Seguridad y Criptografía (Introducción)

Sistemas Distribuidos – ITInformática (UVA)

César Llamas Bello – © 2003

Índice

Introducción

- La seguridad es todo lo que concierne a asegurar que no ocurren cosas **malas**.
  - Alternativa A: no moverse.
  - Alternativa B: moverse, pero con seguridad.
- es relativa a la amenaza que cada uno afronta
- afecta a todos los puntos del sistema
- debe ser fácil de obtener
- debe ser asequible
- debe obtenerse de forma **simple**

Criptografía y Seguridad

- La criptografía es el arte de codificar información de forma secreta
- La criptografía es una herramienta interesante de las técnicas de seguridad

Amenazas y protección

- Tipos de amenazas:
  - A la privacidad
  - A la integridad
  - A la disponibilidad
  - están relacionadas: cuando un sistema cae no lo suele hacer de modo seguro (*fail safe*)

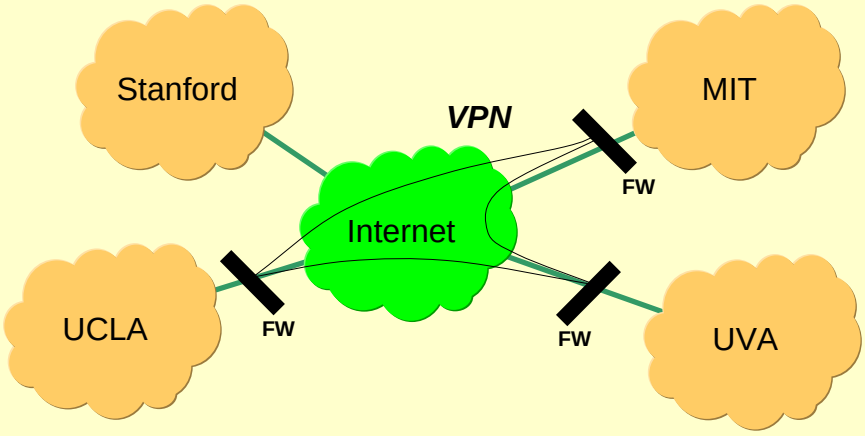
Defensa perimetral

- Aproximación que distingue la parte interna de la externa del sistema
  - Evitando la conexión
  - Encapsulando el sistema (VPN)
- En los sistemas practicables, la defensa perimetral ha de ser selectiva
  - El perímetro puede establecerse en cada capa de un esquema arquitectónico orientado a capas.
  - Puede establecerse por tipos de comunicación

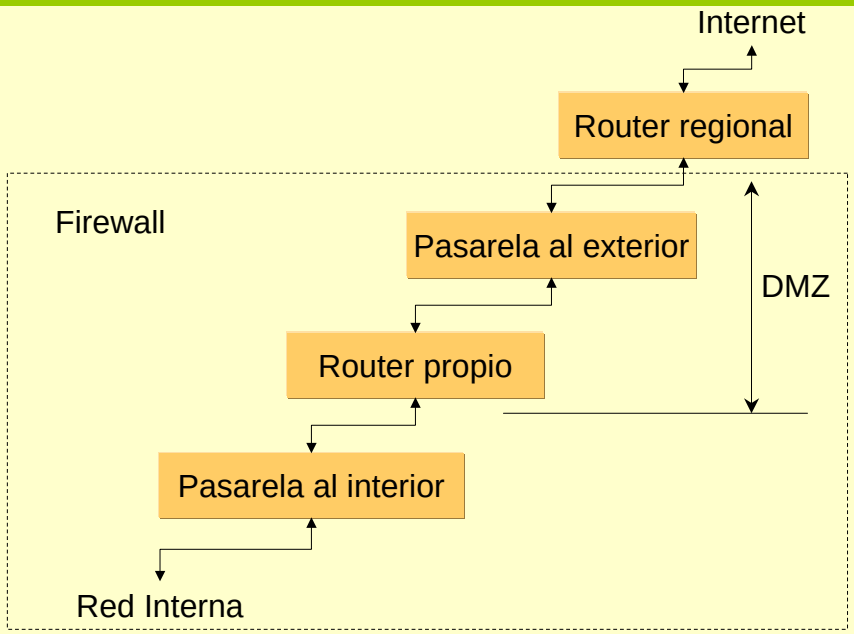
Defensa perimetral (Firewalls)

- Es una máquina entre una red privada y una pública.
  - Filtran el tráfico de la red siguiendo una *política de seguridad*.
  - Redirige tráfico hacia máquinas seguras
  - Manipula el contenido del tráfico.
- Problemas
  - A veces la amenaza proviene del interior.
  - La defensa perimetral limita las posibilidades.
  - Puede ocasionar cuellos de botella

Redes Virtuales Privadas con Firewalls



Esquema de conexión de un Firewall



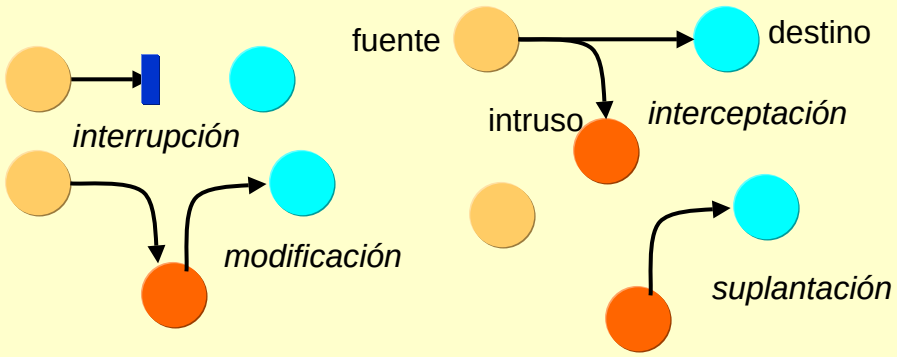
Control de acceso y modelos de seguridad

- Un modelo de seguridad es una abstracción sobre el control del acceso a datos protegidos
- Para implementar la seguridad se utilizan servicios de seguridad.
- Criterios de clasificación de modelos
  - MAC y DAC
  - Modelos de seguridad de datos y de información
  - Modelos dinámicos

Servicios de seguridad

- *Confidencialidad*, es decir el manejo privado de la información.
- *Autentificación* o la capacidad de asegurar la identidad de un sujeto.
- *Integridad*, que asegura que la información que empleamos no ha sido manipulada desde el origen.
- *No repudio*, de una operación de emisión y recepción de información por parte de los agentes.
- *Control de acceso* a la información y/o recursos administrados por un sistema.
- *Disponibilidad* de los recursos necesarios de un sistema cuando sea necesario.

Ataques a la seguridad

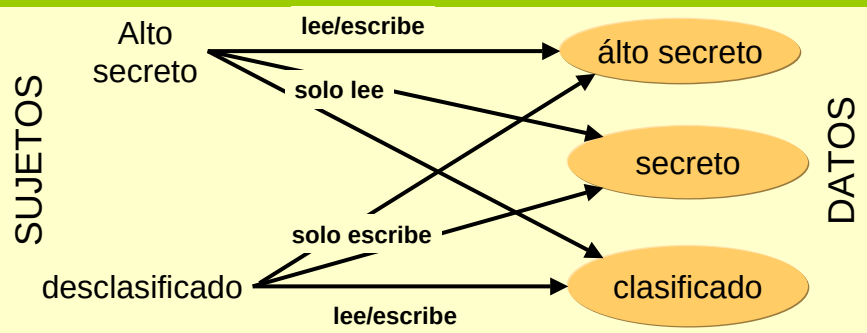


- Interrupción: destruye la información o la inutiliza. Ataca la disponibilidad.
- Interceptación: Obtiene acceso a información. Ataca la confidencialidad.
- Modificación: Modifica la información.Ataca la integridad.
- Fabricación: Falsifica la información. Ataca la autenticidad.

Modelos MAC y DAC

- MAC (mandatory access control)
  - las entidades del sistema son o sujetos u objetos
  - A cada entidad se le asigna un nivel de sensibilidad
    - Típicamente se forma una red sobre una relación **domina_a/2**.
    - Ej: si hay dos niveles o uno domina a otro o ambos son incompatibles.
- Un ejemplo es el sistema de dominios de
  - D.E. Bell y L.J. LaPadula. Secure Computer Systems: A Mathematical Model. Journal of Colmputer Security, 1969.

MAC



- Un sujeto puede tener acceso a un objeto si y solo si su nivel domina el del objeto, y puede escribir si y solo si su nivel es dominado por el del objeto.
  - Se denomina informalmente: *read-down*, y *write-down.* O mejor: *no read-up* y *no write-down*.
- Dos entidades pueden comunicarse en ambas direcciones solo si están en el mismo nivel.

DAC

- DAC (*Discretionary access control*)
  - Ejemplo: UNIX
- El usuario (propietario) de cada archivo puede determinar quién más puede acceder al archivo mediante los bits de permiso.
  - Ojo: Cualquiera que pueda leer un archivo también puede copiarlo y dejarlo leer a otros.

Acceso a los Datos y a la Información

- Modelos basados en
  - acceso a Datos: Quién accede a los datos
  - acceso al Flujo de Información: Qué permisos se tienen sobre la información que va por el canal.
- La aparición de estos últimos se debe a la existencia de:
  - Canales aparentes (*overt channels*)
  - Canales encubiertos (*covert channels*) que aparecen en características sobre recursos.

Modelos Estáticos y Dinámicos

- En la práctica, el estatus de los datos y los sujetos puede cambiar.
  - Ejemplo: en MAC, la visibilidad (*clearance*) del sujeto puede cambiar. Los datos pueden promocionarse o degradarse.
- Modelos:
  - High-Watermark: la sensibilidad del un dato varía en función de la visibilidad del último sujeto que accedió.
  - Chinese-Wall: se erigen barreras de confianza en términos de las relaciones que mantienen los sujetos
  - Clark-Wilson: Condiciones de seguridad para transacciones financieras.

Consideraciones sobre el uso de los modelos

- Decidibilidad: se puede decidir si el sistema es seguro a partir de un modelo general de un sistema real y una condición o requisito peculiar de seguridad.
- Dada la imposibilidad de modelar, especificar o analizar un sistema completo, se trabaja en la Componibilidad:
  - cómo se garantiza la seguridad a partir de la seguridad de componentes.
- Dificultad en integrar sistemas de legado: Debe preservarse la seguridad original de los sistemas de legado al implementar interoperabilidad.
- La seguridad no solo significa confidencialidad, sino también integridad.

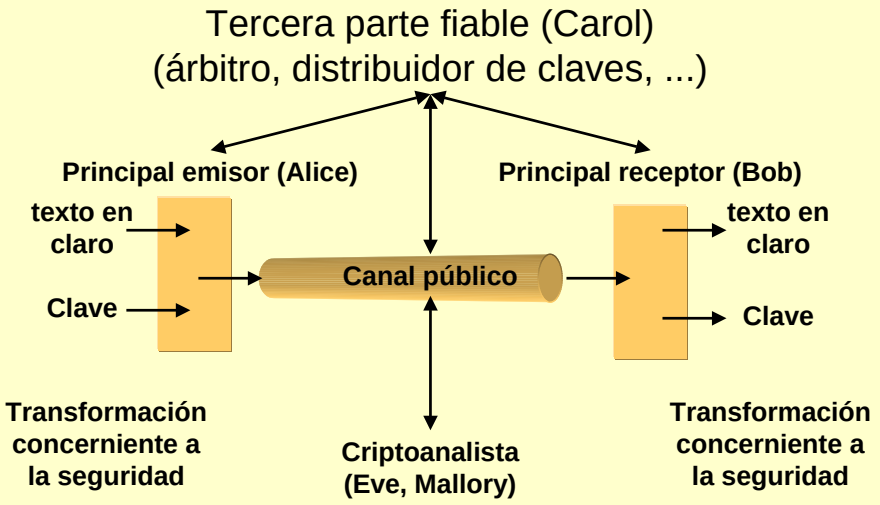
Utilización de criptografía para la seguridad

- Es una parte de los sistemas seguros.
- Disciplinas: Criptografía y Criptoanálisis.
  - Construcción y ataque de criptosistemas
- Conceptos más usuales:
  - Cifradores simétricos.
  - Cifradores asimétricos
  - Funciones de dispersión de un sentido.

Algoritmos para la criptografía

- Algoritmos más conocidos
  - Clave privada: Aplicación más conocida
    - IDEA PGP
    - DES PEM, SNMPv2, Kerberos
    - (X.509) PEM
    - SkipJack, Twofish, AES, ...
  - Clave pública:
    - RSA PGP, PEM
    - LUC
    - DSS, DSA, ElGamal, ...
  - Funciones Hash
    - MD5 SNMPv2
    - SHA-1 DSS
    - Snafu

Modelo criptográfico del sistema



Requisitos de los criptosistemas

- El canal es público
  - Debemos asumir que el enemigo captura mensajes
- Los algoritmos son públicos
  - La seguridad debe recaer sobre la clave
  - El algoritmo será analizado por el criptoanalista

Tipos de ataque criptoanalítico

- Escucha pasiva: el criptoanalista solo registra la actividad, o des-encripta.
- Ataque activo: el enemigo inserta, modifica o borra mensajes legítimos.
- Suplantación: el enemigo suplanta al emisor y malversa los mensajes.
- Repetición: se leen mensajes legítimos y se reinyectan en la red más tarde.
- Cortar y pegar: se crean mensajes nuevos con trozos de mensajes legítimos para enturbiar la comunicación.
- Borrado de tiempo: se intenta confundir al tiempo de red.
- Ataque de cumpleaños: se ataca a una función hash conociendo dos mensajes diferentes con el mismo valor hash.

Cifrador simétrico

Un sistema criptográfico simétrico es una familia de transformaciones uniparamétricas invertibles E_K, donde $K \in \mathbf{K}$.

K es el espacio de claves.

M es es el espacio de mensajes sin encriptar (texto en claro –*plain text*)

C es es el espacio de criptogramas o espacio de texto cifrado, el sistema debe cumplir ciertas propiedades

Propiedades del cifrado simétrico

- El algoritmo de encriptado es una aplicación (invertible)

  $E_K(M) = C$, con $M \in \mathbf{M}$ y $C \in \mathbf{C}$

- Hay un algoritmo inverso D_K llamado algoritmo de desencriptado.

  $E_K^{-1} = D_K$, con $D_K(C) = D[E_K(M)] = M$

- Las claves deben definir de manera única el mensaje encriptado

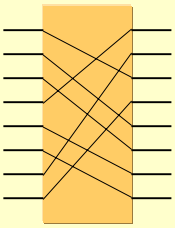
  $E_{K1}(M) \neq E_{K1}(M)$ si $K1 \neq K2$.

Data Encription Standard

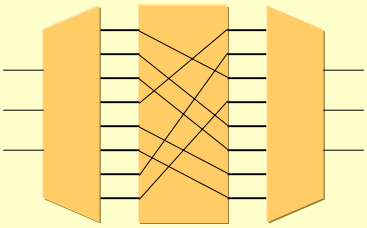
- Usa substitución (caja S) y transposición (caja P) sobre bits
- Encripta bloques de 8 bytes (64 bits) con clave de 56 bits.
- Trabaja a nivel de bit -> robustez
- Efecto avalancha -> cambia completamente el resultado.
- Las cajas básicas se interconectan con registros de desplazamiento, transposición, y operaciones XOR.
- Las permutaciones se almacenan en tablas, que son diferentes en el caso de encriptación y desencriptación.
- (a) líneas generales, (b) detalle de una iteración.

DES

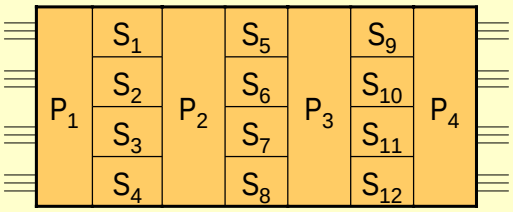
Caja S (substitución)



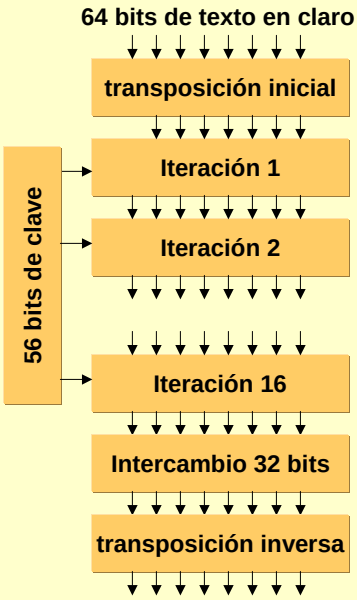
Caja P (permutación)

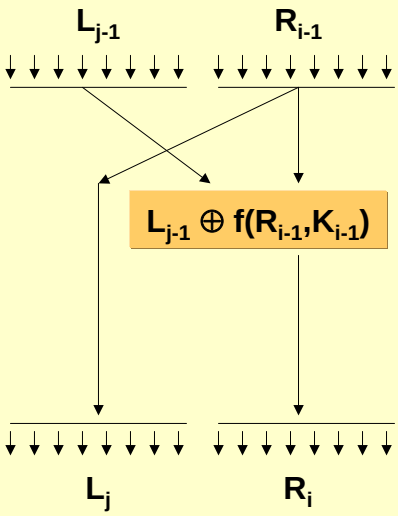


Cifrador Producto



DES





DES

- DES multinivel: etapas con varias claves para aumentar la robustez del sistema.
  - Para información muy sensible o claves maestras.
- DES doble:

  $C \leftarrow E_{K2}[E_{K1}[P]]$ $\quad\quad$ $P \leftarrow D_{K1}[D_{K2}[C]]$
  - Aumenta el tamaño de **C** pero no aumenta su robustez frente a una sola clave.
- DES triple:

  $C \leftarrow E_{K1}[D_{K2}[E_{K1}[\ P]]]$ $\quad\quad$ $P \leftarrow D_{K1}[E_{K2}[\ D_{K2}[[C]]]$
  - Se duplica el tamaño de la clave
  - Adoptada en ANS X9.17 y ISO 8732 para PEM.

Utilización de cifradores simples

- Los métodos criptográficos convencionales, como DES, IDEA y Skipjack, se emplean para construir operadores de encriptación-desencriptación sobre bloques de datos, y se configuran para actuar en *modos de operación*.
  - Modo de libro de códigos electrónico
  - Modo de encadenamiento de bloque de cifrado (CBC)
  - Modo de realimentación de salida
  - Modo de realimentación de cifra
  - Claves de acceso de un solo uso

ECB (Electronic Codebook)

- Se encripta consecutivamente cada bloque de texto sencillo de 8 bytes del mensaje con la misma clave y por separado, encadenando el resultado.
- La principal debilidad es bloques idénticos producen idéntico resultado. Si el texto sencillo está altamente estructurado el criptoanalista dispone de pistas, y posiblemente de bloques de texto conocido.
- Solo se suele emplear en transmisión de claves y vectores de inicialización de otros *modos*.

CBC (Cipher Block Chaining)

$C_n \leftarrow E_K[P_n \oplus C_{n-1}]$ $\quad\quad$ $P_n \leftarrow D_K[C_n] \oplus C_{n-1}$

- Resuelve el problema anterior pero:
  - Encriptación del primer bloque (C_0): emisor y receptor se ponen de acuerdo en el primer bloque o *vector de inicialización* (IV):
    - debe escogerse aleatoriamente
    - no debe usarse en más de una comunicación
    - debe encriptarse en ECB o con clave privada.
    - En el caso de comienzo de bloques estereotipados hay que escoger un IV diferente por cada página de texto sencillo.
  - Relleno final con ceros o con números aleatorios.
  - Un error corrompe el resto del mensaje.

OFM (Output Feedback Mode)

- Para transmisión asíncrona de caracteres aislados (posibilidad de ataque).
  - Se emplea $E_K[\ ]$ como un generador de números aleatorios, y la semilla es el IV.

$$X_n \leftarrow E_K[X_{n-1}]$$

$$C_n \leftarrow P_n \oplus X_n \qquad P_n \leftarrow C_n \oplus X_n$$

  - Tiene la ventaja de que los errores no se propagan.
  - Tiene la desventaja de que el criptoanalista puede obtener información contrastando los cambios que se producen en cada carácter.
  - Notar que en origen y destino, se emplea el mismo método.

CFB (Cipher Feedback)

- Adecuado para *streams* de texto sencillo

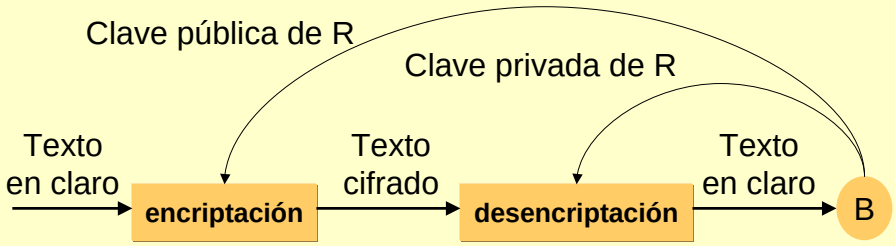
$$C_n \leftarrow P_n \oplus E_K[C_{n-1}] \qquad P_n \leftarrow D_K[C_n] \oplus C_{n-1}$$

  - Ver que al igual que en OFB, se emplea el mismo método para encriptar que para desencriptar.
  - Se puede extender a transmisión de caracteres si se emplea el modo de 8 bits y registro de desplazamiento
  - El método requiere algún tipo de detección de errores, dado que los errores se propagan en cadena.

Ventajas e inconvenientes de la clave privada

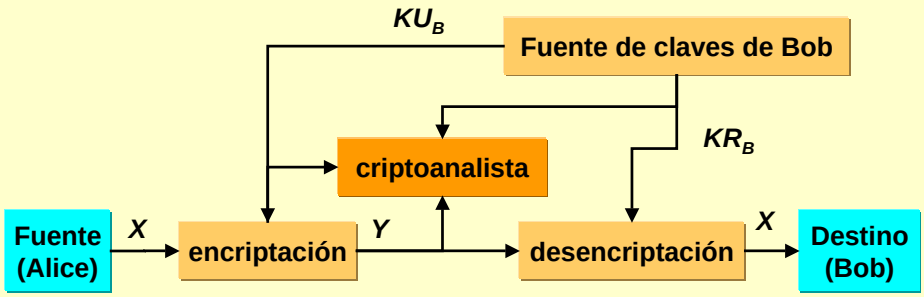
- Ventajas
  - Bajo coste del encriptado y desencriptado (Hay sistemas hardware)
  - Sirve para autenticar al emisor
- Desventajas
  - Distribución de claves entre principales sin contacto en Internet
    Problema del “hombre del maletín”
- ¿Existe un medio de distribución de claves seguro?

Criptosistemas asimétricos (clave privada)



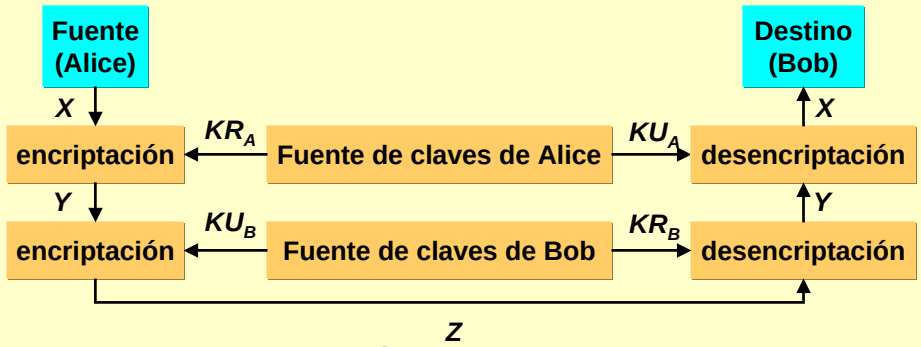
- “B” prepara dos claves: publica una de ellas KU_b, mientras la otra sigue siendo privada KR_b
- El emisor encripta con la clave pública, $Y=E_{KUb}[X]$, y el receptor desencripta con la otra, $X=D_{KRb}[Y]$,
- Problema inicial: Es de suponer que el enemigo conoce el método y accede a la clave pública.

Solución a la confidencialidad



- Este mecanismo resuelve el problema de la distribución de la clave (al menos en teoría), si el problema equivalente de ataque criptoanalista es suficientemente difícil.
- Para la autenticación es similar.
- El Criptosistema debe ser intercambiable

Solución a la autenticación y a la privacidad



- La primera encriptación sobre la firma del documento de la fuente proporciona autenticación. La segunda encriptación protege la privacidad.
  - Su desventaja principal se encuentra en el coste computacional de la encriptación y desencriptación de los métodos de clave pública.

Usos de diferentes algoritmos de clave pública

Algoritmo	Encriptado/ desencriptado	Firma digital	Intercambio de claves
RSA	Si (malo en bloques grandes)	Si	Si
LUC	Si (malo en bloques grandes)	Si	Si
DSS	No	Si	No
Diffie-Hellman	No	No	Si

Requisitos de un criptosistema de clave pública

1. poco costoso, de generar el par de claves.
2. Poco costoso, de encriptar.

$$Y = E_{KUb}[X]$$

3. poco costoso de desencriptar.

$$X = D_{KRb}[Y] = D_{KRb}[E_{KUb}[X]]$$

4. Inabordable determinar la clave privada a partir de la clave pública.

   Y similarmente obtener el texto en claro.

5. Es deseable que la encriptación y desencriptación sean intercambiables.

$$X = E_{KUb}[D_{KRb}[X]]$$

Códigos de autenticación de mensajes (MAC)

- Se añade un MAC (message autentification code), para comprobar la integridad del mensaje.
- Este código depende de una clave secreta K que comparte el emisor y el receptor CK[M]. De este modo el receptor puede evaluar de nuevo este código y comprobar que coincide con el que hay añadido al final del mensaje.
  - Garantiza que el mensaje no ha sido alterado.
  - Garantiza que el mensaje proviene del emisor con el que comparte la clave.
  - Si el mensaje comprende el número de secuencia (como en X.25, HDLC o TCP) el receptor puede asegurar la secuencia de mensajes.

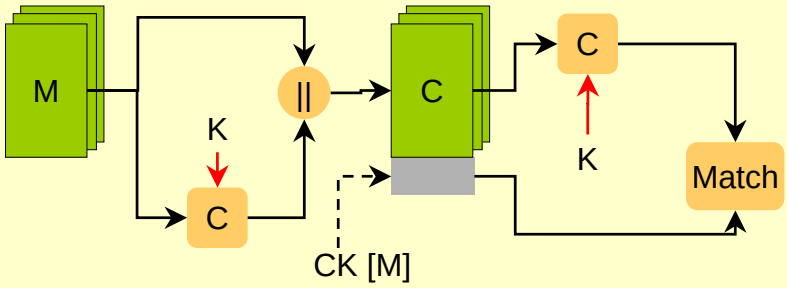
MAC (posibilidades)

- Se aplica una función de resumen (digest) difícil de falsificar.
- Función criptográfica
- Función de dispersión

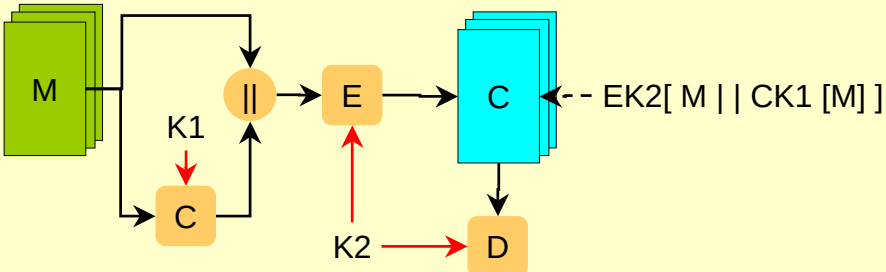
- Si el resumen contiene información de un documento autenticado, se garantiza también el origen de los datos.

MAC (criptо)

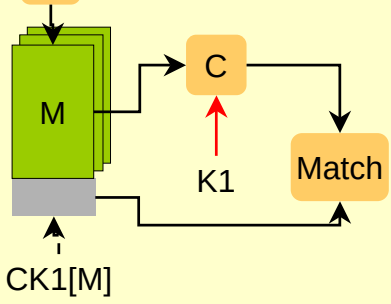
- M | | CK[M]
  - provee autentificación: solo A y B comparten K



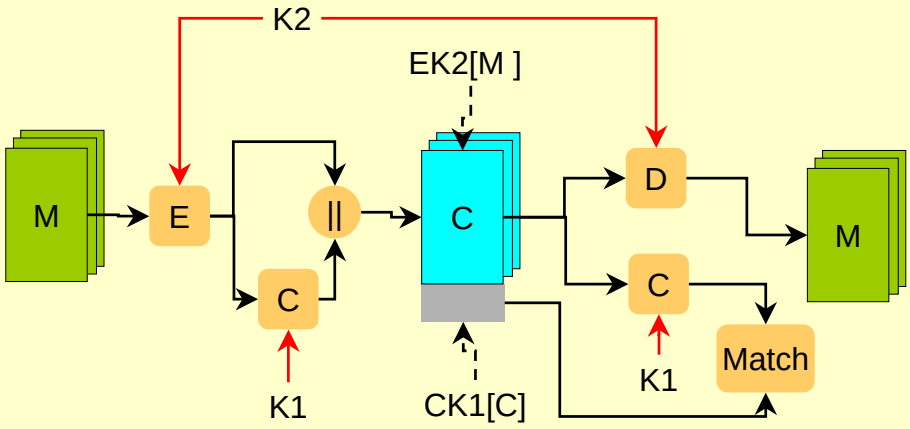
MAC (criptо)



- EK2[M | | CK1[M]]
  - Autentificación: solo A y B comparten K1
  - Confidencialidad: solo A y B comparten K2



MAC (cripto)



- EK2 [M] | | CK1[EK2 [M]]
  - Autentificación: usando K1
  - Confidencialidad: usando K2

MAC (Hash)

- Es una variación de MAC, en la que se calcula una función de dispersión sobre el texto h = H[M]; h es de tamaño fijo.
  - La diferencia radica en que la función H no necesita ser secreta, lo que hace conveniente encriptar el resultado.
  - Su misión es producir una especie de “huella dactilar” del texto.

MAC (Hash)

Para ser útil debe cumplir las siguientes propiedades:

1 Puede ser aplicada a un bloque de datos de cualquier tamaño

2 Produce una salida de longitud fija.

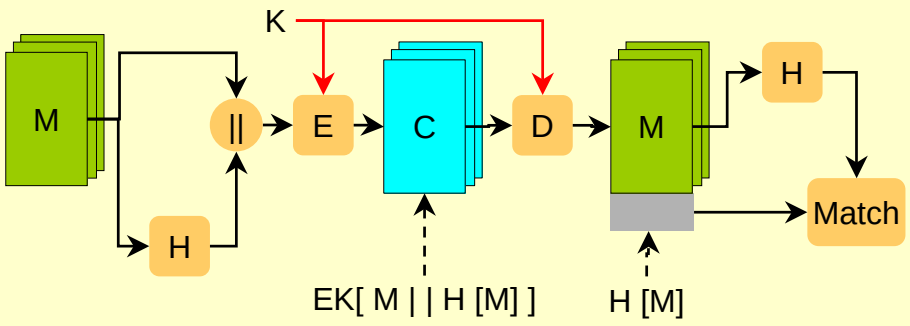
3 Es computacionalmente fácil de calcular.

4 Es computacionalmente impracticable averiguar el texto que da lugar al resultado.

5 Es computacionalmente impracticable averiguar un texto que dé lugar al mismo resultado

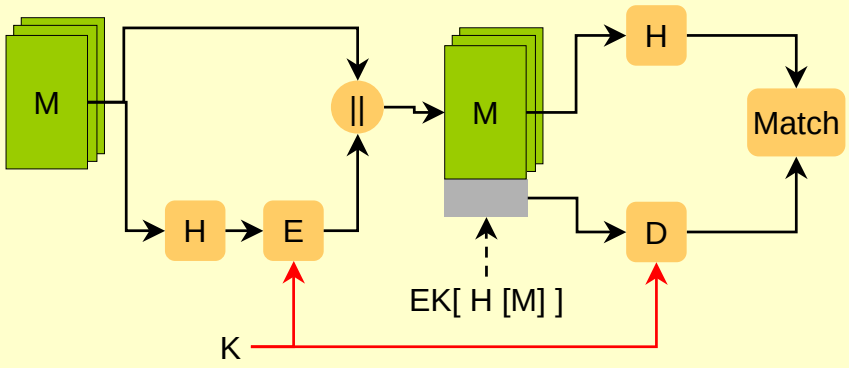
6 Es computacionalmente impracticable averiguar un par de de textos que compartan el mismo resultado.

MAC (Hash)



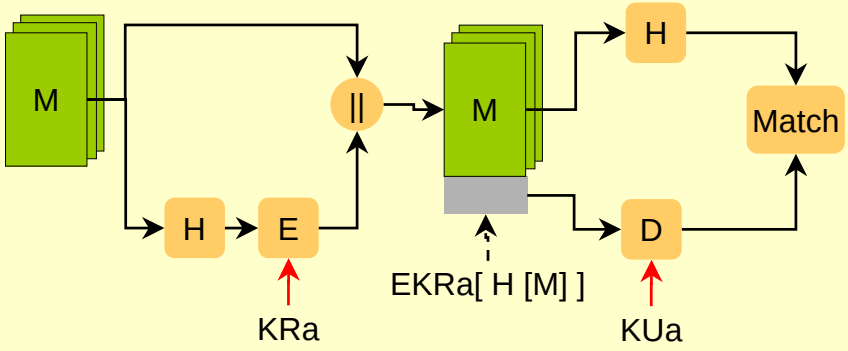
- EK[M | | H[M]]
  - Provee confidencialidad: solo A y B comparten K

MAC (Hash)



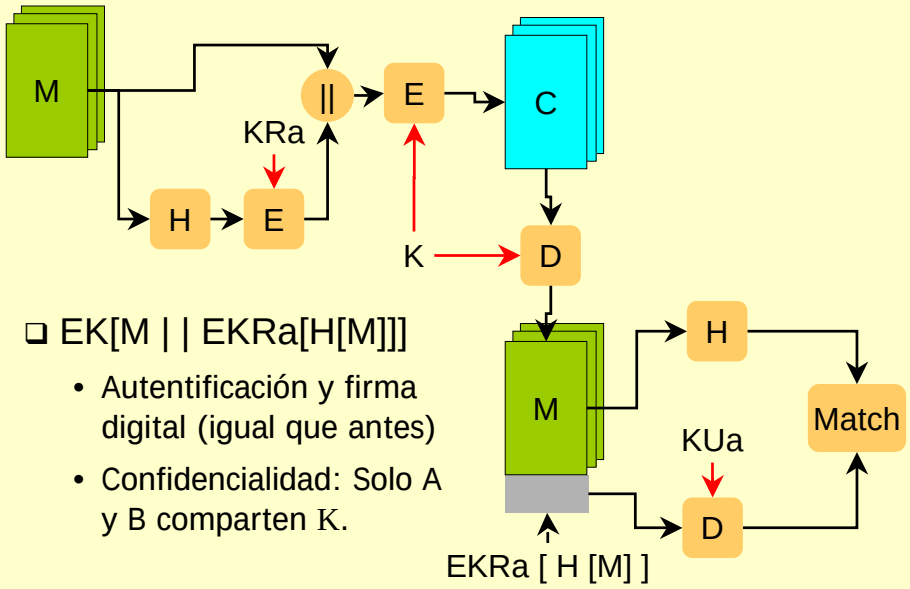
- M | | EK[H[M]]
  - H[M] está criptográficamente protegida.

MAC (Hash)



- M | | EKRa[H[M]]
  - Provee autentificación: H[M] está criptográficamente protegida.
  - Provee firma digital: Solo A pudo crear EKRa[H[M]]

MAC (Hash)

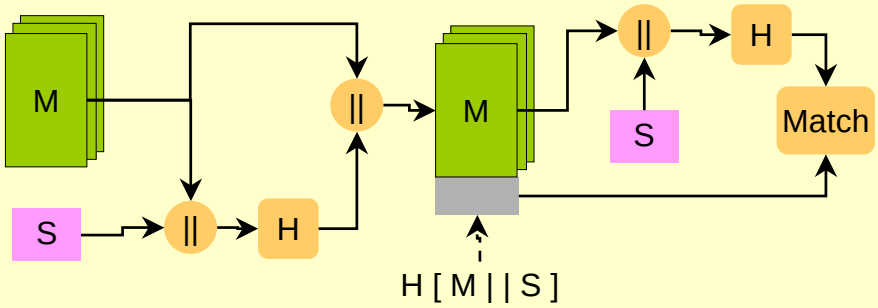


- EK[M | | EKRa[H[M]]]
  - Autentificación y firma digital (igual que antes)
  - Confidencialidad: Solo A y B comparten K.

Firmas digitales

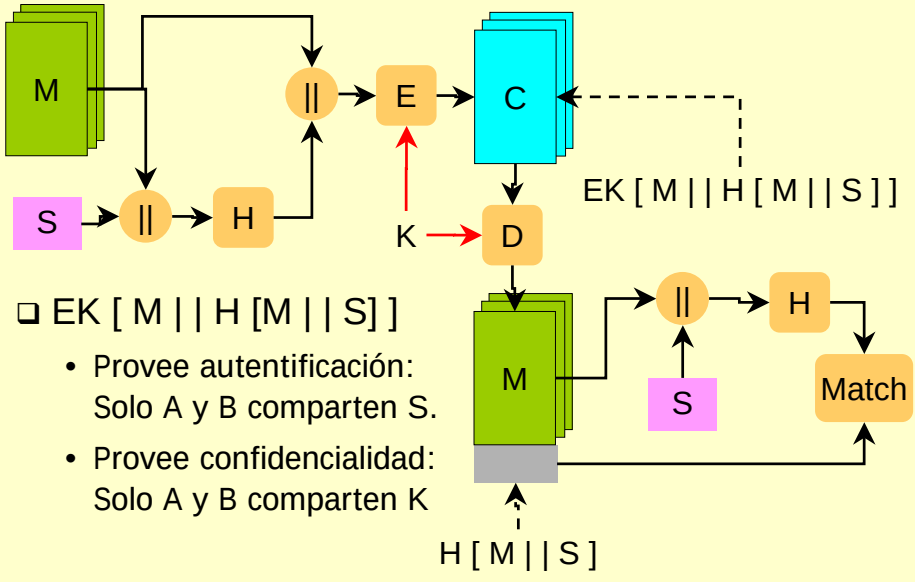
- Las firmas digitales asumen la función de la firma manuscrita en la realización de transacciones, preveniendo la disputa posible en el caso de transmisión de información en redes públicas
- De partida, la firma digital tiene que permitir la autentificación del documento.
- Propiedades:
  - Debe ser posible verificar el autor y la fecha y el tiempo de la firma.
  - Debe ser posible autentificar los contenidos en el momento de la firma.
  - La firma debe ser verificable por terceras partes para resolver la disputa.

Firmas Digitales



- M | | H[M | | S]
  - Provee autentificación de usuario y documento: Solo A y B comparten S.

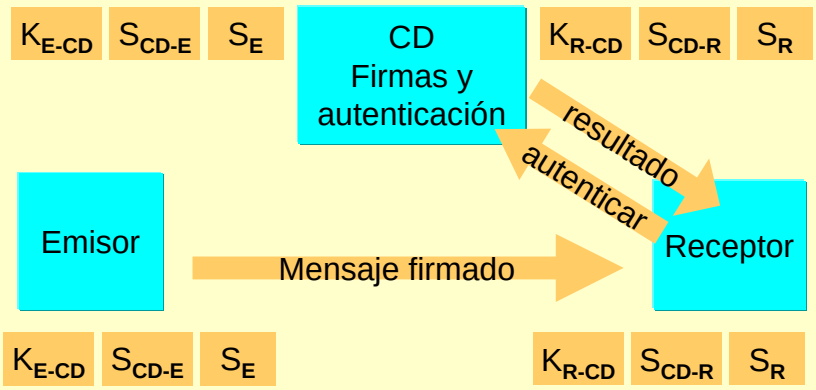
Firmas Digitales



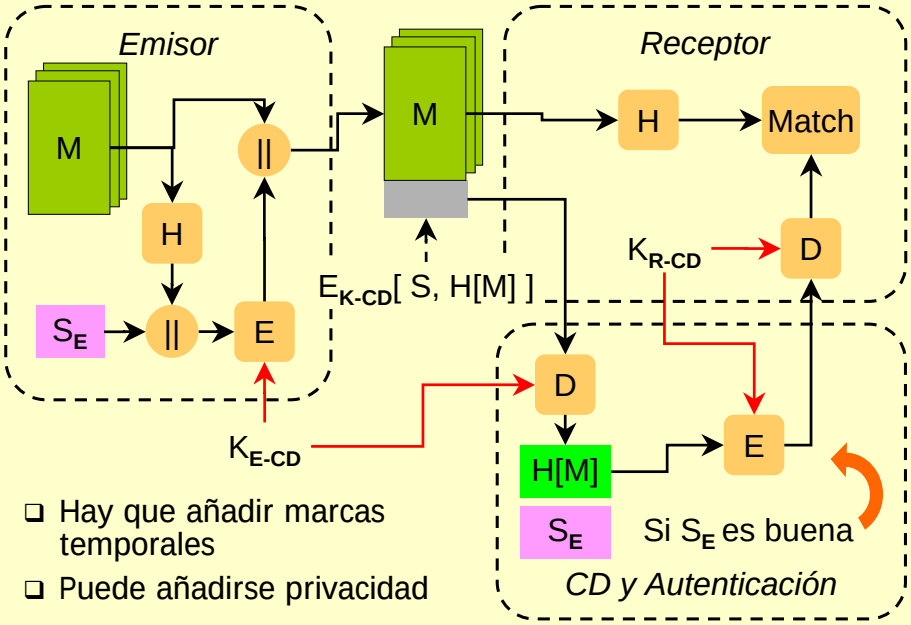
- EK [M | | H [M | | S]]
  - Provee autentificación: Solo A y B comparten S.
  - Provee confidencialidad: Solo A y B comparten K

Firmas digitales con centro de distribución

- Las firmas digitales anteriores son inseguras puesto que el receptor debe conocer la firma del emisor.



Firma autenticada sencilla



- Hay que añadir marcas temporales
- Puede añadirse privacidad

Firma autenticada

- El receptor puede conservar el documento y la firma, y verificar en cualquier momento.
  - Es obligatorio añadir fechas a los documentos.
- El CDA:
  - puede depositar su propia firma en las partes.
  - puede servir de repositorio de claves públicas firmadas para las partes.
  - no conoce el mensaje.
  - Es la autoridad frente a quien se denuncia el robo de claves.
  - Puede añadir caducidad a las firmas y claves.

Firmas Digitales arbitradas

- Aparece un árbitro que realiza las funciones de notario (N) mediante el cual se realiza la transacción.
  - Somete la transacción y la firma a ciertos tests para comprobar su origen (A) y la integridad del mensaje (M)
  - Fecha y envía el mensaje al receptor (B) con una indicación de verificación.

  ↳ La firma del árbitro permite prevenir el repudio del mensaje (análogo a una escritura)
- La fiabilidad de este árbitro es el punto clave del sistema