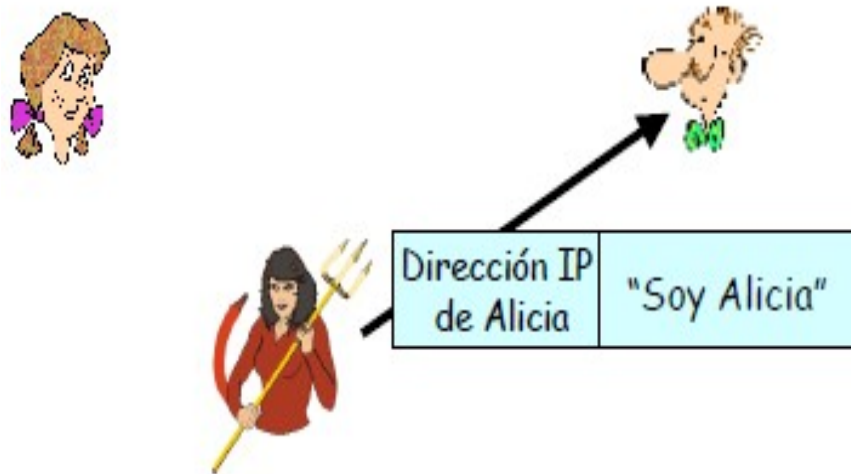
¿Escenario de fallo?

# Autenticación

---

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa2.0:** Alicia dice “Soy Alicia” en un paquete IP que contiene su dirección IP origen

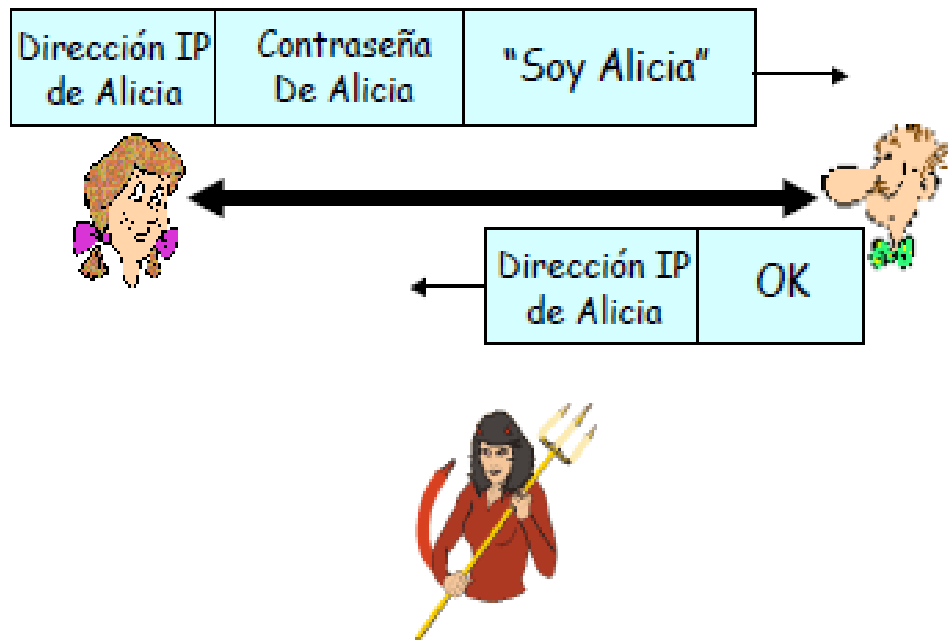


Gertrudis puede crear un paquete falso con la dirección IP de Alicia

# Autenticación

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa3.0:** Alicia dice “Soy Alicia” y envía su contraseña secreta para demostrarlo



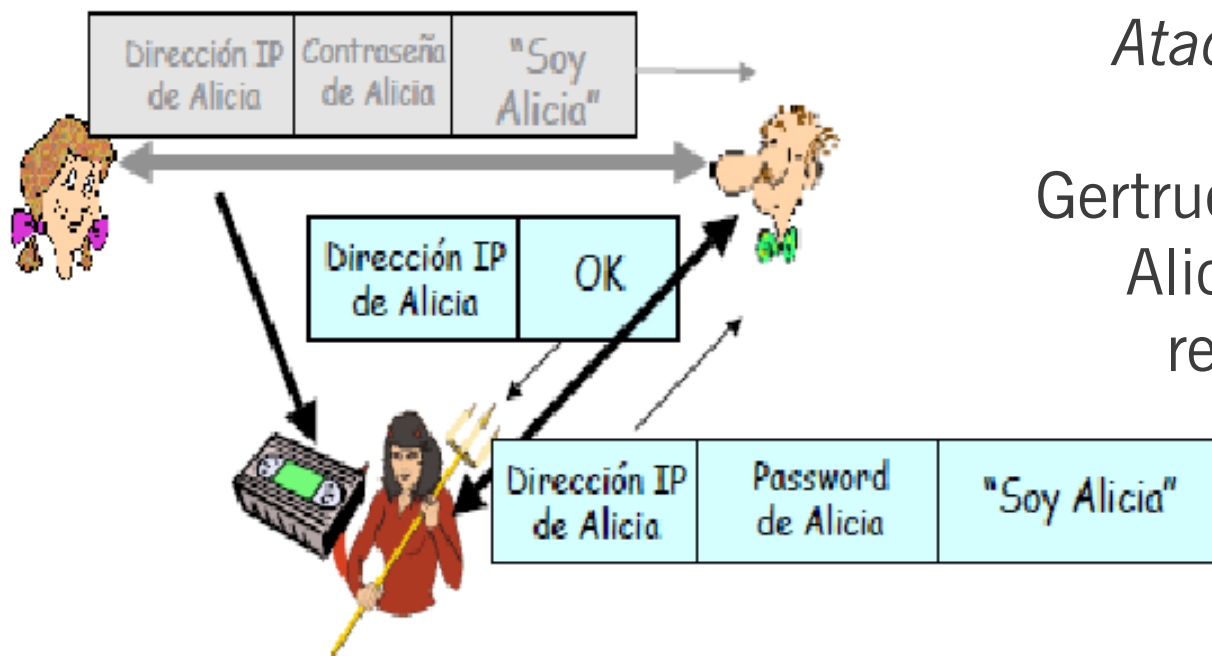
¿Escenario de fallo?



# Autenticación

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa3.0:** Alicia dice “Soy Alicia” y envía su contraseña secreta para demostrarlo

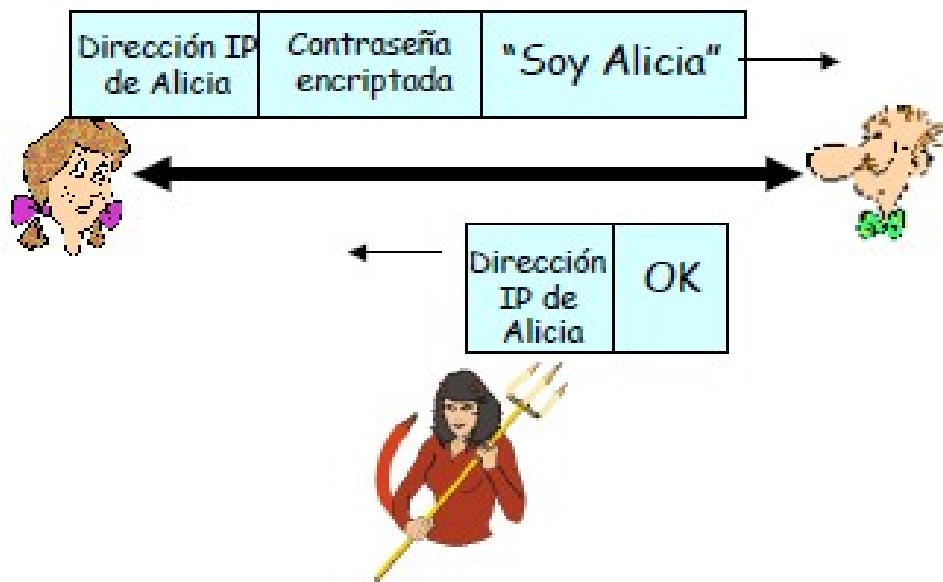


*Ataque de reproducción (replay):*  
Gertrudis graba el mensaje de Alicia y más tarde se lo reproduce a Roberto

# Autenticación

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa3.1:** Alicia dice “Soy Alicia” y envía su contraseña secreta encriptada para demostrarlo

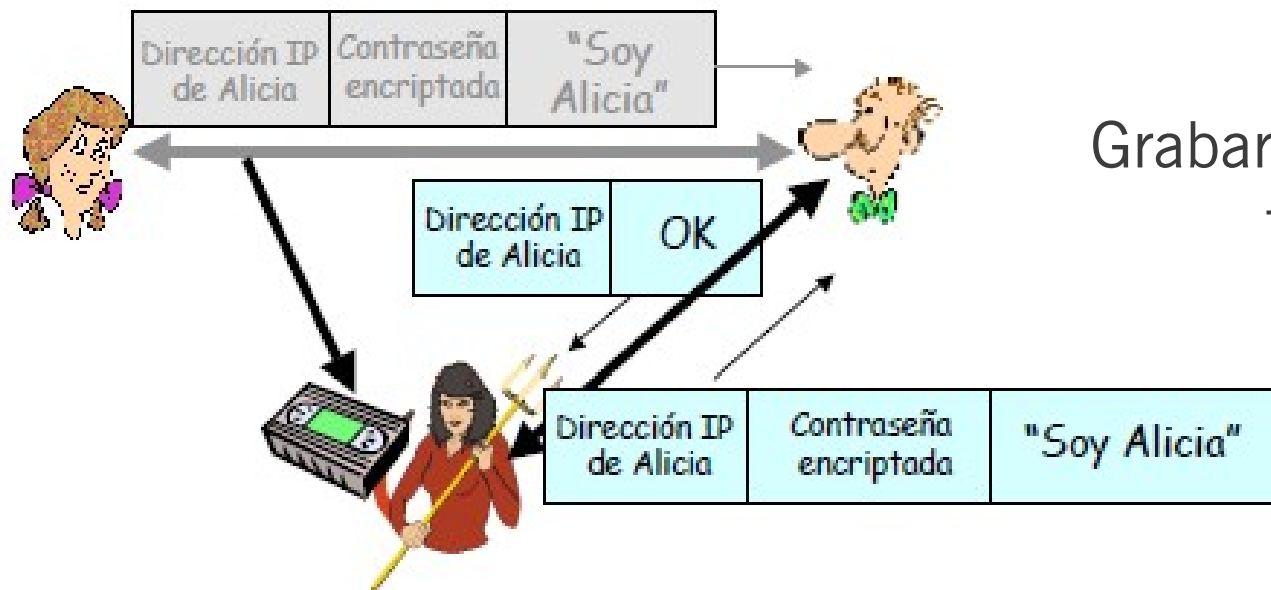


¿Escenario de fallo?

# Autenticación

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa3.1:** Alicia dice “Soy Alicia” y envía su contraseña secreta encriptada para demostrarlo

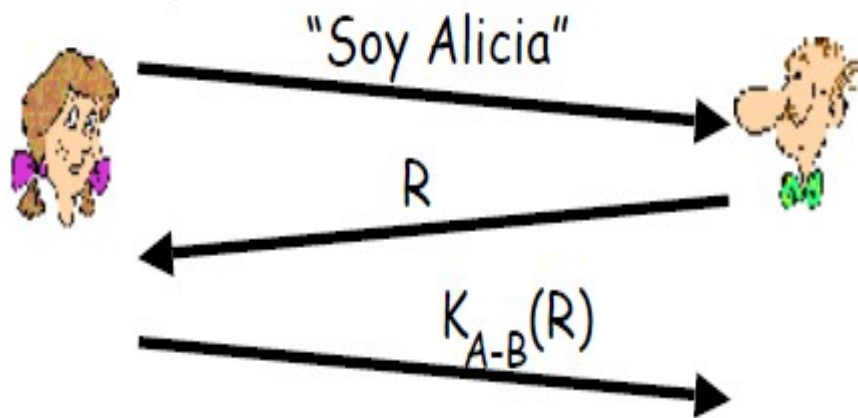


Grabar y reproducir sigue funcionando

# Autenticación

Objetivo: Roberto quiere que Alicia le *demuestre* su identidad

**Protocolo pa4.0:** Para evitar ataques de replay, Roberto le envía un número (nonce),  $R$ . Alicia debe devolver  $R$ , encriptado con una clave secreta compartida



Alicia *está en directo* y sólo ella conoce la clave secreta compartida, así que ella tiene que ser Alicia!

# Autenticación

Pa4.0 requiere una clave simétrica compartida previamente. ¿La podemos autenticar usando técnicas de clave pública?

**Protocolo pa5.0:** usa un número y criptografía de clave pública



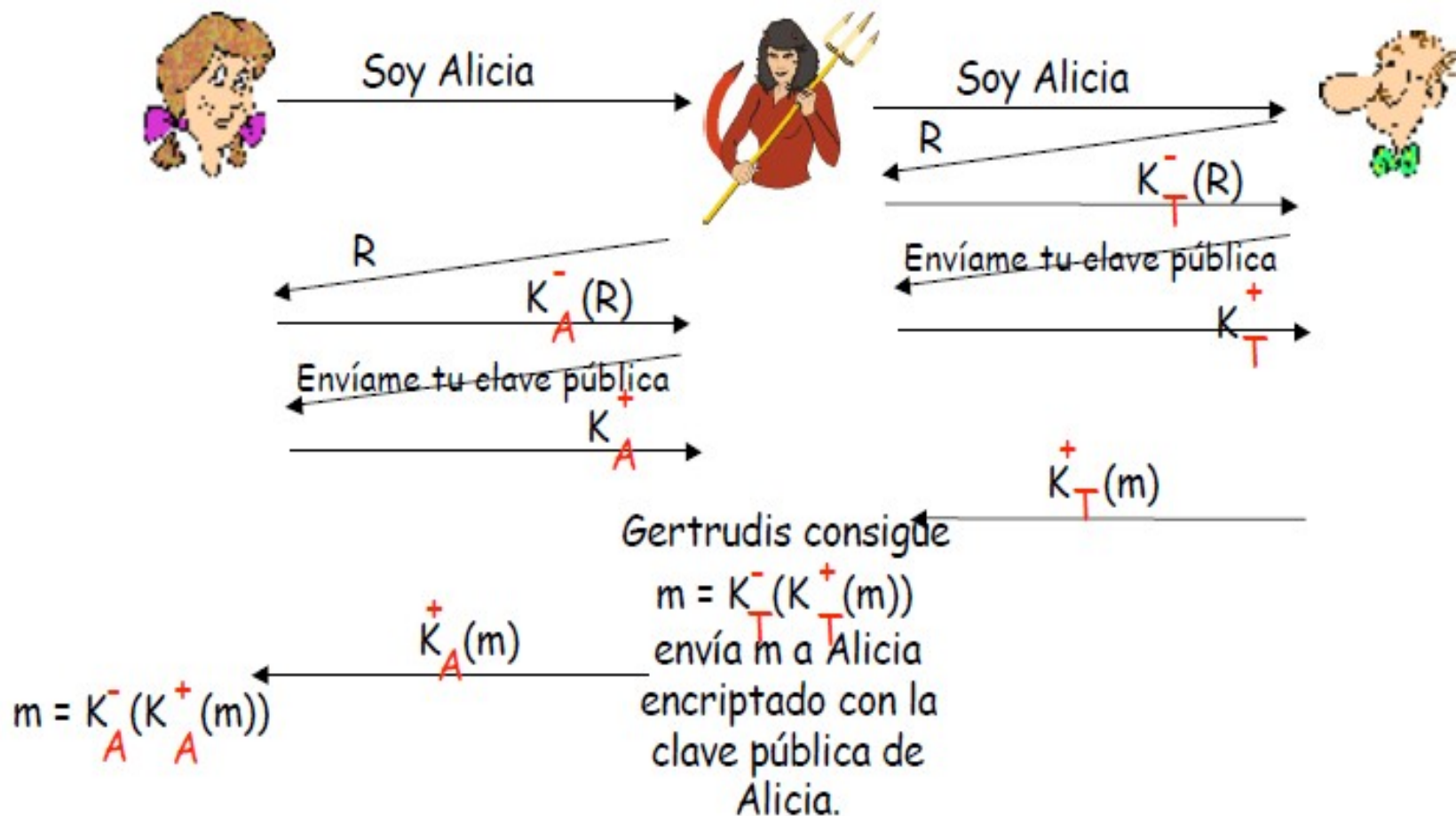
Roberto calcula  
 $K_A^+(K_A^-(R)) = R$   
y sabe que sólo Alicia  
puede tener la clave  
privada que encripta a  
 $R$ , esto es:

$$K_A^+(K_A^-(R)) = R$$

¿Escenario de fallo?

# Autenticación

Pa5.0 presenta un agujero de seguridad frente a ataques MITM



# Autenticación

---

Pa5.0 presenta un agujero de seguridad frente a ataques MITM

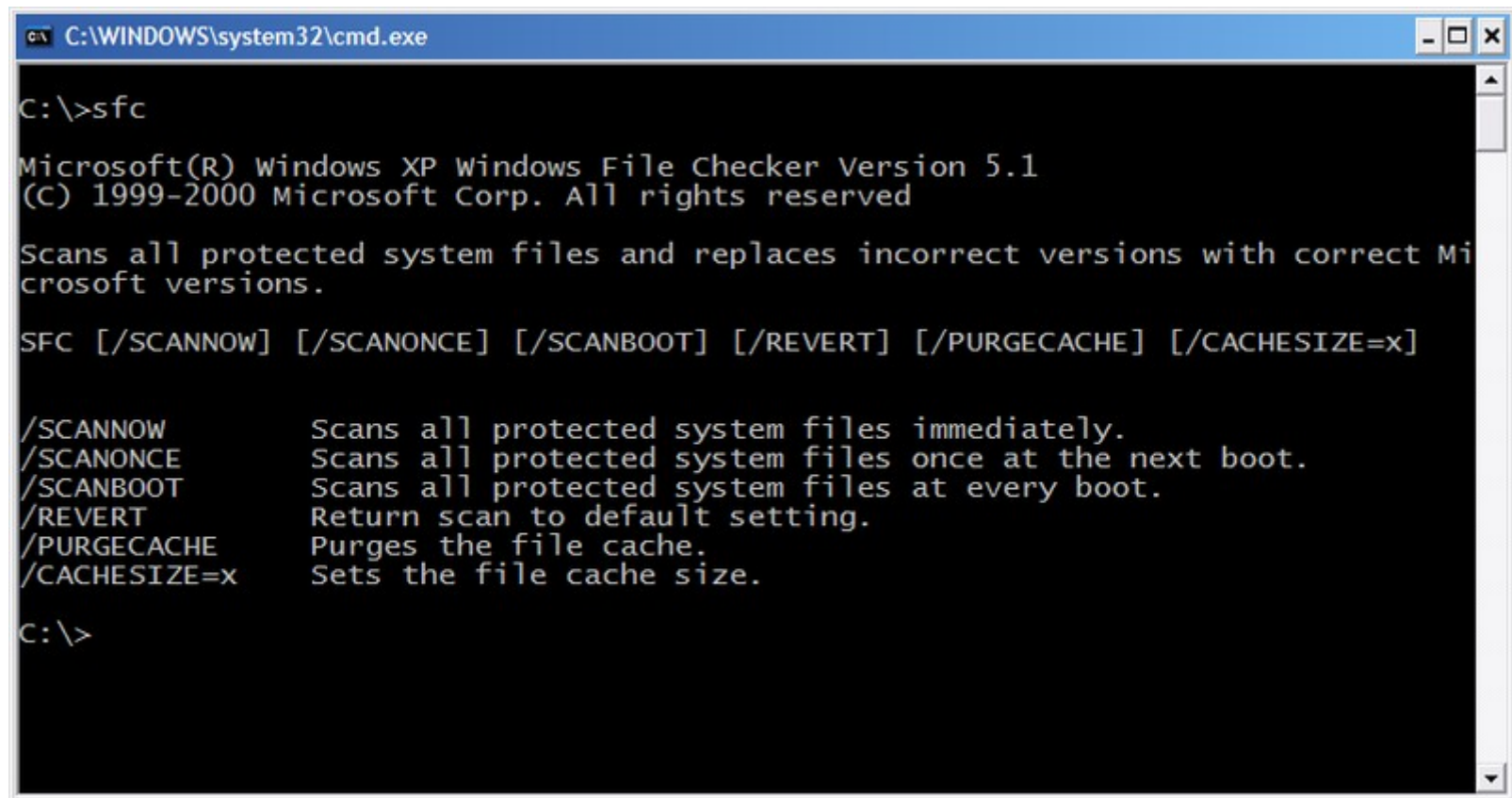


Difícil de detectar:

- Roberto recibe todo lo que Alicia le envía y viceversa
- El problema es que Gertrudis también recibe los mensajes

# Integridad

## System File Checker (sfc.exe)



```
C:\WINDOWS\system32\cmd.exe

C:\>sfc

Microsoft(R) Windows XP Windows File Checker Version 5.1
(C) 1999-2000 Microsoft Corp. All rights reserved

Scans all protected system files and replaces incorrect versions with correct Microsoft versions.

SFC [/SCANNOW] [/SCANONCE] [/SCANBOOT] [/REVERT] [/PURGECACHE] [/CACHESIZE=x]

/SCANNOW           Scans all protected system files immediately.
/SCANONCE          Scans all protected system files once at the next boot.
/SCANBOOT          Scans all protected system files at every boot.
/REVERT            Return scan to default setting.
/PURGECACHE        Purges the file cache.
/CACHESIZE=x       Sets the file cache size.

C:\>
```



# Integridad

- **Tripwire** security and data integrity tool

```
chen@laptop: ~  
Archivo Editar Ver Terminal Ayuda  
chen@laptop:~$ tripwire --help  
tripwire: File integrity assessment application.  
  
Tripwire(R) 2.3.1.2 built for  
  
Tripwire 2.3 Portions copyright 2000 Tripwire, Inc. Tripwire is a registered  
trademark of Tripwire, Inc. This software comes with ABSOLUTELY NO WARRANTY;  
for details use --version. This is free software which may be redistributed  
or modified only under certain conditions; see COPYING for details.  
All rights reserved.  
Usage:  
  
Database Initialization: tripwire [-m i|--init] [options]  
Integrity Checking: tripwire [-m c|--check] [object1 [object2...]]  
Database Update: tripwire [-m u|--update]  
Policy Update: tripwire [-m p|--update-policy] policyfile.txt  
Test: tripwire [-m t|--test] --email address  
  
Type 'tripwire [mode] --help' OR  
'tripwire --help mode [mode...]' OR  
'tripwire --help all' for extended help  
chen@laptop:~$
```

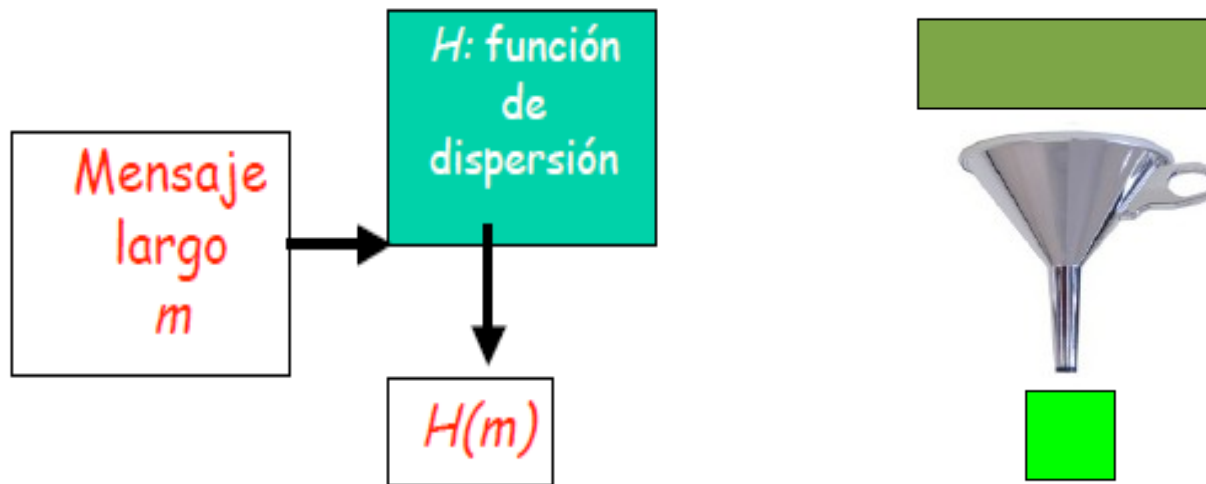


# Integridad

---

Comprobar los ficheros completamente es computacionalmente muy caro.

Se utilizan funciones de dispersión  $H$  con las que se obtiene un resumen del fichero de tamaño fijo  $H(m)$



# Integridad

---

Algoritmos para la función de dispersión:

- MD5
- SHA-1



## Ver para crear

---

- Obtener el resumen de un fichero con SHA-1:

```
$ openssl sha1 fichero
```



# Ver para crear

# OpenSSL<sup>TM</sup>

Cryptography and SSL/TLS Toolkit

[Tarballs](#) | [License](#) | [Repository](#) | [Mirror](#) | [CVS](#)

- Title
- FAQ
- About
- News
- Documents
- Source
- Contribution
- Support
- Related

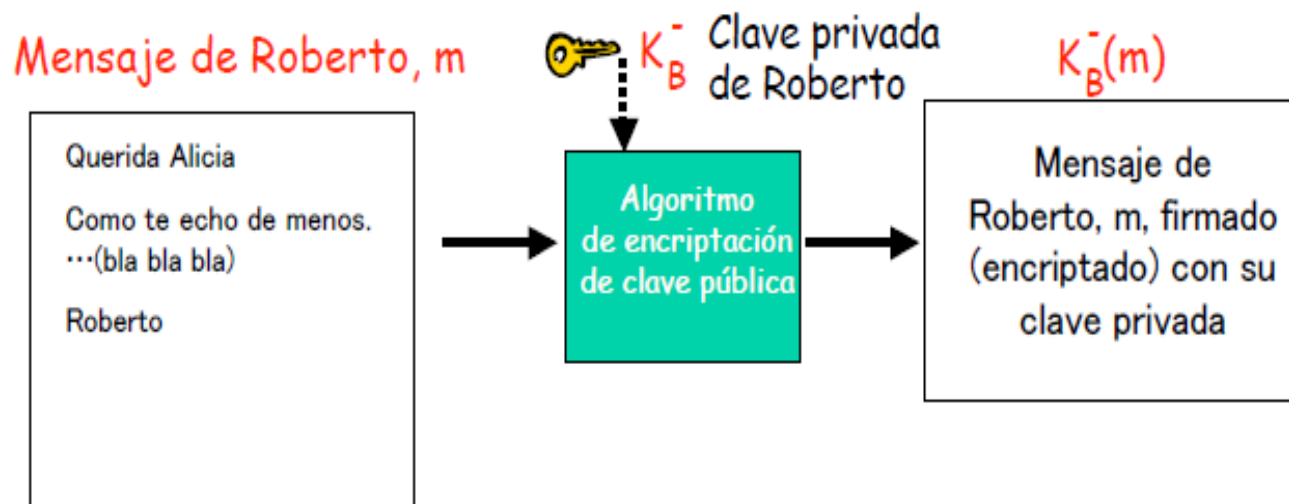
## Tarballs

Here you can find all distribution tarballs (and sometimes corresponding patches) you can also download them via FTP from the OpenSSL FTP area under [ftp://ft](ftp://ftp.openssl.org/ft) the latest development version can be found under <ftp://ftp.openssl.org/snaps>

Bytes	Timestamp	Filename
3772542	Jun 1 16:56:21 2010	<a href="#">openssl-0.9.8o.tar.gz</a> (MD5) (SHA1) (PGP sign)
4015794	Jun 1 15:46:21 2010	<a href="#">openssl-1.0.0a.tar.gz</a> (MD5) (SHA1) (PGP sign) [LATEST]
4010166	Mar 29 15:24:59 2010	<a href="#">openssl-1.0.0.tar.gz</a> (MD5) (SHA1) (PGP sign)
3770041	Mar 24 14:25:16 2010	<a href="#">openssl-0.9.8n.tar.gz</a> (MD5) (SHA1) (PGP sign)
3767604	Feb 25 18:24:43 2010	<a href="#">openssl-0.9.8m.tar.gz</a> (MD5) (SHA1) (PGP sign)
3767860	Jan 20 18:40:03 2010	<a href="#">openssl-0.9.8m-beta1.tar.gz</a> (MD5) (SHA1) (PGP sign)
4006467	Jan 20 16:14:14 2010	<a href="#">openssl-1.0.0-beta5.tar.gz</a> (MD5) (SHA1) (PGP sign)
2100	Nov 20 23:16:38 2009	<a href="#">openssl-fips-1.2.crossbuild.diff.gz</a> (MD5) (SHA1) (PGP sign)
4000628	Nov 10 14:44:01 2009	<a href="#">openssl-1.0.0-beta4.tar.gz</a> (MD5) (SHA1) (PGP sign)

# Firma digital

Roberto podría firmar el mensaje encriptándolo con su clave privada:

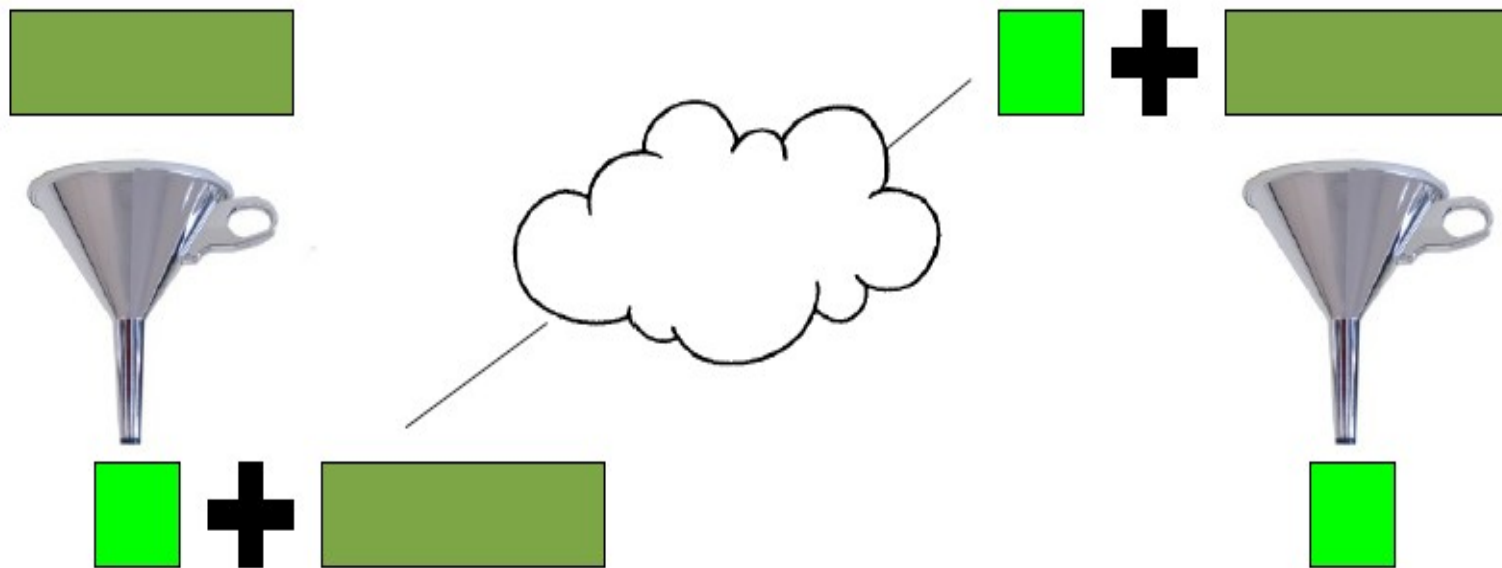


Al recibirlo, Alicia lo descripta utilizando la clave pública de Roberto → autenticación, integridad y no repudio

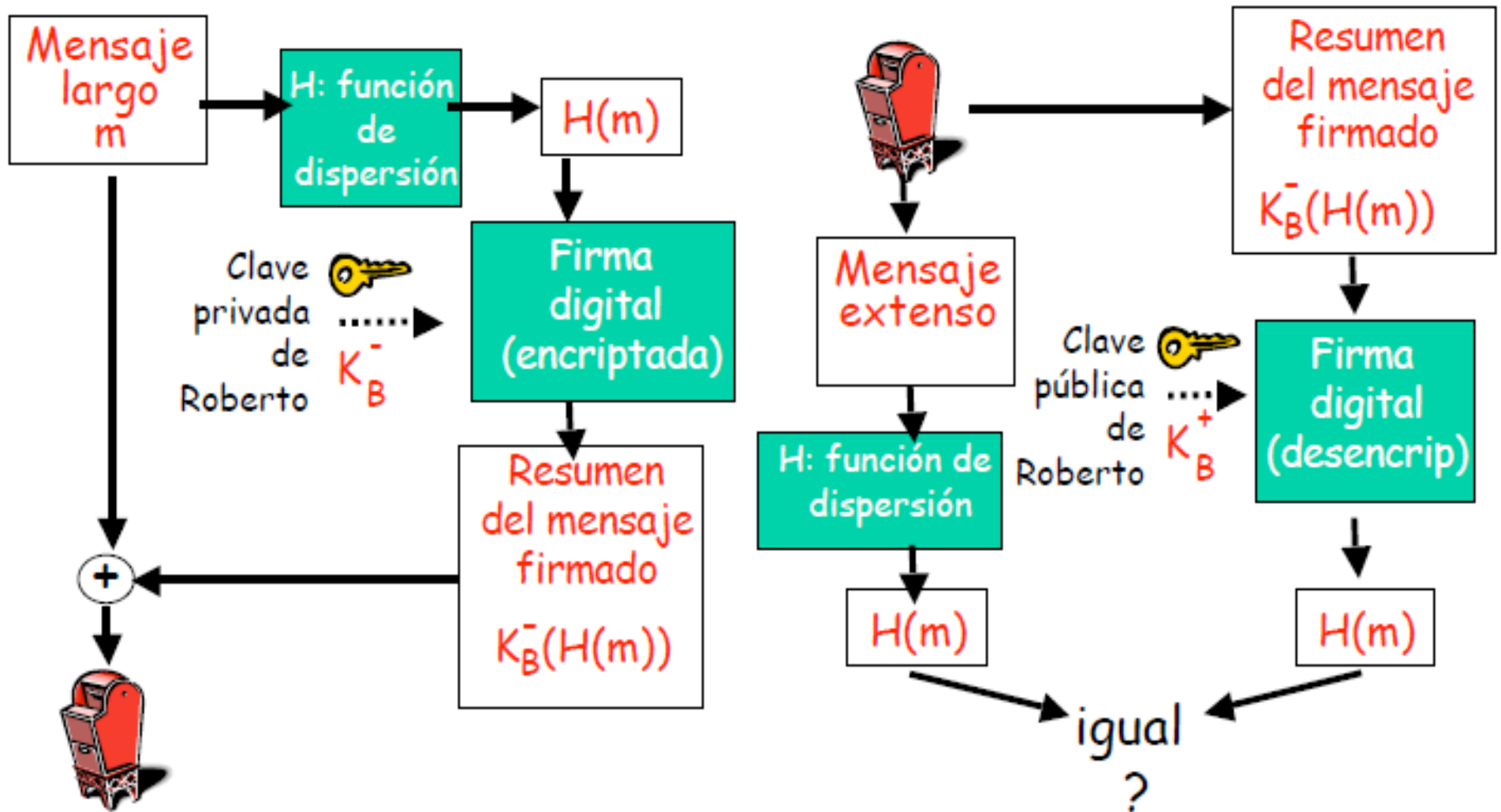
# Firma digital

---

Resulta computacionalmente caro encriptar mensajes largos con clave pública → usaremos funciones de dispersión



# Firma digital





## Ver para crear

---

- Obtener la firma digital de un mensaje con RSA:

```
$ openssl dgst -sha1 -sign privada.key -out firmadigital.sha1  
mensaje.txt
```

- Verificar el mensaje recibido:

```
$ openssl dgst -sha1 -verify publica.key -signature  
firmadigital.sha1 mensaje.txt
```

## Ver para creer

---

Imagina que has recibido un correo electrónico desde mi cuenta con dos ficheros adjuntos `calificacion.txt` y `firma.sha1`. El contenido de `calificacion.txt` es el siguiente:

Estimado alumno/a,

tras consultar las notas de tus tareas y llevar a cabo un estudio pormenorizado de tu evolución y progresos durante el curso, el departamento de informática ha decidido ponerte un 10 en la calificación del módulo Seguridad Informática.

No es necesario que vengas más a clase. Enhorabuena.

Fdo: Jesús Moreno



## Ver para creer

---

En el foro de la asignatura puedes encontrar los dos ficheros *recibidos en el mail* (`calificacion.txt` y `firma.sha1`) y mi clave pública `publica.key`.

¿Cómo podrías comprobar que el mensaje recibido ha sido firmado por mí y que no se ha modificado el contenido del fichero `calificacion.txt`?

