Seguridades

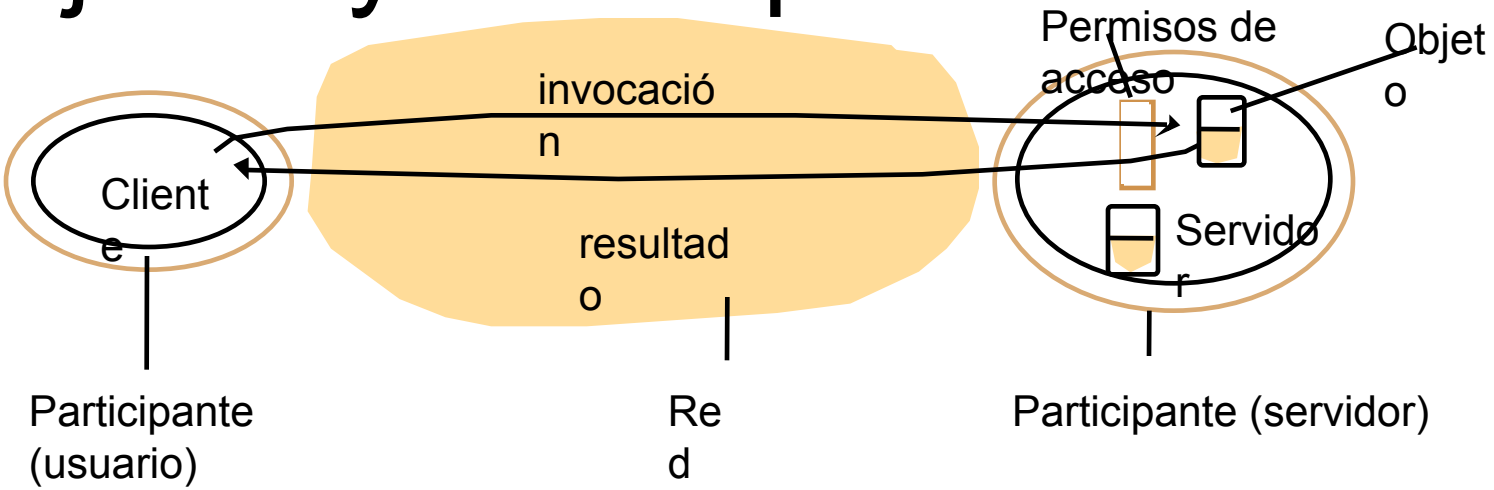
Temas a Tratar

- Modelo de seguridades
  - Tipos de amenazas
- Técnicas básicas
  - Técnicas criptográficas
    - Secretismo
    - Autenticación
    - Certificados y credenciales
- Algoritmos de encriptación simétrica y asimétrica
- Firmas digitales
- Enfoques para un diseño de sistemas seguros
- Caso de estudio: TLS

Pilares

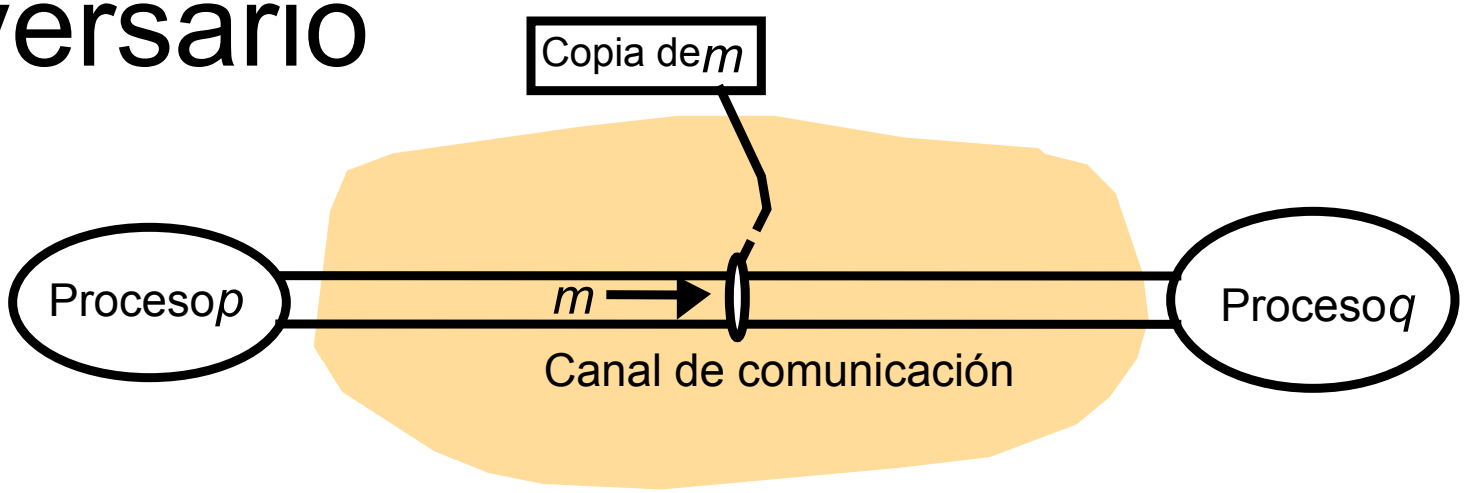
- Confidencialidad
  - Privacidad: canales seguros
  - Anonimidad: anonimizadores
- Integridad
  - Autenticación del origen: firmas digitales
  - No alteración de datos: checksums criptográficos
- Disponibilidad
  - Que el servicio/recurso esté siempre disponible: replicación y enfoques peer-to-peer

Objetos y Participantes



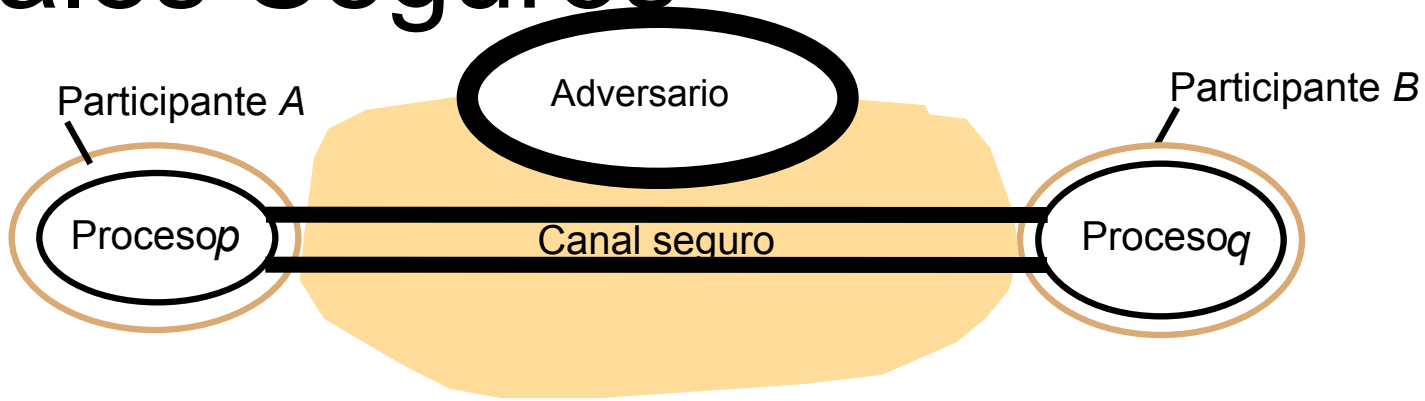
- Objeto (o recurso)
  - Mailbox, archivo del sistema o parte de un website comercial
- Participante
  - Usuario o proceso que tiene la autoridad (permisos) para realizar acciones
  - La identidad del participante es importante

Adversario



- Ataques
  - A aplicaciones que administran transacciones financieras u otro tipo de información cuya confidencialidad o integridad es importante
- Adversario
  - Puede tratar de “escuchar” la comunicación, hacerse pasar por uno de los participantes, alterar los mensajes, inundar puertos con los mensajes
- Amenazas
  - A los procesos, canales de comunicación, negación del servicio

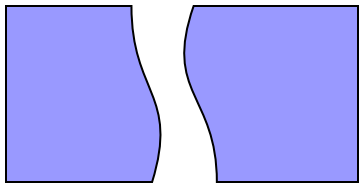
Canales Seguros



- Propiedades
  - Cada proceso está seguro de la identidad del otro
  - Los datos son confidenciales (no pueden ser leídos por terceros)
  - Los datos no pueden ser alterados por terceros
  - Existe protección contra ataques de repetición y re-ordenamiento de los datos
- Solución: usar criptografía
  - Confidencialidad
  - Autenticación

Uso de Criptografía

- Para confidencialidad
  - Confusión
  - Difusión
- Basado en secretos
  - Compartidos: claves secretas de encriptación
  - No compartidos: claves privada/pública



Amenazas y Formas de Ataques

- Escuchar
  - Para obtener información privada o secreta
- Enmascararse
  - Se asume la identidad de otro usuario/participante
- Alteración de mensajes
  - Alteración del contenido de los mensajes en tránsito
    - Ataque de hombre-en-el-medio
- Repeticiones
  - Almacenamiento de mensajes seguros y re-envío de los mismos posteriormente
- Negación del servicio
  - Inundación de un canal o de otro recurso, para negar el acceso a otros

Amenazas no Combatidas por los Canales Seguros

- Ataques de negación del servicio
  - Uso de recursos excesivos de tal manera que se le afecta el acceso a los mismos para los usuarios legítimos
- Caballos de Troya y otros virus
  - Defensas:
    - Autenticación del código (firmado)
    - Validación del código (pruebas formales)
    - Cajas de arena

Nomenclatura

K_A	Clave secreta de A
K_B	Clave secreta de B
K_{AB}	Clave secreta compartida entre A y B
K_{Apriv}	Clave privada de A
K_{Apub}	Clave pública de A
$\{M\}_K$	Mensaje M encriptado con la clave K
$[M]_K$	Mensaje M firmado con la clave K

Convención

Alice	Primer participante
Bob	Segundo participante
Carol	Participante en protocolos de tres y cuatro miembros
Dave	Participante en protocolos de cuatro miembros
Eve	Eavesdropper (que está escuchando en el canal)
Mallory	Ataque malicioso
Sara	Un servidor

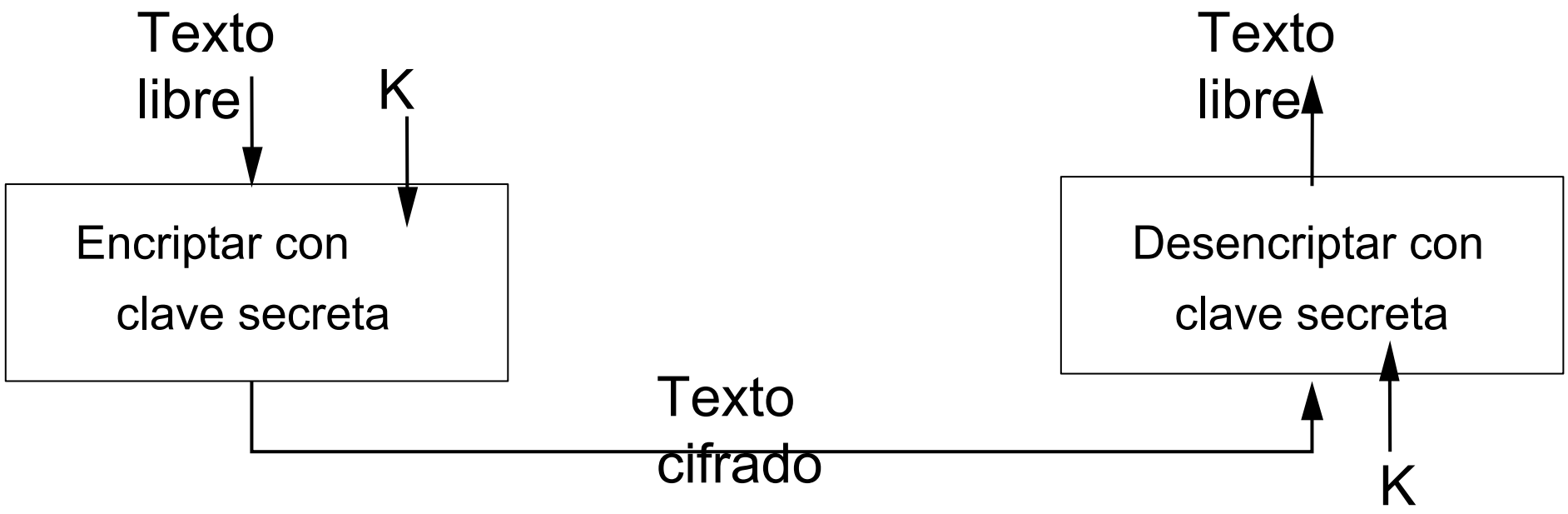
Algoritmos Criptográficos

Encriptación

- Proceso mediante el cual se convierten los datos (texto libre) en algo no interpretable por quien no tiene la clave para hacerlo (texto cifrado)
- Dos tipos
  - Simétrica
  - Asimétrica

Encriptación Simétrica

- También llamada de *clave secreta*
- A veces mal llamada: de *clave privada*

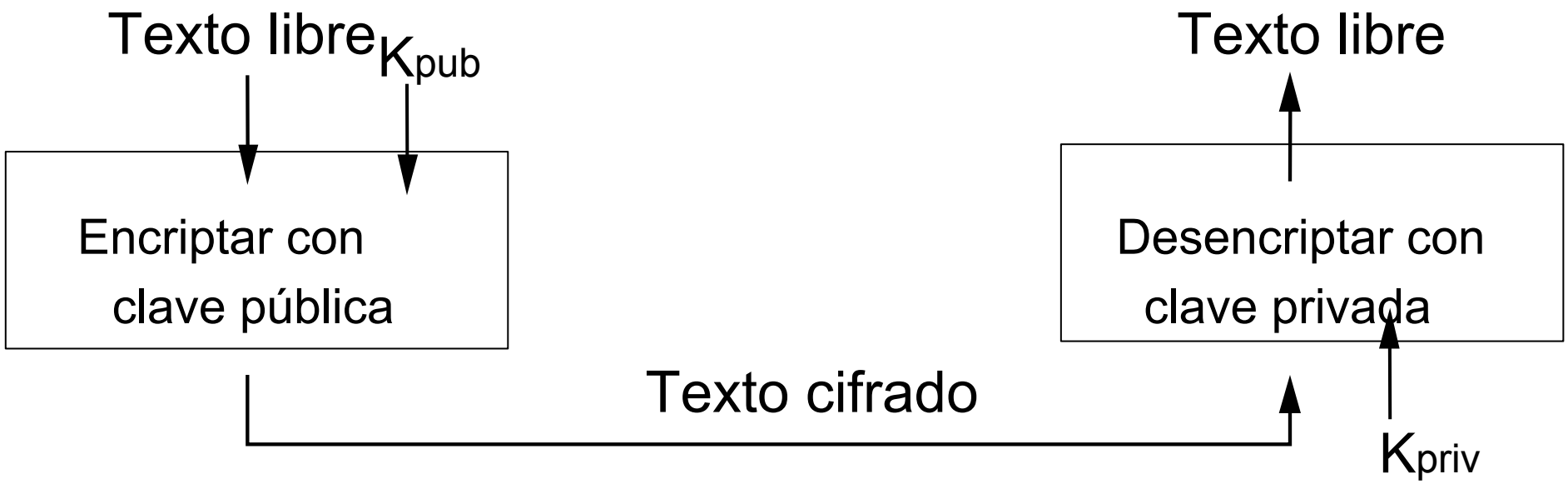


Encriptación Simétrica

- Algoritmos
  - DES: Data Encryption Standard
  - Triple DES
  - IDEA: International Data Encryption Standard
  - AES: Advanced Encryption Standard
  - Blowfish y Twofish
  - RC4 (ARC4)
  - Skipjack

Encriptación Asimétrica

- También llamada de *clave privada/clave pública*
- Más lenta que la encriptación simétrica



Encriptación Asimétrica

- Algoritmos
  - Diffie-Hellman
    - Para establecer secretos compartidos
  - RSA: Rivest, Shamir y Adleman
    - Para encriptar y firmar
- Ventaja sobre encriptación simétrica
  - No hay problemas de distribución de claves

Resumen de Mensajes

- También llamado
  - Hash
    - Mapean un mensaje potencialmente grande en un número pequeño de tamaño fijo
  - Checksum criptográfico
    - Checksums protegen contra alteraciones en mensajes
    - Checksums criptográficos protegen contra alteraciones *maliciosas* de mensajes

Resumen de Mensajes

- Resumen (*digest*) producido por una función de *una-vía*
  - Función de una-vía: Dado un checksum criptográfico, es virtualmente imposible hallar un mensaje entendible que produzca ese checksum
- Algoritmos
  - MD5: Message Digest versión 5
    - Muy eficiente: muy rápido de calcular
    - Se han detectado vulnerabilidades
  - SHA: Secure Hash Algorithm
    - SHA-1 es inseguro
    - SHA-2 es lo recomendado

Firmas Digitales usando Resúmenes de Mensajes

Alice quiere publicar un documento M de tal manera que cualquiera pueda verificar que proviene de ella

1. Alice computa un resumen de un mensaje Digest(M)
2. Alice encripta el resumen con su clave privada y lo adjunta a M; el resultado es el documento firmado (M, $\{Digest(M)\}K_{Apriv}$), el cual es publicado para que lo puedan accesar otros usuarios
3. Bob obtiene el documento firmado, extrae M y calcula Digest(M)
4. Bob usa la clave pública de A para desencriptar $\{Digest(M)\}K_{Apriv}$ y lo compara con el resumen calculado. Si son iguales, se ha verificado la firma de A

Resumen de Algoritmos Criptográficos

- Simétricos (clave secreta)

  $E(K, M) = \{M\}_K$ $\quad\quad$ $D(K, E(K, M)) = M$

  Ataque: fuerza bruta (tratar todas las claves posibles)

  Solución: hacer K grande
- Asimétricos (clave pública)

  Claves separadas para encriptación y desencriptación: K_{pub} y K_{priv}

  $D(K_{priv}. E(K_{pub}, M)) = M$

  "E" tiene un alto costo de computación
- Híbridos

  Utilizan criptografía asimétrica para transmitir la clave simétrica que posteriormente se utiliza para encriptar la sesión

  Ej.: SSH y TLS

Algoritmos recomendados (2017)

- Criptografía simétrica: AES
- Criptografía asimétrica: RSA
- Resumen de mensajes: SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256)

Nota: Esto cambia con el tiempo; en un año puede que alguno de estos ya no sea recomendado

Certificados Digitales

- Certificado: un enunciado firmado por una autoridad pertinente
- Un certificado requiere:
  - Un formato pre-establecido
  - Un acuerdo de cómo formar cadenas de confianza
  - Fechas de expiración, para que puedan ser revocados

Certificados Digitales

Certificado digital del banco de Bob

1.	*Tipo*	:	Clave pública
2.	*Nombre*	:	Banco de Bob
3.	*Clave pública*	:	K_{Bpub}
4.	*Autoridad de cert.*	:	Fred – La Federación de Bancos
5.	*Firma*	:	$\{Digest(campo\ 2 + campo\ 3)\}\ K_{Fpriv}$

Formato X.509

Sujeto	Nombre (o dominio) y clave pública
Emisor	Nombre y firma
Periodo de validez	No antes de y no después de
Información administrativa	Versión y número de serie
Información extendida	

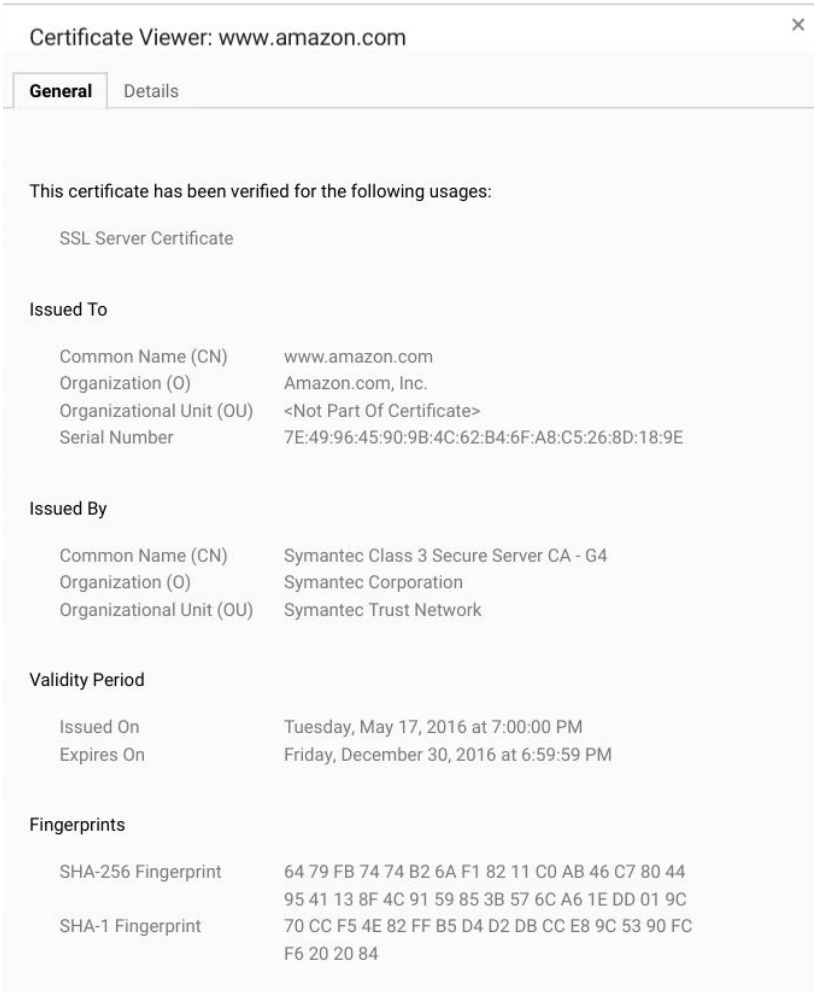
Certificados como Credenciales

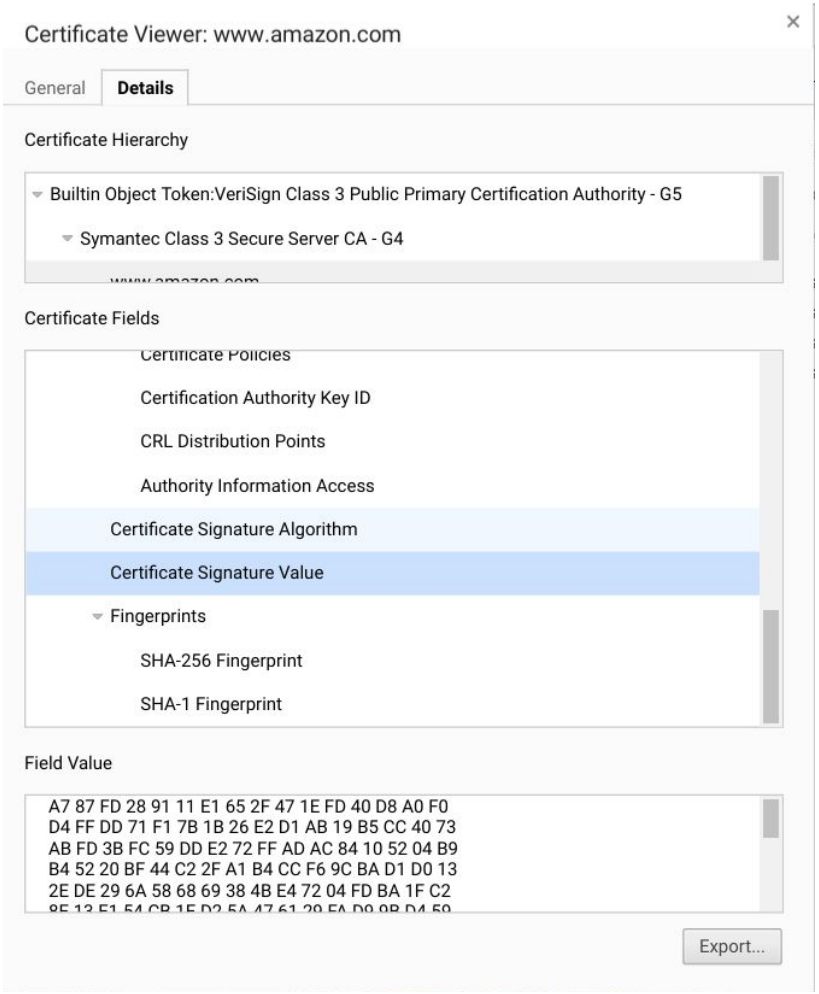
- Certificados sirven de credenciales
  - Evidencia para probar identidad de un participante
- Tener un certificado digital no prueba nada (son públicos)
- Tener la clave privada de la correspondiente K_{pub} del certificado, prueba la identidad de la entidad
  - Desafío respuesta

Revocación de Certificados

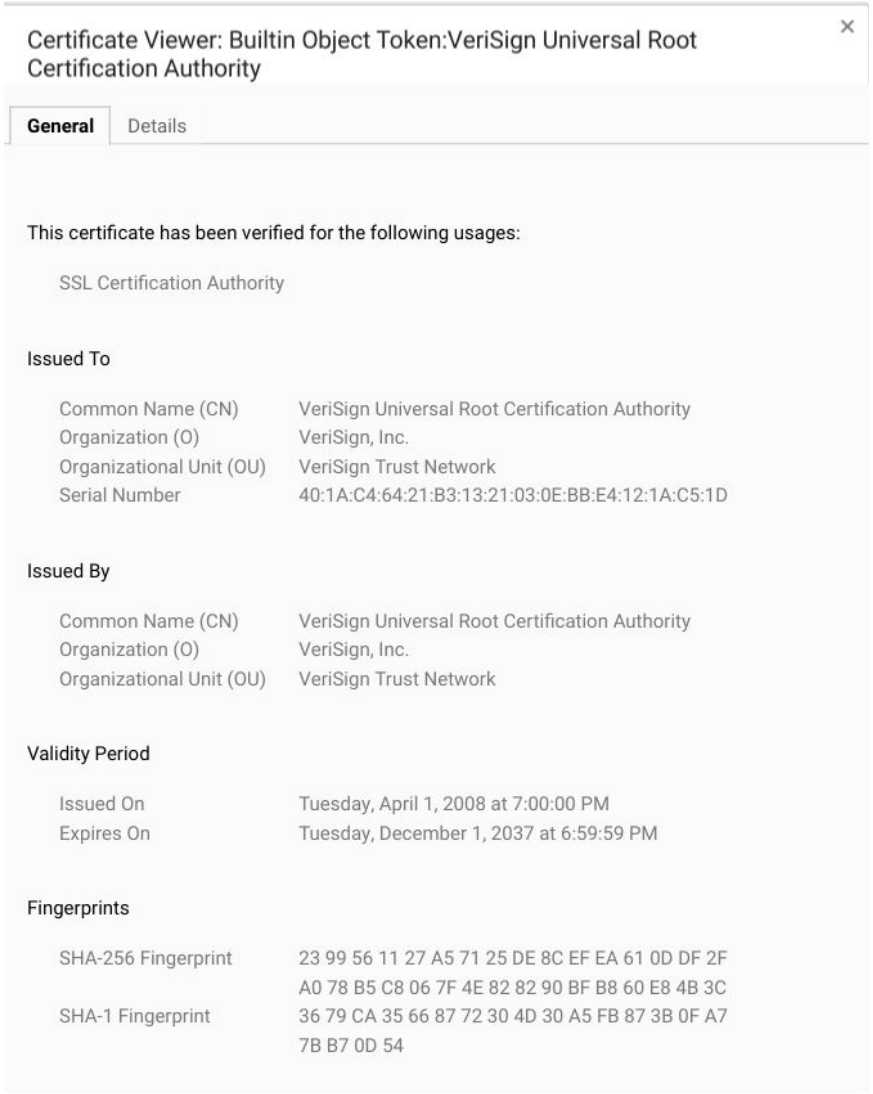
- Si se sospecha que la clave privada ha sido comprometida, certificado debe ser revocado
- CRL: lista de revocación de certificados
  - Generada y distribuida por la CA
  - Actualizada periódicamente
  - Disponible públicamente
  - Cuando A recibe un certificado de B, debe revisar que no haya sido revocado

Ejemplo: CD de Amazon





Ejemplo: CD de Verisign



Certificate Viewer: Builtin Object Token:VeriSign Universal Root Certification Authority

General | Details

This certificate has been verified for the following usages:

SSL Certification Authority

Issued To

Common Name (CN)	VeriSign Universal Root Certification Authority
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network
Serial Number	40:1A:C4:64:21:B3:13:21:03:0E:BB:E4:12:1A:C5:1D

Issued By

Common Name (CN)	VeriSign Universal Root Certification Authority
Organization (O)	VeriSign, Inc.
Organizational Unit (OU)	VeriSign Trust Network

Validity Period

Issued On	Tuesday, April 1, 2008 at 7:00:00 PM
Expires On	Tuesday, December 1, 2037 at 6:59:59 PM

Fingerprints

SHA-256 Fingerprint	23 99 56 11 27 A5 71 25 DE 8C EF EA 61 0D DF 2F A0 78 B5 C8 06 7F 4E 82 82 90 BF B8 60 E8 4B 3C
SHA-1 Fingerprint	36 79 CA 35 66 87 72 30 4D 30 A5 FB 87 3B 0F A7 7B B7 0D 54

Firmas Digitales

- Requerimientos
  - Autenticar documentos almacenados o mensajes enviados
  - Proteger contra falsificaciones
  - Prevenir que el origen niegue su participación (y niegue así su responsabilidad)

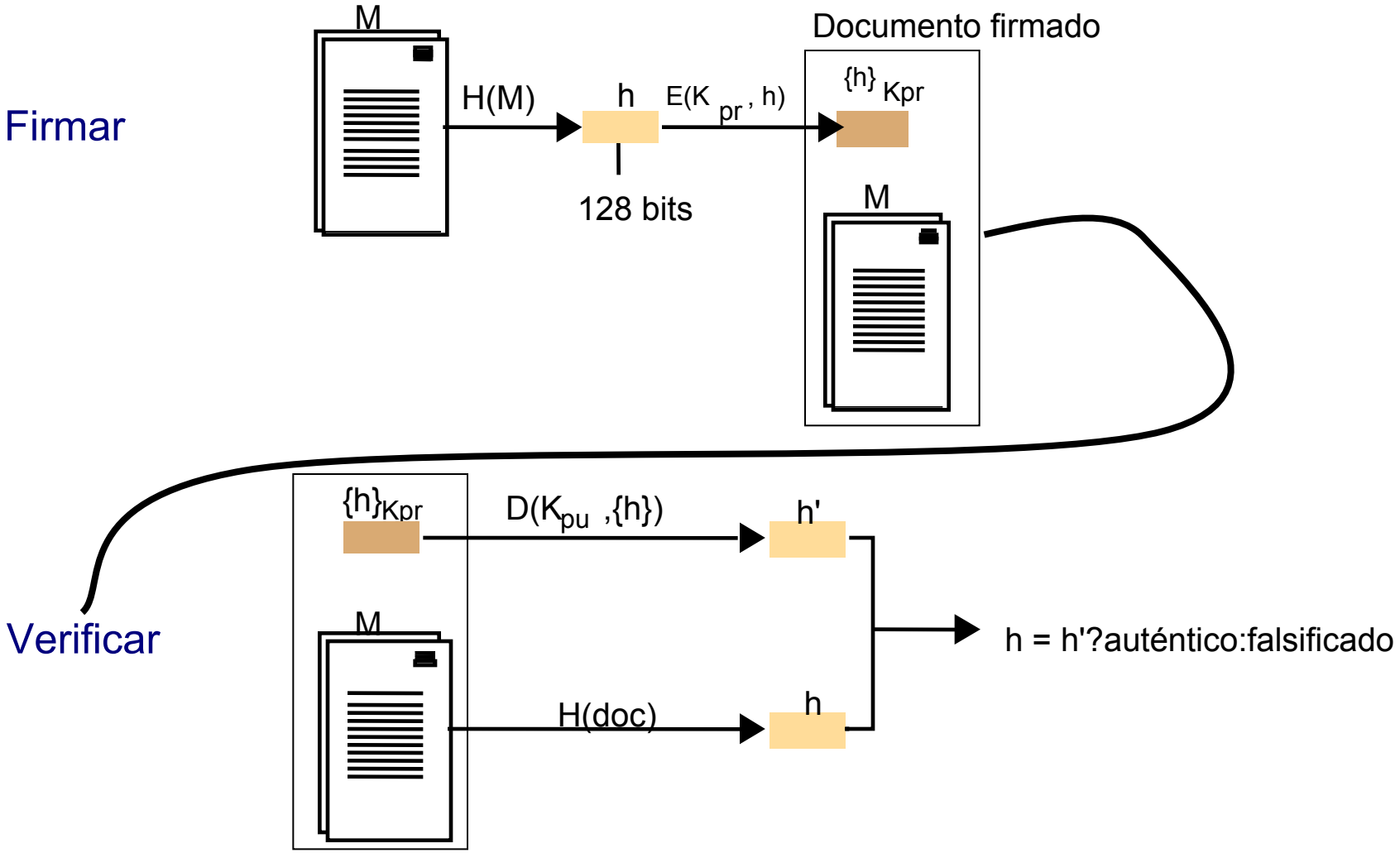
Firmas Digitales

- Encriptar un documento con una clave privada constituye una firma digital
  - Imposible que otros lo realicen sin poseer la clave
  - Autenticación del documento
  - Protección contra falsificaciones
  - Negación de participación: origen puede aludir que la clave estuvo comprometida

Firmas Digitales

- Esquema descrito en diapositiva anterior es muy caro:
  - Costo de procesamiento
  - Firma es muy grande
- Alternativa: resumen seguro
  - $E(K_{priv}, Digest(M))$

Ejemplo


Firmar
M
H(M)
h
E(K pr , h)
128 bits
Documento firmado
{h} Kpr
M
Verificar
{h}Kpr
D(Kpu ,{h})
h'
M
H(doc)
h
h = h'?auténtico:falsificado

Comunicación Secreta con una Clave Compartida

- Alice y Bob comparten una clave secreta K_{AB}
  1. Alice utiliza K_{AB} y una función de encriptación acordada $E(K_{AB}, M)$ para encriptar y enviar cualquier número de mensajes $\{M\}_{K^{AB}}$ a Bob
  2. Bob desencripta el mensaje con la función correspondiente $D(K_{AB}, \{M\}_{K^{AB}})$

Comunicación Secreta con una Clave Compartida

- Problemas
  - Distribución de claves
    - ¿Cómo puede Alice enviarle a Bob la clave secreta K_{AB} de manera segura?
  - Frescura de los mensajes
    - ¿Cómo puede Bob saber que cualquier $\{M_i\}$ no es una copia de un mensaje anterior de alice que fue capturado por Mallory y re-enviado posteriormente?

Comunicación Autenticada con Claves Públicas

Bob tiene un par de claves <K_{Bpub}, K_{Bpriv}>

1. Alice obtiene la clave pública de Bob, K^{Bpub}
2. Alice crea una nueva clave secreta compartida K_{AB}, y la encripta usando K_{Bpub}, con un algoritmo de clave pública
3. Bob usa su correspondiente clave privada K_{Bpriv} para desencriptar el mensaje y obtener K_{AB}

Si quieren estar seguros de que el mensaje no ha sido alterado, Alice puede añadir un valor acordado al mismo, para que Bob pueda verificarlo

Problema: distribución segura de la clave pública
Solución: uso de certificados digitales firmados por una autoridad de certificación

SSL/TLS

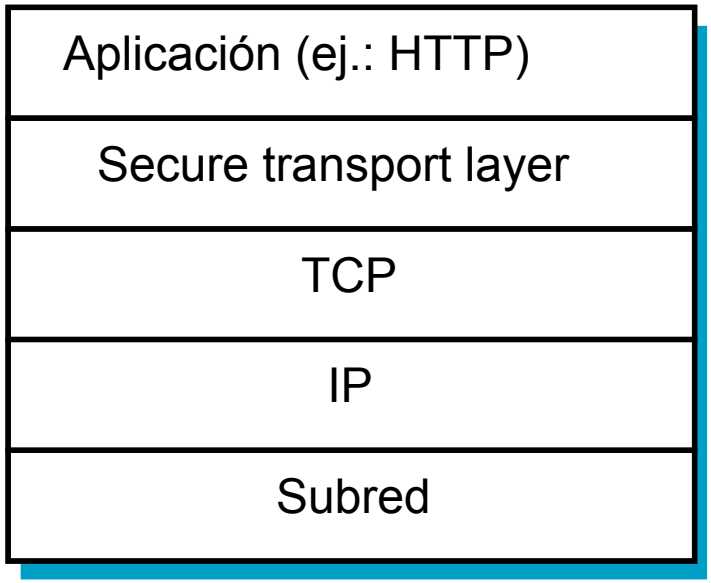
SSL: Secure Socket Layer

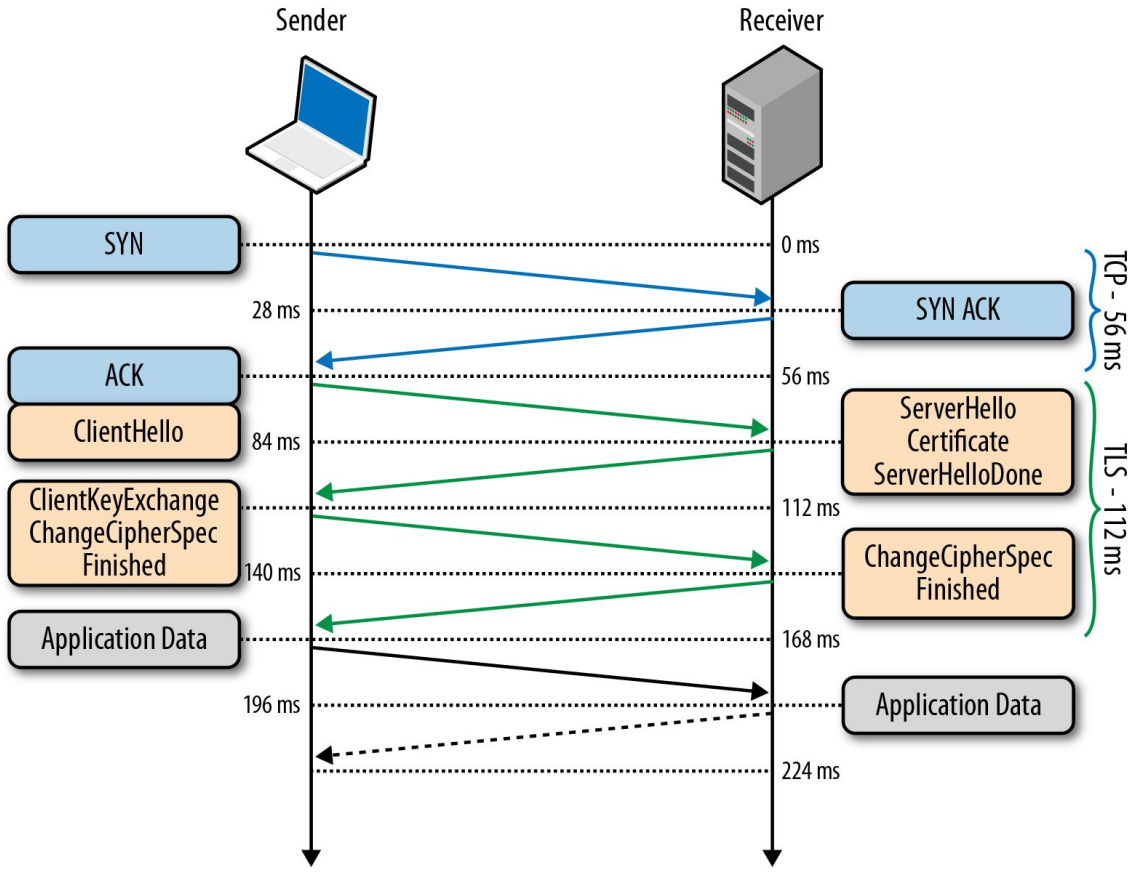
- Actualmente: TLS
  - Seguridad de capa de transporte
- Para transacciones Web (u otras) seguras
- Canales seguros para comercio electrónico
- Protocolo híbrido

Requerimientos de Diseño

- Comunicación segura sin negociación previa o ayuda directa de 3eros
- Opción de escoger algoritmos criptográficos
- Comunicación en ambas direcciones puede ser autenticada, encriptada o ambas

Seguridad de Capa de Transporte



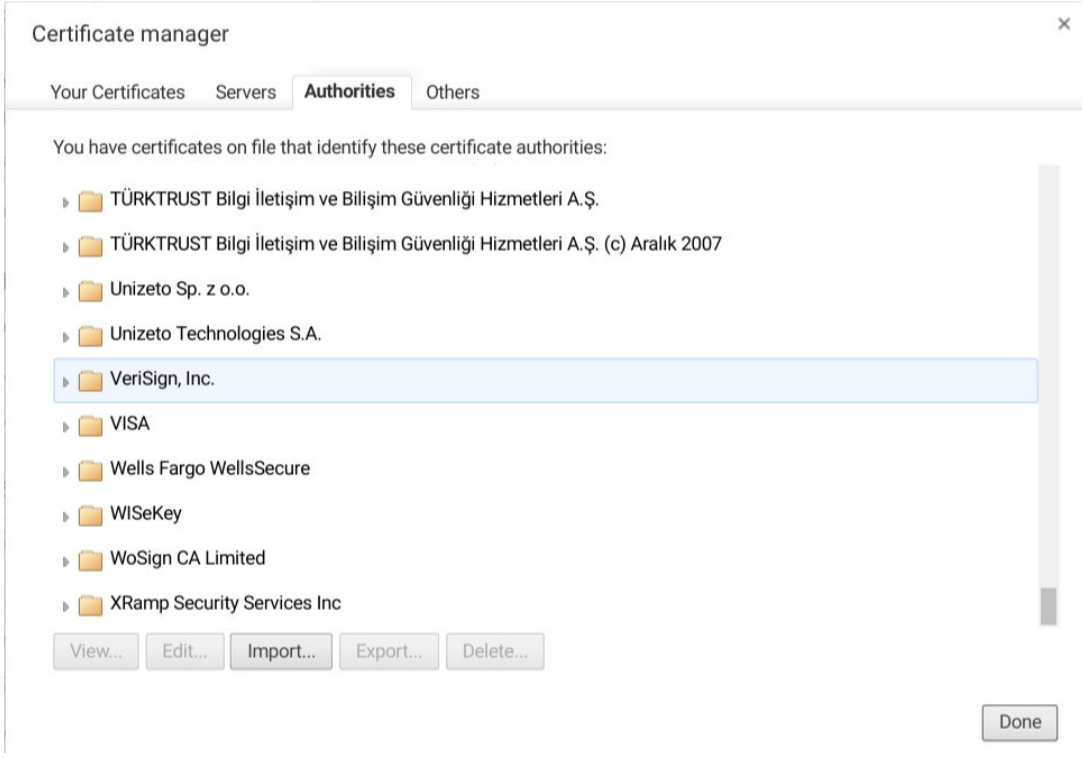


TLS

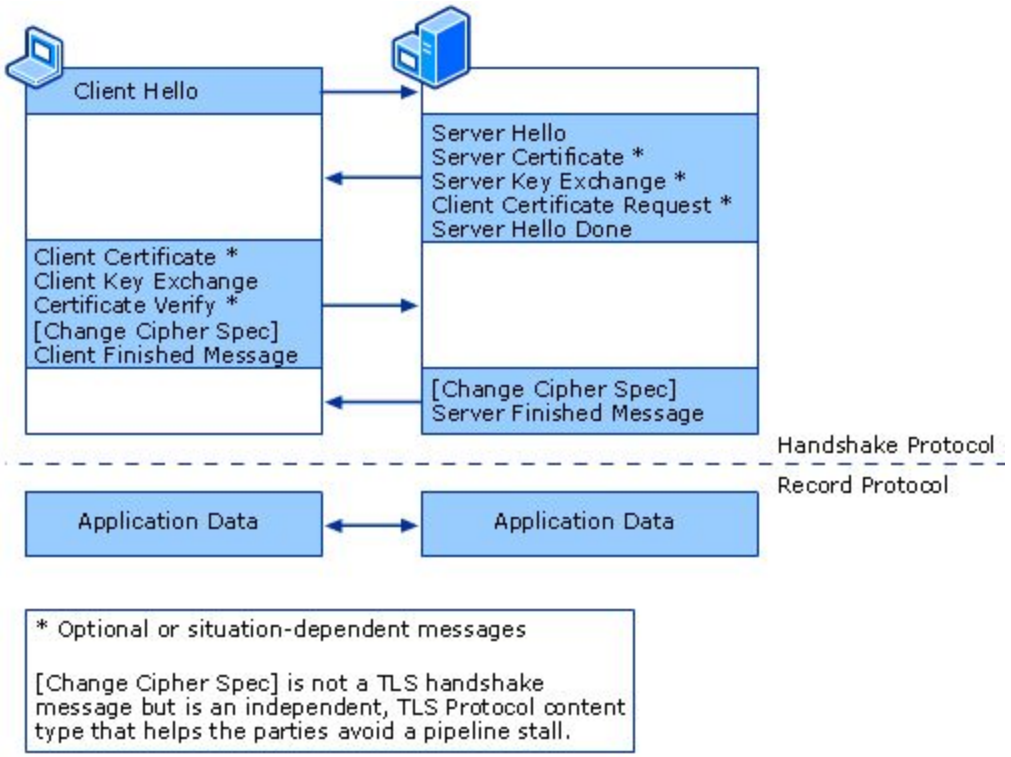
- Tiene dos partes
  - Protocolo de saludo
    - Usado para negociar parámetros de la comunicación
  - Protocolo de registro
    - Usado para la transferencia (encriptada) de datos

TLS

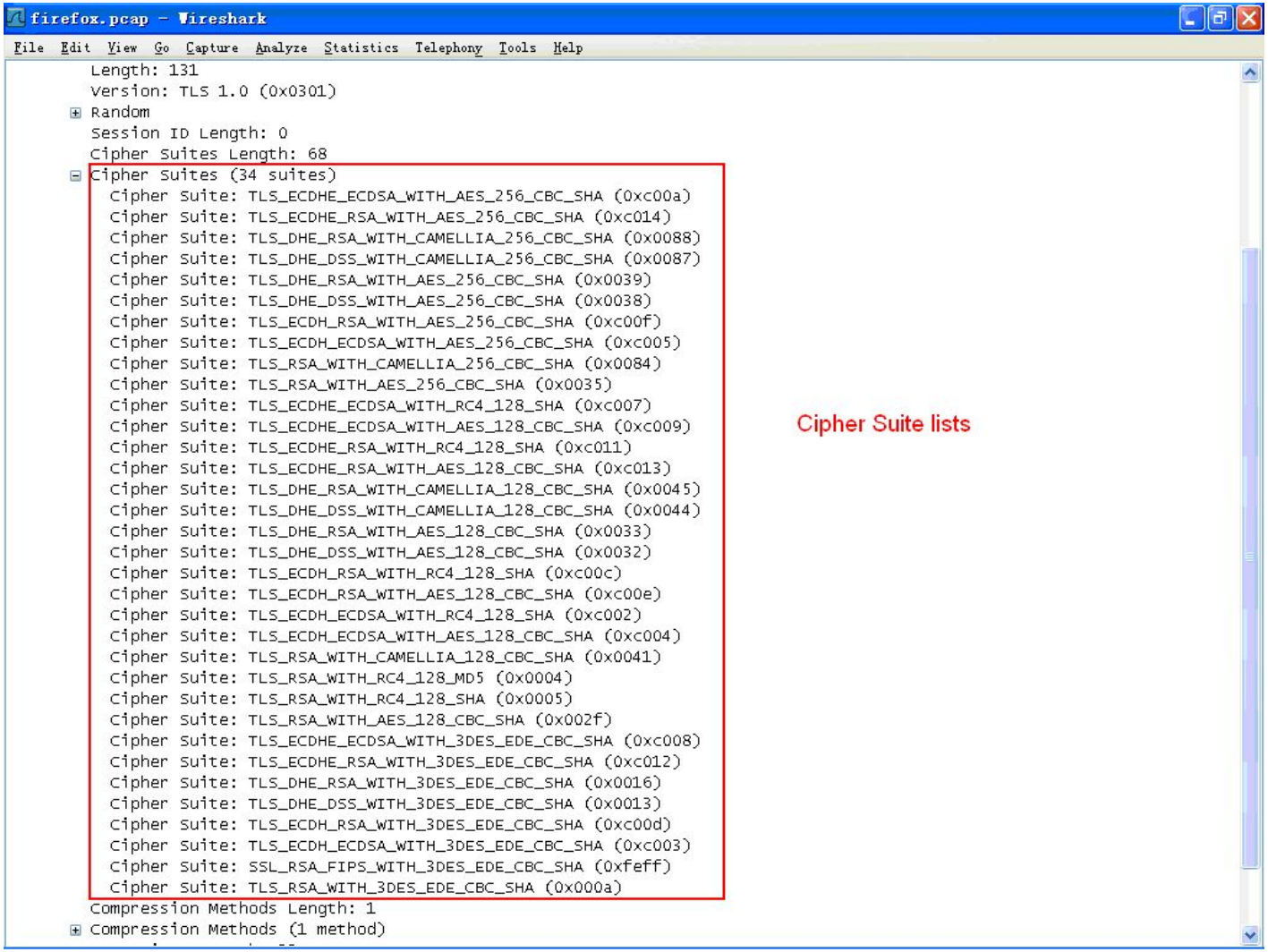
- No especifica una estructura de claves en particular
- Actualmente, una CA firma los certificados
  - Clave pública de varias CAs incluidas con todos los navegadores



TLS


Client Hello
Server Hello
Server Certificate *
Server Key Exchange *
Client Certificate Request *
Server Hello Done
Client Certificate *
Client Key Exchange
Certificate Verify *
[Change Cipher Spec]
Client Finished Message
[Change Cipher Spec]
Server Finished Message
Handshake Protocol
Record Protocol
Application Data
Application Data
* Optional or situation-dependent messages
[Change Cipher Spec] is not a TLS handshake message but is an independent, TLS Protocol content type that helps the parties avoid a pipeline stall.

Negociación de algoritmos



Referencia: http://ipseclab.eit.lth.se/tiki-index.php?page=3.+SSL+and+TLS

Ejercicios

Ejemplo: Ejercicio de examen

- Está usted navegando en Internet y se conecta a un sitio Web que desea establecer un canal seguro (HTTPS). En ese momento, el navegador le muestra una mensaje de alerta en pantalla indicando que ha habido algún problema con el certificado digital presentado por el sitio Web.

¿Por qué pudo haber ocurrido este problema?
Nota: Debe proporcionar al menos 4 razones para recibir el puntaje completo.

Solución

1. El CD puede estar en una lista CRL (estar revocado).
2. El CD puede estar en la lista de mi navegador de CD no confiables
3. El CD puede haber caducado (expirado) → ¿Razones?
4. El CD todavía no es válido → ¿Razones?
5. La firma del CD no es válida.
6. El CD ha sido emitido para otro nombre de dominio.
7. CD ha sido emitido por una CA desconocida (es decir, una CA para la cual el navegador no tiene cargado el CD de la CA).
8. El CD esté auto-firmado.

Otros:

- Fechas de cliente y servidor no coinciden

Caso de Estudio: Vulnerabilidad de MD5

En agosto de 2004 unos matemáticos chinos publicaron un paper donde indican que como hallar colisiones para la función MD5; es decir, no es realmente una función de una vía. A raíz de eso, se publicaron varios papers en el 2005 donde se indica paso a paso cómo se puede crear dos certificados digitales X.509 que generen el mismo resumen MD5.

NOTA: cabe recalcar que aún no se sabe cómo, dado un certificado digital V, generar otro certificado W que tenga el mismo resumen MD5. Lo que se sabe es cómo crear dos certificados digitales que generen el mismo resumen MD5.

1. ¿Qué implicaciones tiene esto para una autoridad de certificación (CA)?
2. ¿Qué habría que hacer para montar un ataque que explote esta vulnerabilidad de MD5?
3. ¿Qué puede hacer una CA para evitar problemas con los certificados digitales que firma? (hay al menos dos maneras de evitar tener problemas)

Referencias:

- MD5, Wikipedia: http://en.wikipedia.org/wiki/MD5
- Hash Collission Q&A: http://www.cryptography.com/cnews/hash.html
- Attacks on Cryptographic Hashes in Internet Protocols: http://www.ipa.go.jp/security/rfc/RFC4270EN.html
- Colliding X.509 Certificates: http://eprint.iacr.org/2005/067
- Finding MD5 Collisions – a Toy For a Notebook: http://eprint.iacr.org/2005/075
- Tunnels in Hash Functions: MD5 Collisions Within a Minute: http://eprint.iacr.org/2006/105
- Target Collisions for MD5 and Colliding X.509 Certificates for Different Identities: http://eprint.iacr.org/2006/360