Latin American and Caribbean Internet Addresses Registry
Registro de Direcciones de Internet para América Latina y Caribe
Registro de Endereços da Internet para América Latina e Caribe

Conceptos generales de DNSSEC

4 de agosto de 2011

Carlos Martínez-Cagnazzo
carlos @ lacnic.net

DNSSEC

- Conceptos de Criptografía
- DNSSEC
- Donde DNSSEC
- Como DNSSEC
- Nuevos registros
- Cadena de confianza

Tutorial DNS Capítulo III

CRIPTOGRAFÍA

Criptografía

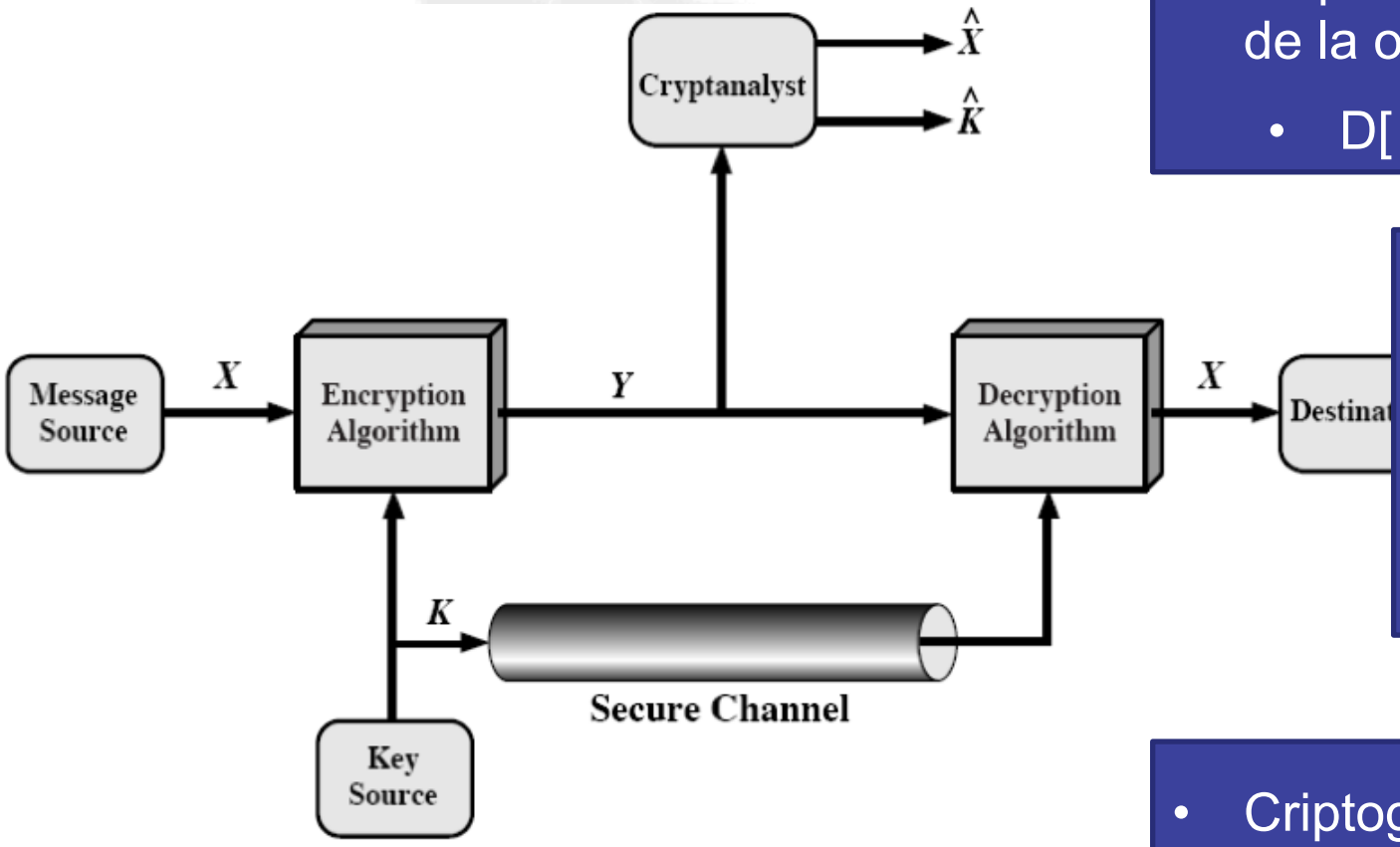
- Conceptos importantes de criptografía para DNSSEC
  - Cifrado de clave pública
  - Algoritmos de *hashing*
  - Firma digital
  - Cadena de confianza

Criptografía (ii)

- En general, dos partes necesitan comunicarse de forma **privada** buscan asegurar algunas propiedades de la comuniación y de los mensajes:
  - Estar seguras de que nadie más ha podido **ver o leer** sus mensajes (propiedad de ***privacidad***)
  - Estar seguras de que nadie ha podido **alterar** sus mensajes (propiedad de ***integridad***)
  - Estar seguras de que quien envía los mensajes **es quien dice ser** (propiedad de ***autenticidad***)

Criptografía simétrica

[Fuente: Stallings]

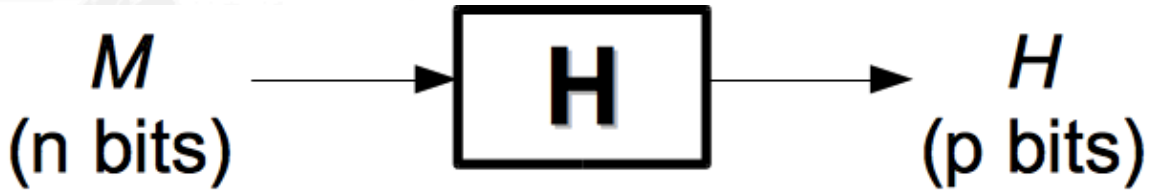


- E[.] y D[.] son dos funciones respectivamente inversas una de la otra
  - D[E [X]] = X

- La clave *K* es un parámetro adicional que se introduce para facilitar la recuperación frente a intrusiones

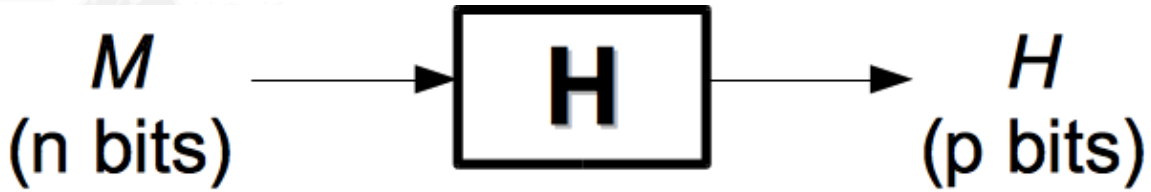
- Criptografía simétrica
  - D[*K*, E [*K*, X]] = X

Hashes criptográficos



- H es una transformación que cumple
  - p << n
  - Dado el algoritmo, n es fijo
- Esto implica que existen colisiones
  - Colisión: Encontrar M1 y M2 tales que H(M1) == H(M2)
  - Si H() es buena tiene que ser muy difícil encontrarlos
- Intuitivamente
  - Una función de hash es tanto mejor en cuanto el resultado aparece mas “randómico”

Hashes criptográficos (ii)



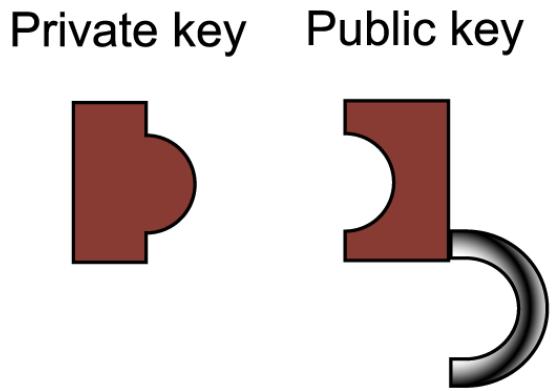
- Algunos algoritmos conocidos:
  - MD5
    - 128 bits
  - SHA1 / SHA256
    - 160 / 256 bits

Criptografía de clave pública

- La distribución de claves siempre fue el punto débil de la criptografía tradicional
- Interés en buscar alternativas
- (*Diffie-Hellman ca. 1976*) “Criptografía de Clave Pública”
- La CCP es un criptosistema con las siguientes propiedades
  - D[E(P)] = P
  - D no se puede deducir fácilmente de E
  - E no puede romperse con un ataque de texto plano elegido

Criptografía de clave pública (ii)

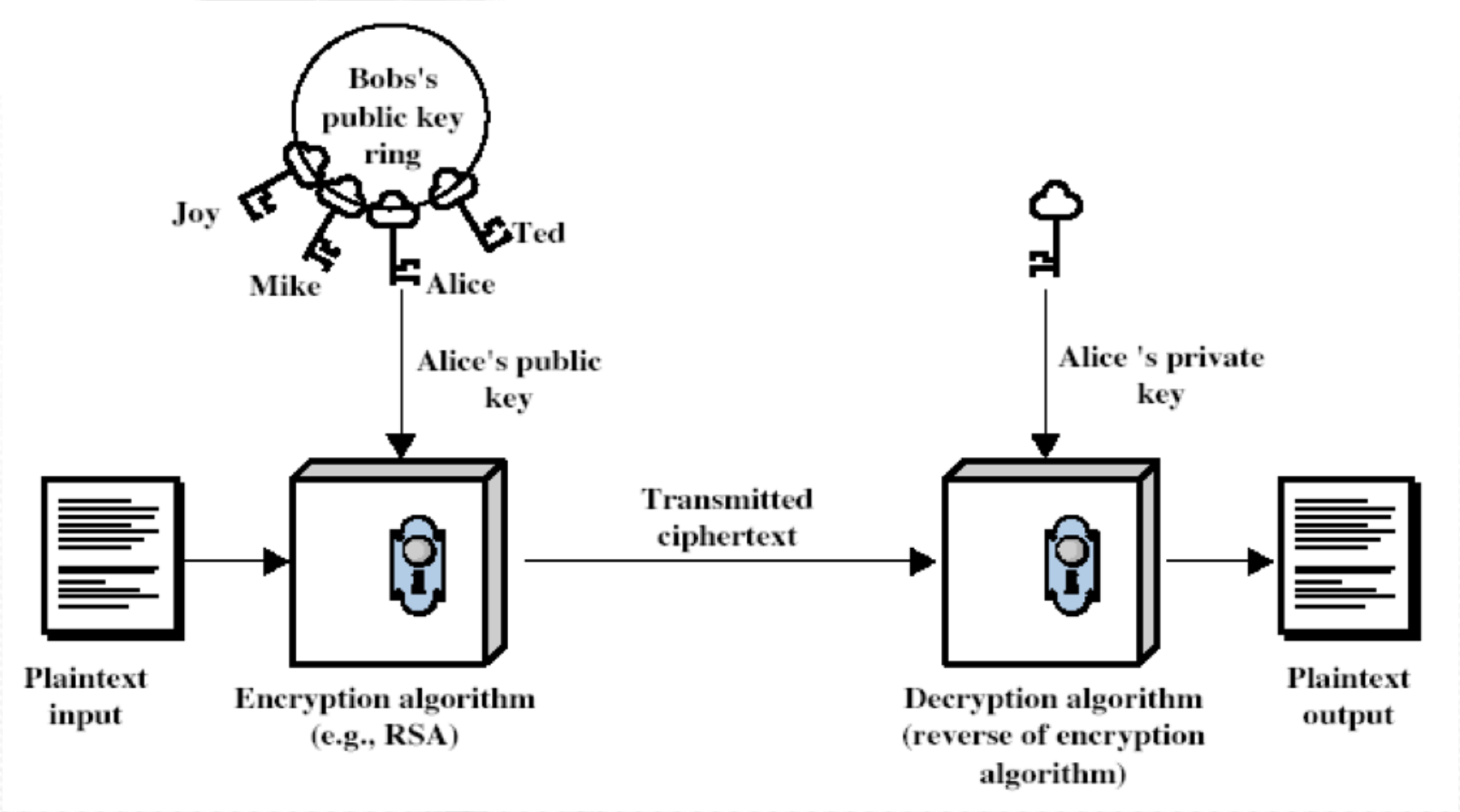
- Cada entidad genera un *par de claves*, una será la pública y otra la privada
  - Kpub, Kpriv
  - No son independientes entre sí
    - Dada una está dada la otra



- Para transimitir un mensaje “X” de A -> B se calcula:
  - $Y = E [Kpub_B, X]$
- Al recibir, B calcula:
  - $X' = D[Kpriv_B, Y]$

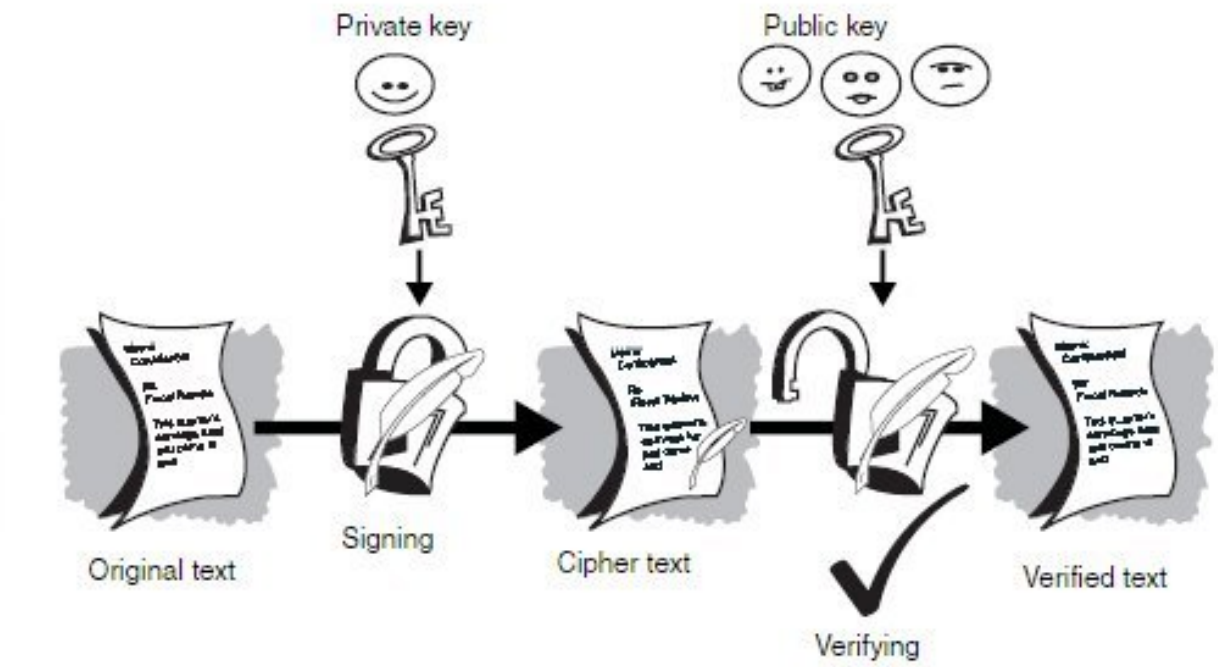
Criptografía de clave pública (iii)

- (fuente: Stallings) ***



Firma digital

- Objetivo de la firma digital:
  - *Establecer pruebas de integridad de documentos digitales*
- Implementable utilizando criptografía de clave pública

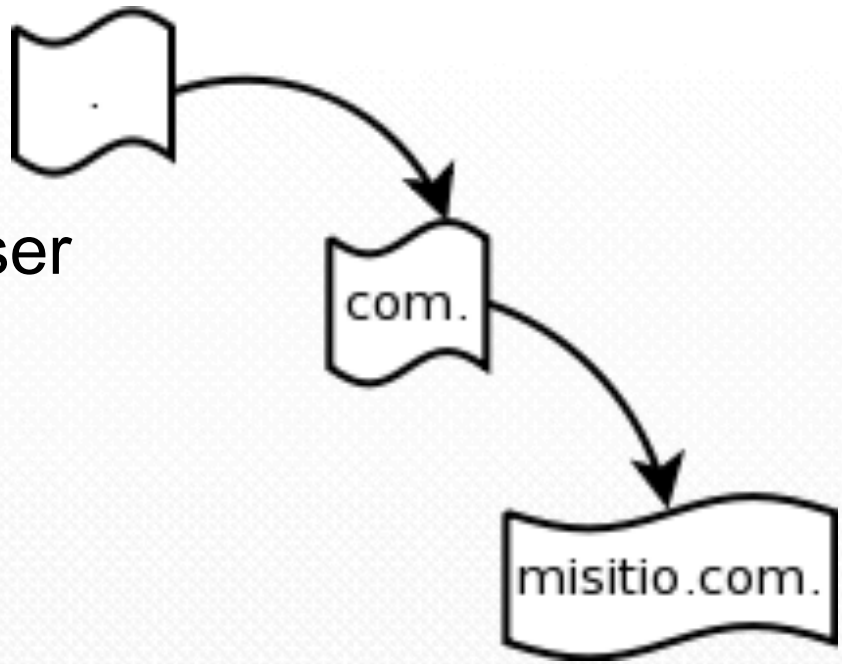


Firma digital (ii)

- Dado un documento M a ser firmado por A(lice) para ser recibido por B(ob)
  - A calcula:
    - Un hash de M, **H = Hash[M]**
    - Una firma del mensaje, **F = E[$Kpriv_A$, H]**
  - A transmite {M, F} hacia B
- Al recibir, B calcula:
  - El hash de M, **H' = Hash[M]**
  - Regenera el hash a partir de la firma **H = D[$Kpub_A$, F]**
  - ***Es H == H' ??***

Firma digital (iii)

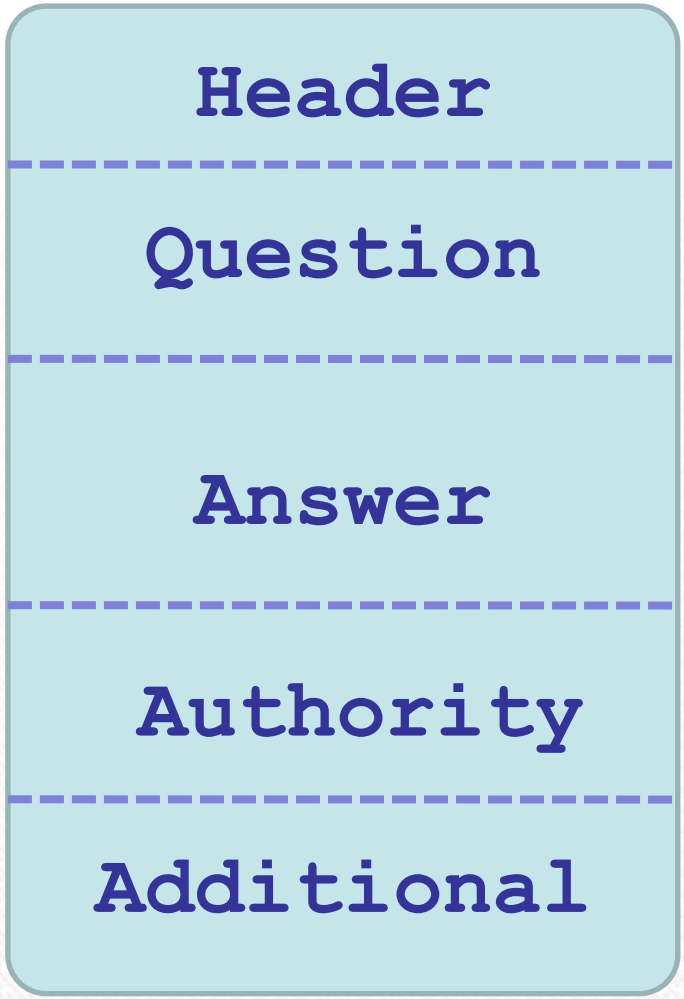
- Cadenas de confianza
  - Cada nivel de una jerarquía firma material de la siguiente
  - La raíz de la jerarquía debe ser considerada especialmente
  - La validación puede ser
    - Top down
    - Up down



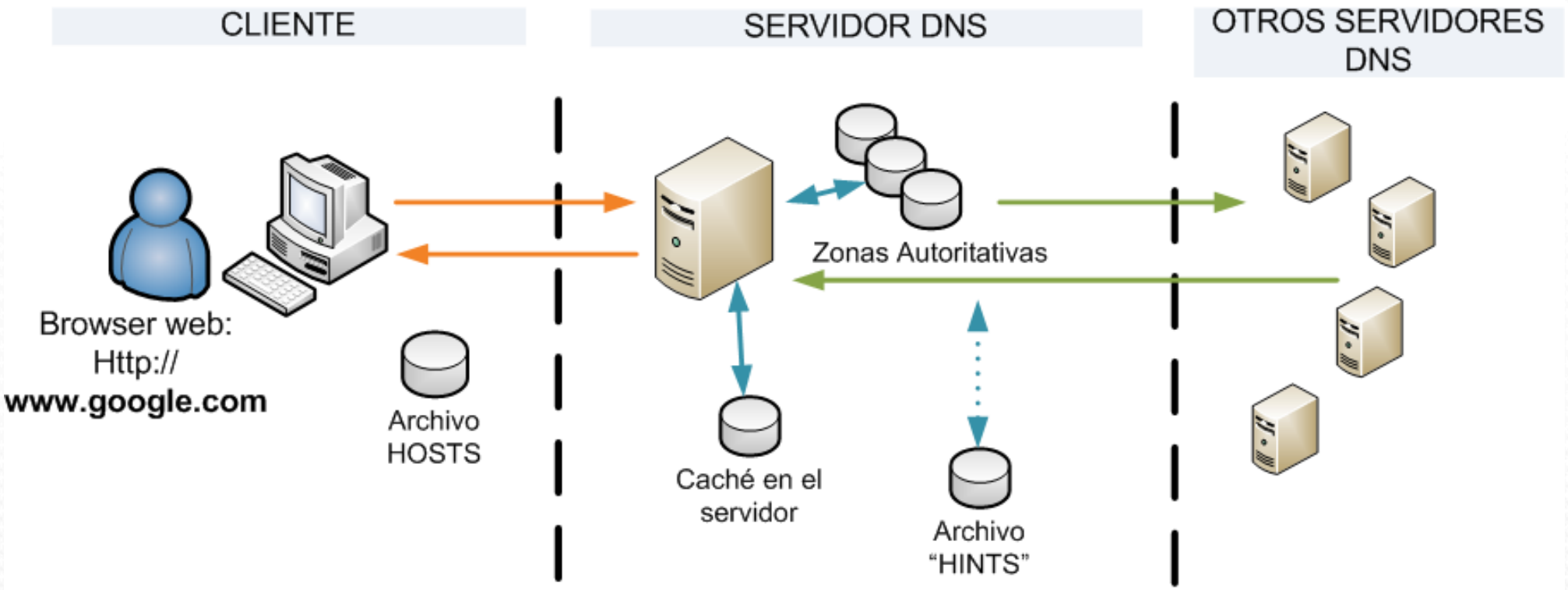
DNSSEC: MOTIVACIÓN

Especificacion del protocolo

- Recordamos: formato de paquetes DNS
  - Header
    - Encabezado del protocolo
    - Flags (QR, RA, RD,…)
  - Question Section
    - La pregunta que hacemos al DNS
      - Tuplas (*Name, Type, Class)*
  - Answer Section
    - RRs que responden la pregunta (si es que hay), también en (N, T, C)
  - Authority Section
    - RRs que apuntan a una autoridad (opcional)
  - Additional Section
    - RRs que a juicio del DNS pueden ser útiles para quien está preguntando, y que pueden no ser autoritativos



Consultas DNS

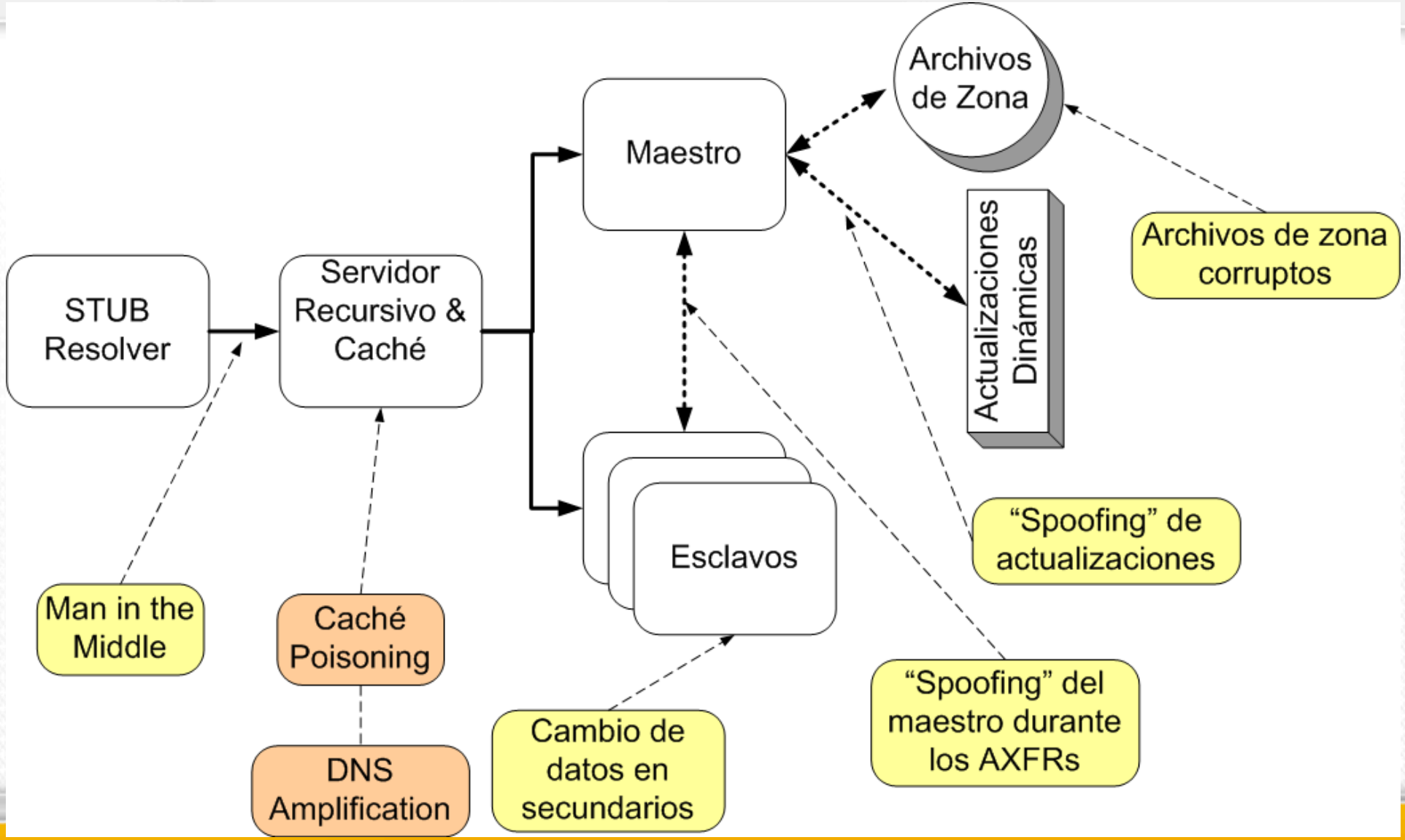


"resolver" local

DNS recursivo local

Otros servidores autoritativos

Vectores de ataque en DNS



Vulnerabilidades del protocolo DNS

- La información transmitida en DNS puede ser "*spoofed*"
  - Entre maestro y esclavo (AXFR)
  - Entre maestro y sus clientes "*resolver*"
- Actualmente el protocolo DNS no permite validar la información contenida en una respuesta
  - Vulnerable a las diferentes técnicas de *poisoning*
  - Datos envenenados siguen causando problemas por un tiempo (potencialmente grande, TTL)
- Tampoco los secundarios tienen manera de autenticar al primario con el que están hablando

Introduciendo DNSSEC

- Análisis de vulnerabilidades en DNS
  - RFC 3833: "*Threat Analysis of the Domain Name System (DNS)*"
- DNSSEC:
  - "*DNS Security Extensions*"
  - RFC 4033, 4034, 4035
  - ~ Marzo 2005
    - Aunque DNSSEC viene siendo tratado desde hace mucho mas tiempo en el IETF

¿De que nos protege DNSSEC?

- DNSSEC nos protegerá de corrupción y del *spoofing* de datos
  - Proporciona un mecanismo para poder validar la autenticidad y la integridad de los datos contenidos en una zona DNS
    - DNSKEY/RRSIG/NSEC
  - Proporciona un mecanismo para delegar la confianza en ciertas claves públicas (cadena de confianza)
    - DS
  - Proporciona un mecanismo para autenticar las transferencias de zona entre primarios y secundarios
    - TSIG

Introducción a DNSSEC

- DNSSEC *no* es un nuevo protocolo
- Es un conjunto de **extensiones** al protocolo DNS tal como lo conocemos
  - Cambios en el "*wire protocol*" (EDNS0)
    - Extensión del tamaño máximo de una respuesta UDP de 512 a 4096 bytes
  - Agregado de nuevos *resource records*
    - RRSIG, DNSKEY, DS, NSEC
  - Agregado de nuevos flags
    - Checking Disabled (CD)
    - Authenticated Data (AD)

Introducción a DNSSEC (2)

- Nuevos RR
  - RRSIG: *Resource Record Signature*
  - DNSKEY: *DNS Public Key*
  - DS: *Delegation Signer*
  - NSEC: *Next Secure*
- Nuevos Flags:
  - AD: indica que la respuesta esta autenticada
  - CD: indica que no se realiza chequeo (deshabilitado)

Introducción a DNSSEC (3)

- (Repaso) Un *resource record* en DNS es una tupla de cinco valores
  - (*nombre, clase, tipo, TTL, valor)*
- El registro:
  - `www.empresa.com. 86400 IN A 200.40.100.141`
  - Esta representado por la tupla:
    - Nombre (www.empresa.com)
    - Clase (IN)
    - Tipo (A)
    - TTL (86400 segundos)
    - Valor (200.40.100.141)

Introducción a DNSSEC (4)

- *Resource Record Sets (*RRSets)
  - DNSSEC opera firmando *RRSet*s (no RR individuales)
  - Un RRSet es un conjunto de resource records que comparten igual:
    - Clase
    - Tipo
    - Nombre
- Ejemplo de RRSet (TTL omitido):
  - `www IN A 200.40.241.100`
  - `www IN A 200.40.241.101`

Introducción a DNSSEC (5)
Firma de zona

- Se genera un par de claves (publica y su correspondiente privada) para cada **zona**
  - El par de claves es propio de cada zona y no del servidor autoritativo
  - La parte privada se debe mantener bajo custodia
    - La privada firma los RRSets de la zona
  - La publica se debe publicar en DNS mediante un registro DNSKEY
    - La privada permite verificar las firmas de los RRSets
  - Un RRSet puede tener multiples firmas generadas con diferentes claves

Introducción a DNSSEC (6)

- La firma digital de un RRSet se devuelve en forma de un registro RRSIG que es parte de la respuesta
- Ejemplo:

```
~ carlosm$ dig +dnssec www.nic.se

;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 1

;; ANSWER SECTION:
www.nic.se.             60      IN      A       212.247.7.218
www.nic.se.             60      IN      RRSIG   A 5 3 60 20101021132001
20101011132001 23369 nic.se. HeeUZ5h5iExK5uU1SuNRIf2Dbmh2/
aWV8FkjmzixUzTAVrHv39PfmfnG DHdHoZxoz85hqqYiWb
+t9EZh5+iqxQk8AxRDic9Nn6WxifOoWeS+IUKQ
rVyqXf1NtkZvu1A325vwa8obtbeVGVkhqg6bDIjKYeHixjlQ4cRoFcEW Izk=

;; AUTHORITY SECTION:
nic.se.                 2974    IN      NS      ns3.nic.se.
nic.se.                 2974    IN      NS      ns2.nic.se.
nic.se.                 2974    IN      NS      ns.nic.se.
nic.se.                 3600    IN      RRSIG   NS 5 2 3600
20101021132001 20101011132001 23369 nic.se. GSzAUC3SC3D0G/
iesCOPnVux8WkQx1dGbw491RatXz53b7SY0pQuyT1W
eb063Z62rtX7etynNcJwpKlYTG9FeMbDceD9af3KzTJHxq6B+Tpmmxyk
FoKAVaV0cHTcGUXSObFquGr5/03G79C/YHJmXw0bHun5ER5yrOtOLegU IAU=
```

Cadena de confianza

- ¿Como puede un cliente verificar un RRSet de una cierta zona?
  - Hace una consulta por el DNSKEY correspondiente
  - Realiza los calculos correspondientes y los compara con el RRSIG
    - Si coinciden, la firma verifica, de lo contrario, no
- Pero ¿como se puede confiar en la DNSKEY si sale de la misma zona que queremos verificar?
  - Necesitamos verificar la **cadena de confianza**

Cadena de confianza (ii)

- Registro DS "*Delegation Signature*"
  - Los registros DS "firman" claves de zonas **hijas**
  - De esta forma uno puede verificar el DNSKEY de una zona buscando un registro DS en la zona padre
- El registro DS contiene un hash de la una clave pública
  - Es decir, del contenido de un registro DNSKEY
- Los registors DS en la zona padre están firmados con la(s) claves de esa zona
- Para completar la cadena de confianza tiene que estar firmada la **raíz del DNS**

Cadena de confianza (iii)

- Pero ¿que pasa con la zona raíz?
  - La zona raíz no tiene “padre” a quien ir a pedirle un registro DS
  - La raíz del DNS esta firmada desde julio de 2010
    - *[http://www.root-dnssec.org]*
  - El registro DS para “.” se puede obtener fuera de banda
    - [http://data.iana.org/root-anchors/root-anchors.xml]
    - . IN DS 49AAC11D7B6F6446702E54A1607371607A1A41855200FD2CE1CDDE32F24E8FB5

Introducción a DNSSEC (9)
Firma de la raíz

- ¿Cómo se verifica la autenticidad del root trust-anchor?
- El TA de la zona raíz se publica fuera de banda, por ello la validación debe ser diferente
  - Se puede bajar por HTTP/HTTPS
  - Se puede verificar por otros mecanismos (certificados, firmas PGP)
  - Similar a lo que pasa con la zona raíz misma, se debe cargar manualmente

Introducción a DNSSEC (10)
Negación de existencia

- Respuestas con “NXDOMAIN”
  - Niegan la existencia de un nombre
  - Son respuestas “cacheables” a pesar de ser negativas
- ¿Como firmar la no-existencia?
  - Necesito tener un RRSet para firmar
    - Recordar que en DNSSEC lo que se firma siempre son RRSets
  - Técnicas propuestas:
    - NSEC
    - NSEC3

ZSK vs KSK***

- ZSK
  - Zone Signing Key
- KSK
  - Key Signing Key

Consideraciones finales DNSSEC vs PKI

- DNSSEC no implementa una PKI sobre DNS
  - Si bien es cierto que se parece ☺
- ¿Por qué no?
  - Los procedimientos de gestión de claves están basados en políticas locales
    - No hay "*certificate authority*"
    - Si todo un dominio y subdominios están bajo una administración única, entonces si se puede aplicar mas estrictamente un conjunto de políticas
  - No hay CRL ("*Certificate Revocation List*")

Desplegando DNSSEC

- Veremos cuales serían los pasos para desplegar DNSSEC en una zona
- Los comandos que mostraremos son específicos de BIND 9.6/9.7

Procedimiento básico de firma de zona

- Generación de un par de claves
  - Incluir el DNSKEY creado en la zona
  - Si lo hacemos con BIND esto dispara:
    - El ordenamiento de la zona
    - Inserción de los registros RRSIG
    - Generación de registros DS
      - Recordar que van en el padre

LACNIC

Latin American and **Caribbean** Internet Addresses Registry
Registro de Direcciones de Internet para **América Latina** y **Caribe**
Registro de Endereços da Internet para **América Latina** e **Caribe**

¿Preguntas?